

Bridging IT and OT:

Cisco's Industrial Networking for Secure, Automated Operations



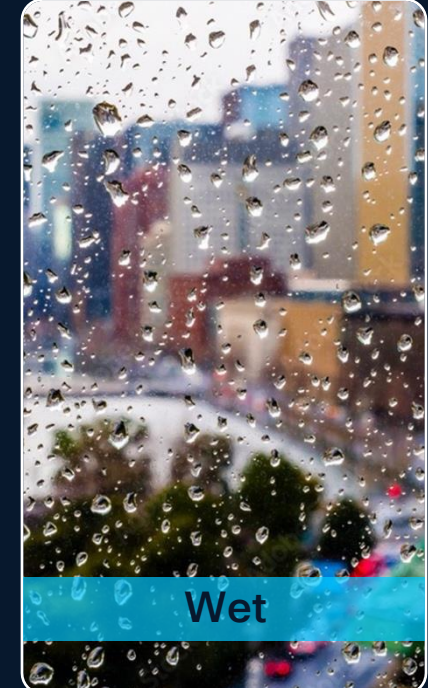
Kayla Gerry
Account Executive, IloT

Mike Wooten
Solutions Engineer, IloT

Agenda

1. Market trends
2. Securing your OT network
3. Move to Artificial Intelligence
4. Reliable connectivity for automation
5. Bring IT skill to OT

Non-climate-controlled spaces require an environmentally hardened network



Extend connectivity beyond the building with networking equipment made to last

Industries are accelerating their operational transformation



Building future-ready operations for today's challenges and tomorrow's innovations

Common issues in industrial operations



Lack of OT visibility



Vulnerable assets



Lack of segmentation



Limited OT security skill sets



Securing vendor remote access



Ineffective workflow between OT and IT

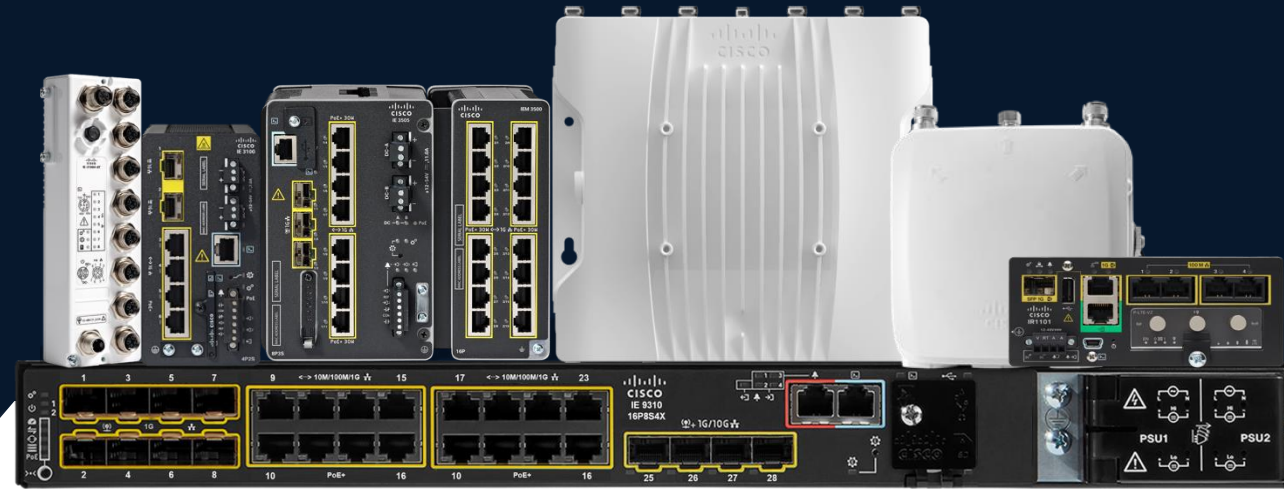


Supply chain and geopolitical risk



Operational Efficiency and MTTR

Cisco is bringing the best of IT to rugged networking



Enterprise IT Grade

Best of IT innovations



Industrial Strength

Purpose built for Operations



Embedded industrial cybersecurity and zero-trust policy enforcement

IE switching is OT environment friendly

Ease of Use



Device Manager / Web UI



Management integration



Dying Gasp



SD Swap Drive



Layer 2 NAT

Industry Protocols



Industry Certifications



Manufacturing

- ✓ EN/IEC 61000-6-2
- ✓ EN/IEC 61000-6-4
- ✓ EN/IEC 61326
- ✓ EN 300-328



Mining

- ✓ EN/IEC 61000-6-2
- ✓ EN/IEC 61000-6-4
- ✓ EN/IEC 61326
- ✓ EN 300-328



Energy-Utility

- ✓ EN 61850-3
- ✓ IEC 61850-3
- ✓ KEMA
- ✓ EN 300-328



Oil and Gas

- ✓ EN/IEC 61000-6-2
- ✓ EN/IEC 61000-6-4
- ✓ EN/IEC 61326
- ✓ EN 300-328



Transportation

- ✓ EN 50155
- ✓ EN 50125-1
- ✓ EN 50121-3-2
- ✓ EN 61373 -61375



City

- ✓ NEMA TS-2
- ✓ EN 300-328

Cisco's solution for industrial digital resilience



Securing your OT network



Move to Artificial Intelligence



Reliable connectivity for automation



Bring IT skill to OT

Cisco's solution for industrial digital resilience

Addresses your top 4 priorities



Securing your OT
network



Move to Artificial
Intelligence



Reliable connectivity
for automation



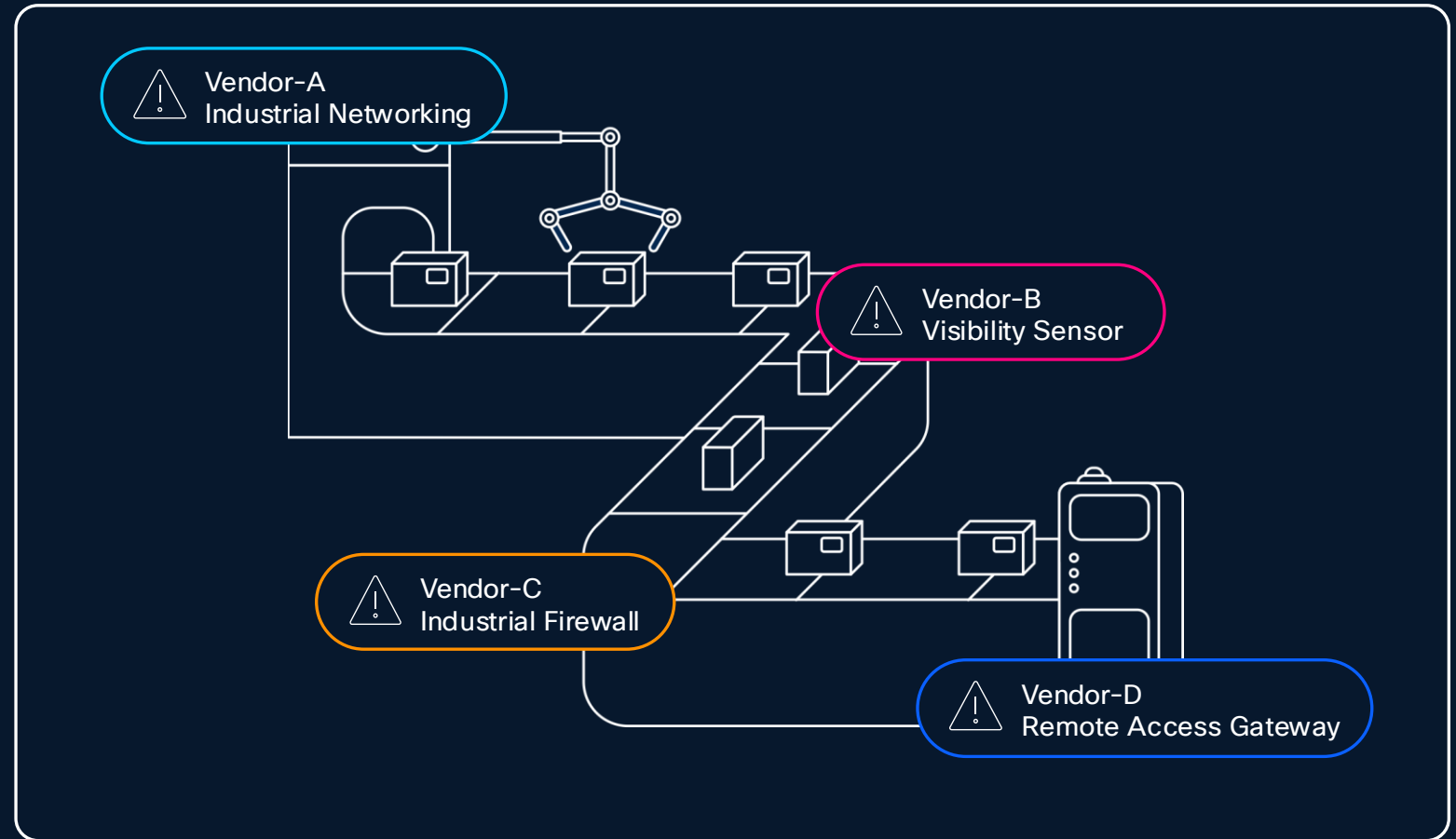
Bring IT
skill to OT

Why is it challenging to secure OT?

⚠️ Hard to scale

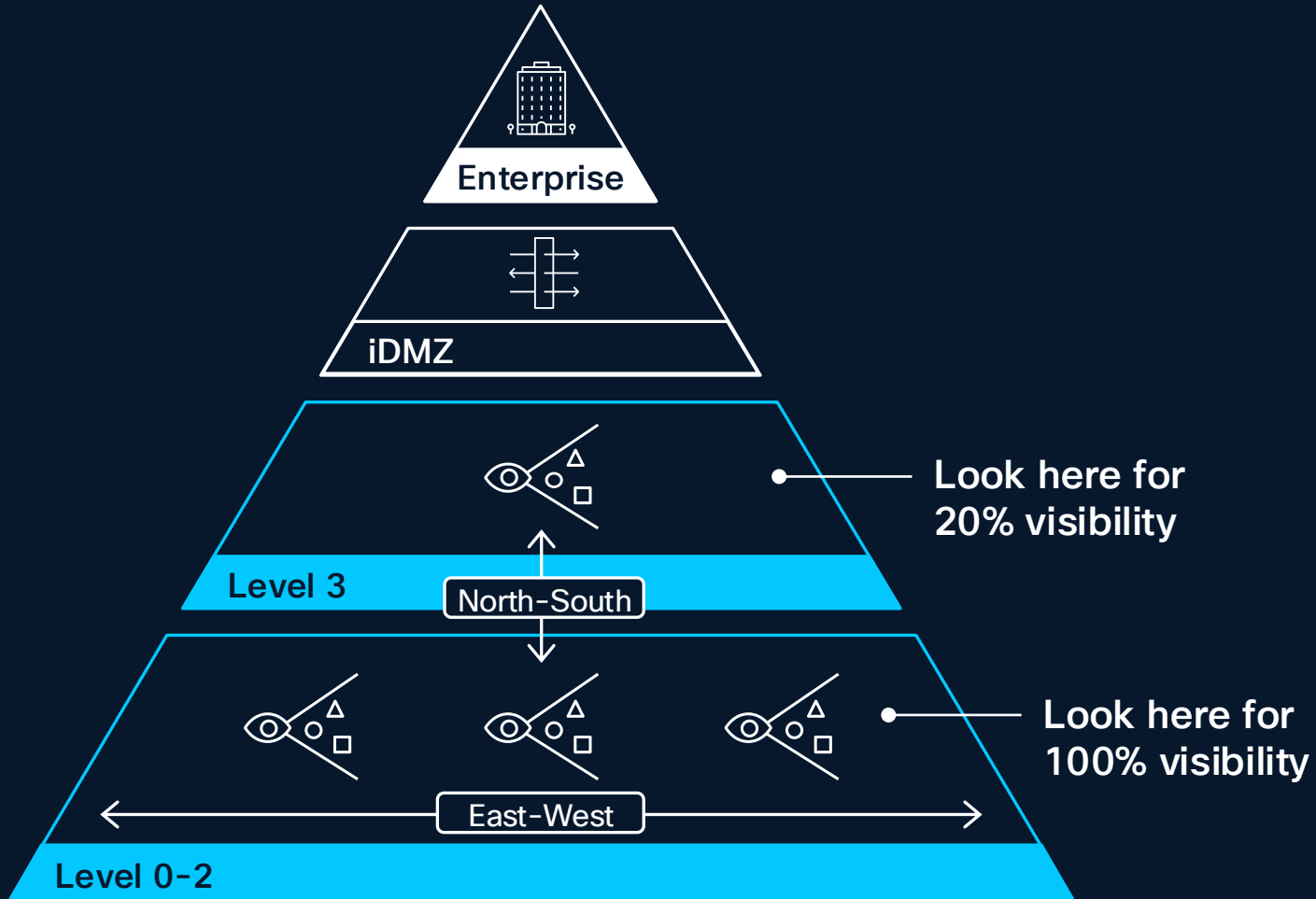
⚠️ Complexity

⚠️ Shadow IT



Industrial cybersecurity is fragmented by a patchwork of bolt-on solutions from different vendors

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

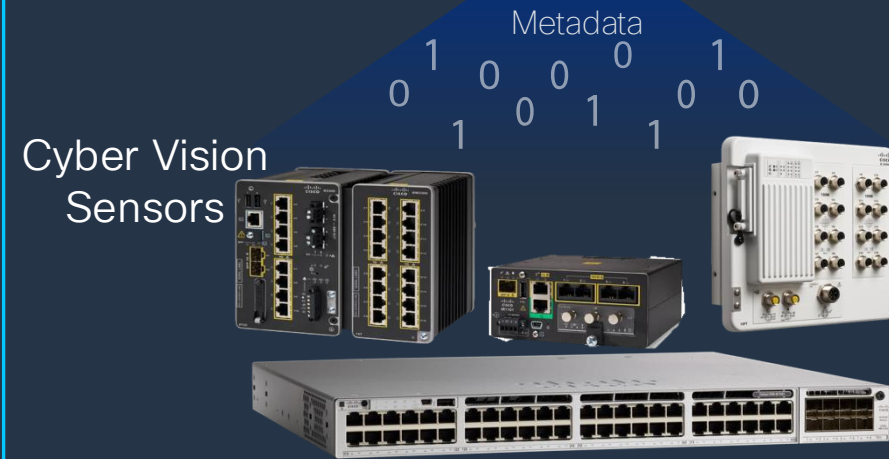
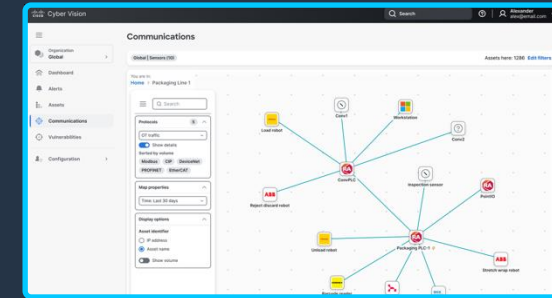
You run the risk of downtime if you try to segment Level 0-2 without 100% visibility

Cyber Vision helps gain comprehensive visibility at scale

OT visibility built in, not bolted on

- ✓ Visibility sensor is a software feature running in switches and routers
- ✓ No additional appliances needed
- ✓ No out-of-band collection network needed
- ✓ Active discovery requests see past NAT and firewall boundaries

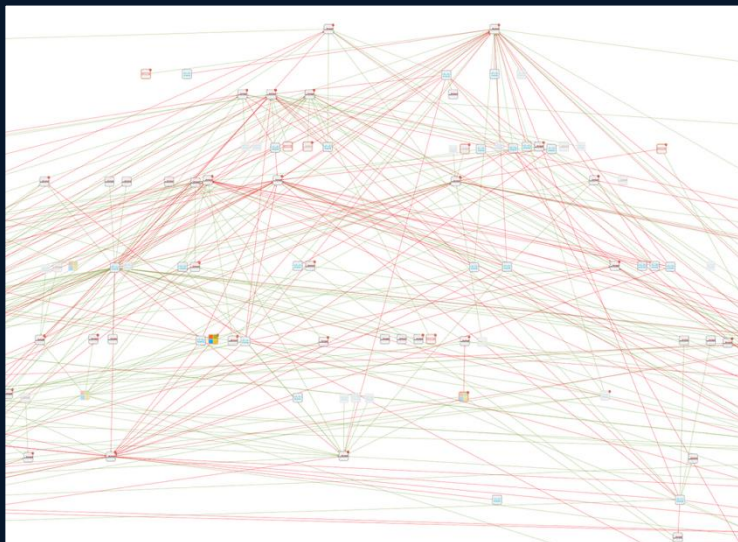
Cyber Vision Center



Deep Packet Inspection & Active Discovery
built into your network infrastructure

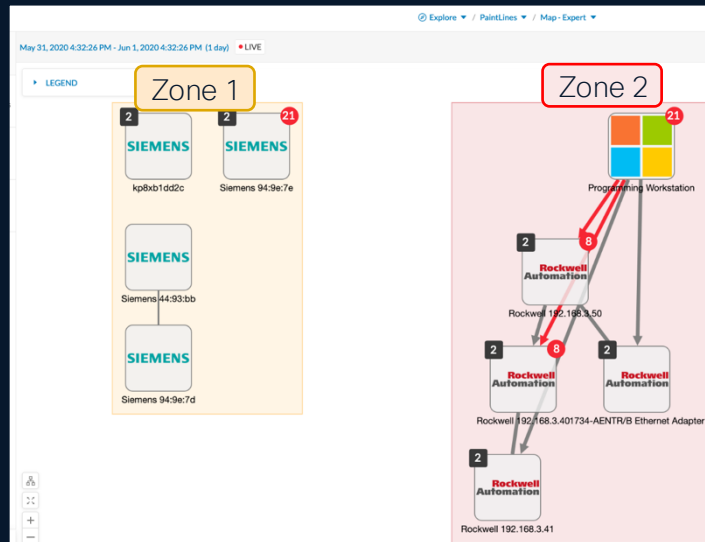
Leverage visibility to drive segmentation

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



Adaptive macro/micro segmentation enforced by IT, controlled by OT

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

Introducing Cisco Cyber Vision Site Manager

- Easily monitor the health of your entire OT security infrastructure from a central console
- No more siloes – ensure all sites have the latest threat detection intelligence
- Augment Cyber Vision’s alerting engine with real-time IP geolocation information

Give security teams time back
to effectively manage cyber risks

The screenshot displays the Cisco Cyber Vision Site Manager dashboard. At the top, the Cisco logo and the product name "Cyber Vision Site Manager" are visible. The dashboard features a "Dashboard" header and a navigation menu on the left. Below the header, there are four summary cards: "3 Total", "1 Unreachable" (with a warning icon), "0 Out of date", and "0 Non-compliant licensing". The main content area shows a map view of North Carolina, with a pop-up window for "Center52" at IP address "172.26.136.52". The pop-up indicates that the site has a "Connection", "License", "Version", and "Health" status, all of which are shown as green checkmarks. The map includes various cities and highways, and a Google logo is visible in the bottom left corner.

“Secure” remote access typically means user frustration with cumbersome experiences



“I need to give an OEM remote access to a machine for maintenance”



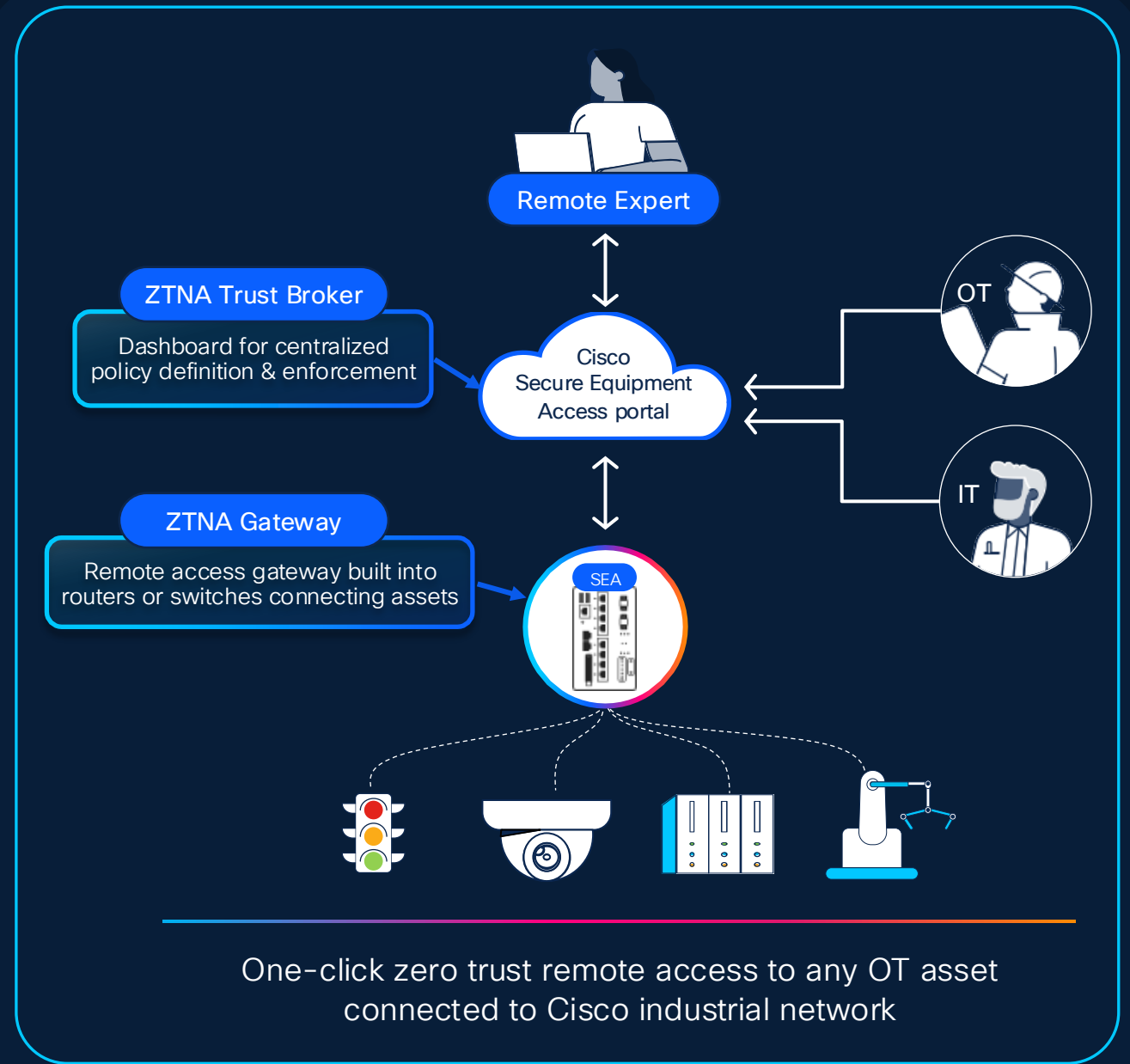
sigh...“Ok.”

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

How long does it take you to grant remote access?

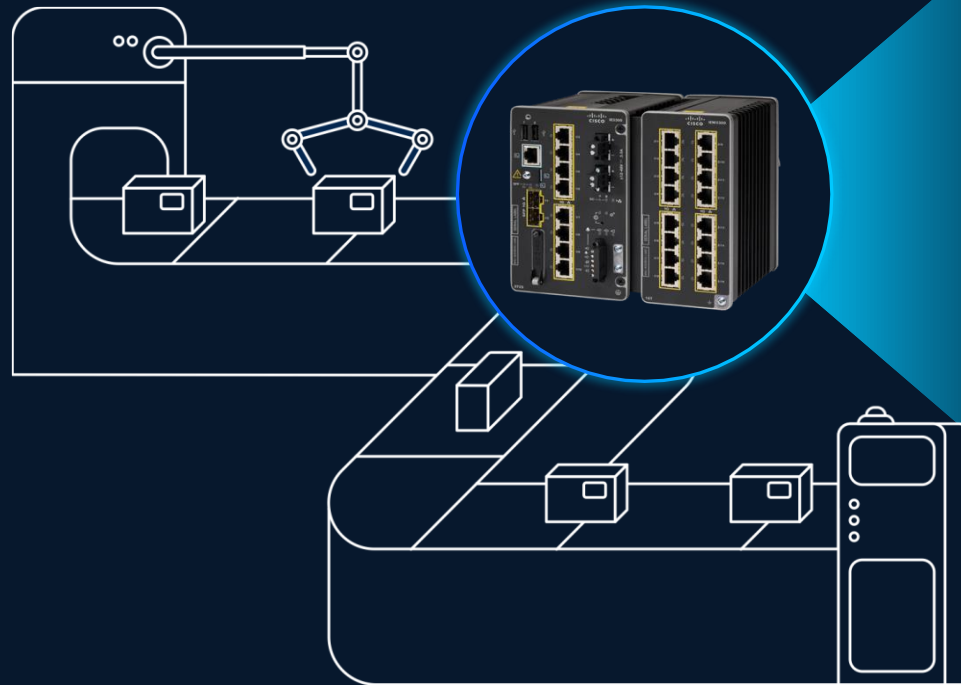
Cisco Secure Equipment Access

OT self-service remote access with zero-trust control



Cisco Industrial Security

Security fused into the network to protect OT at scale



OT Visibility
embedded in
network equipment



Segmentation
enforced by
network equipment



Secure Remote Access
embedded in
network equipment

Dynamic segmentation of 10,000+ assets

Challenges

- Massive automotive network that has grown organically over time without separation
- Board level directive to implement segmentation to reduce “blast radius” in case of cyber attack
- Segmentation must be enforced within short planned downtime without disrupting production

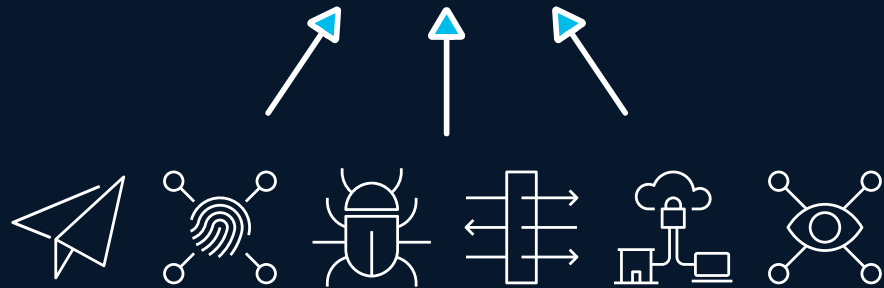
Solutions

- Cyber Vision on Industrial Ethernet footprint in levels 0-2
- Ensure no inter-zone communications were blocked before enforcing policy
- Cyber Vision + ISE to dynamically enforce segmentation policy on industrial switches



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

splunk>



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's solution for industrial digital resilience

Addresses your top 4 priorities



Securing your OT
network



Move to Artificial
Intelligence

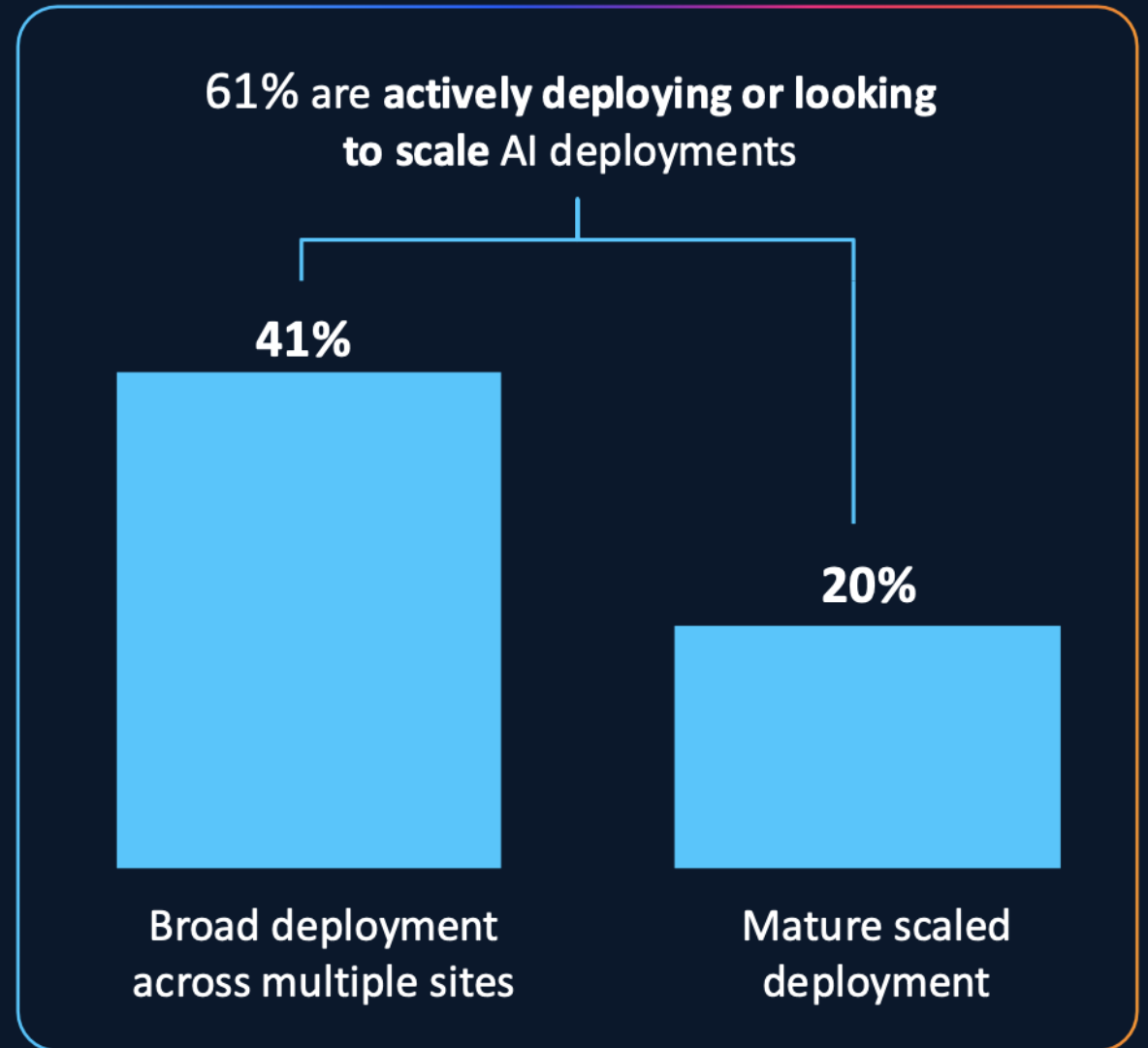
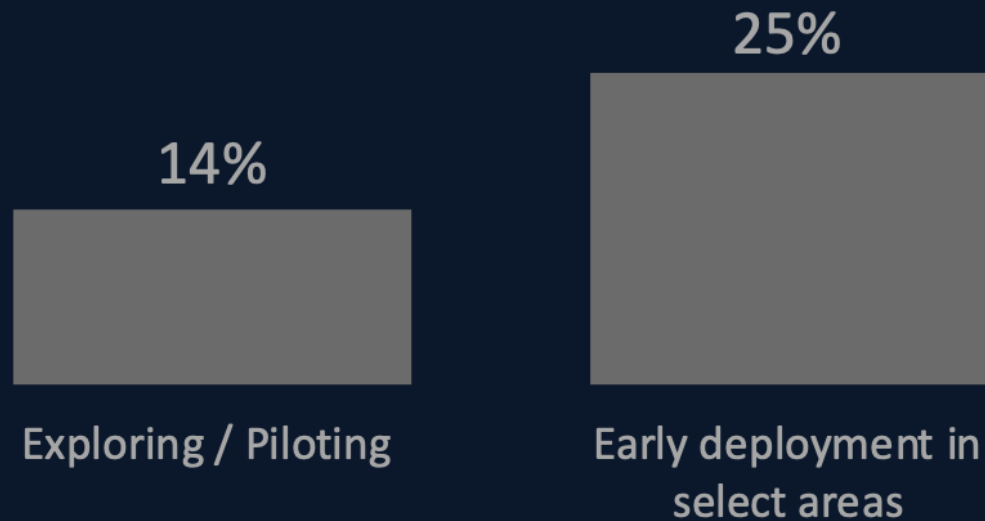


Reliable connectivity
for automation

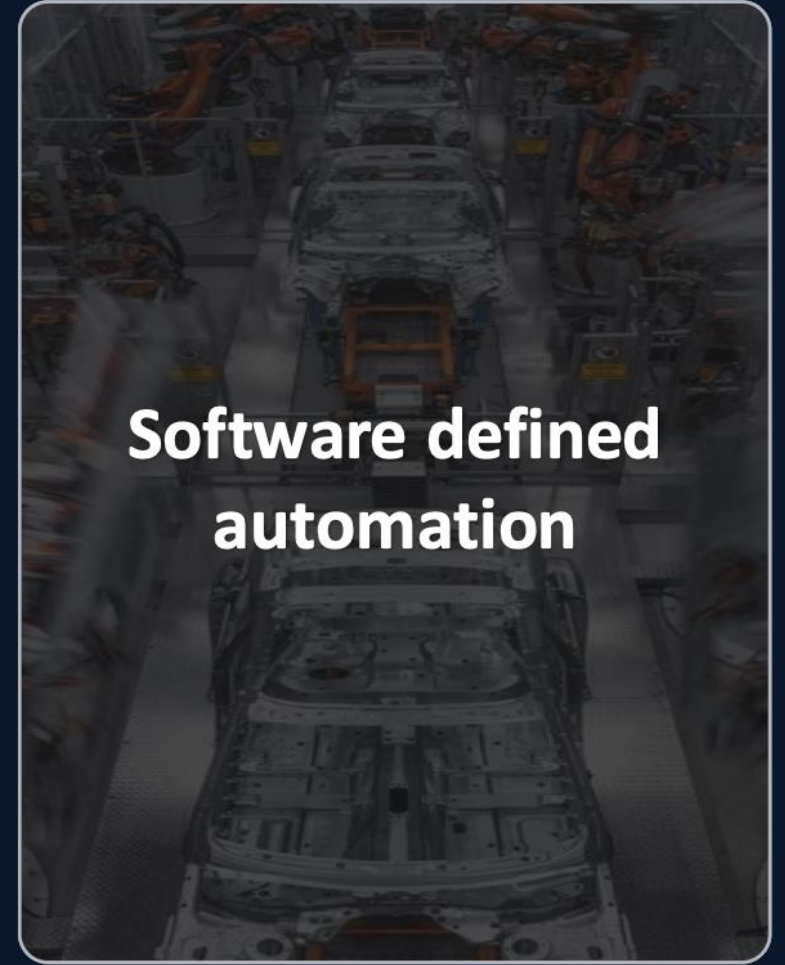
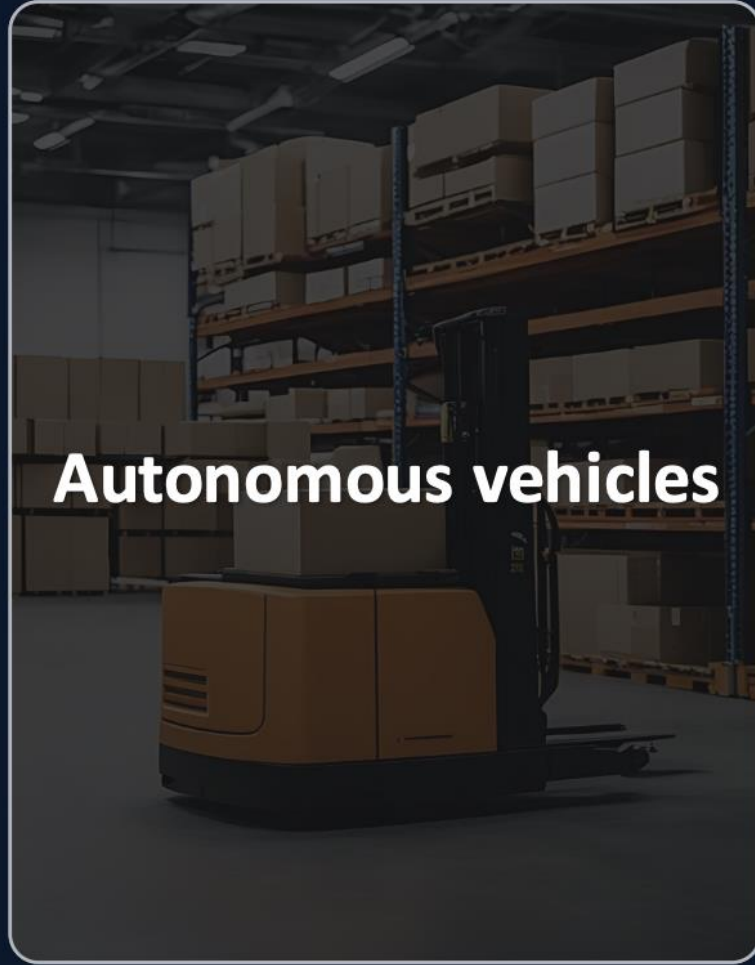


Bring IT
skill to OT

Industrial AI adoption is firmly underway

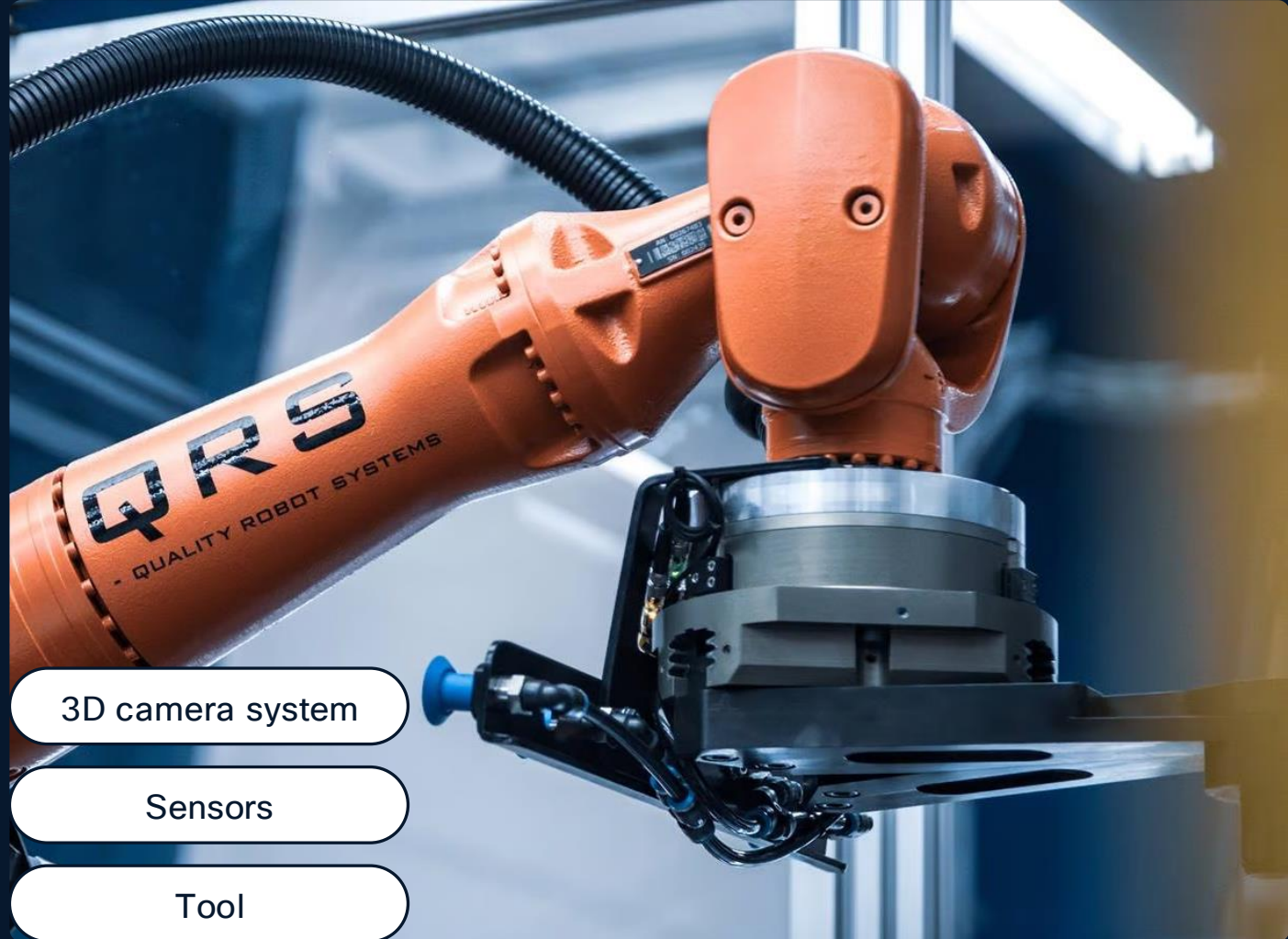


AI is revolutionizing manufacturing



The evolution to networked machine vision

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



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

Brains
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

Keeping industrial networks running

Increased pressure on OT personnel to ensure network availability



Available on site

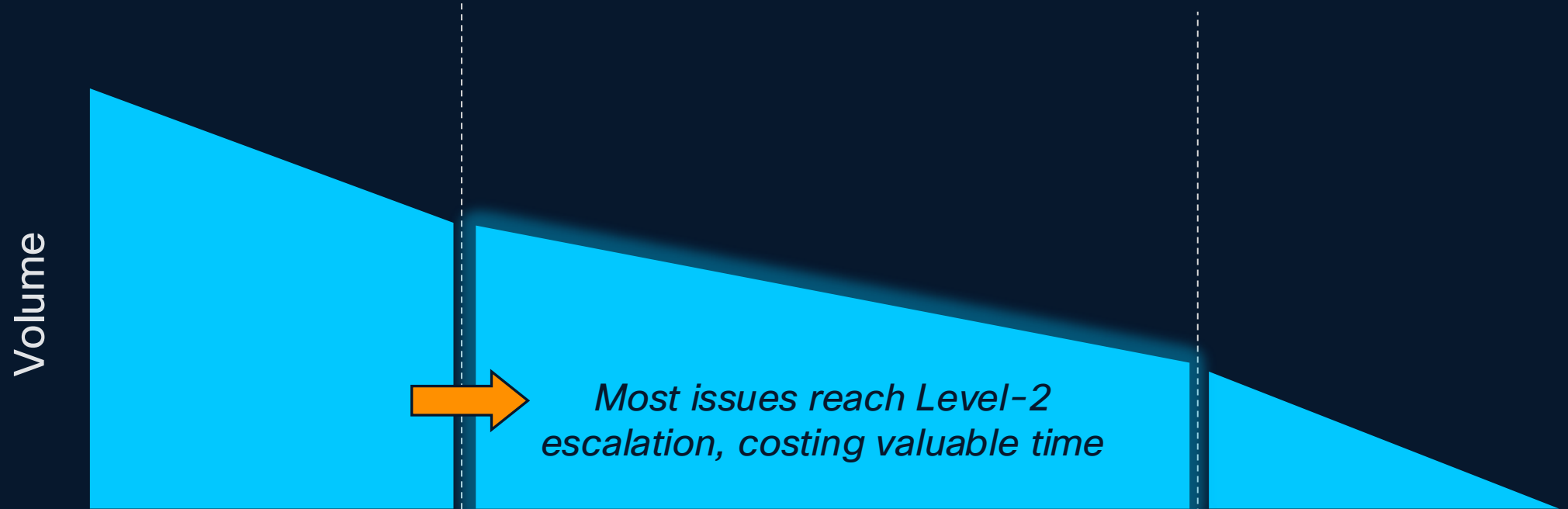
Low IT skills

Not available on site

High IT skills

First responders lack advanced troubleshooting skills

Today



Introducing AgenticOps for Industrial Networks

- An OT centric conversational interface for first responders to troubleshoot without escalation
- Proactively root cause issues in industrial networks to maximize availability
- Provides actionable guidance to enable OT teams to implement fixes quickly

**Empowering OT teams to
maximize network availability**

The screenshot displays the Cisco AI Troubleshooting for Industrial Networks interface. The top navigation bar includes the Cisco logo, the title "AI Troubleshooting for Industrial Networks", and the user profile "Elías Nordstrom Automotive". The main interface is divided into a left sidebar and a main content area. The sidebar contains "Threads", "Alerts", and "Settings" sections. The "Threads" section has a search bar, a "+ New thread" button, and a "Today" section with a "Network topology inquiry" thread. The main content area shows a conversation with the AI agent. The user's question is "What's our network topology like?". The AI agent's response is a network topology diagram titled "Topology". The diagram shows a central switch (LINE02-SW04) connected to several other switches: LINE01-SW01, LINE03-SW06, CELL01-SW03, CELL02-SW02, and CELL02-SW03. Additionally, there are two WELD02 switches (CELL02-WELD02) and a CONV01 switch (DRIV-CONV-01). Each switch is labeled with its name and IP address. Below the diagram is a text input field with the placeholder "Ask about your network or describe an issue" and a submit button. A small disclaimer at the bottom reads: "Agent can make mistakes. Verify responses. Learn how the Agent handles data in the AI disclosures."

Introducing AgenticOps for industrial networks

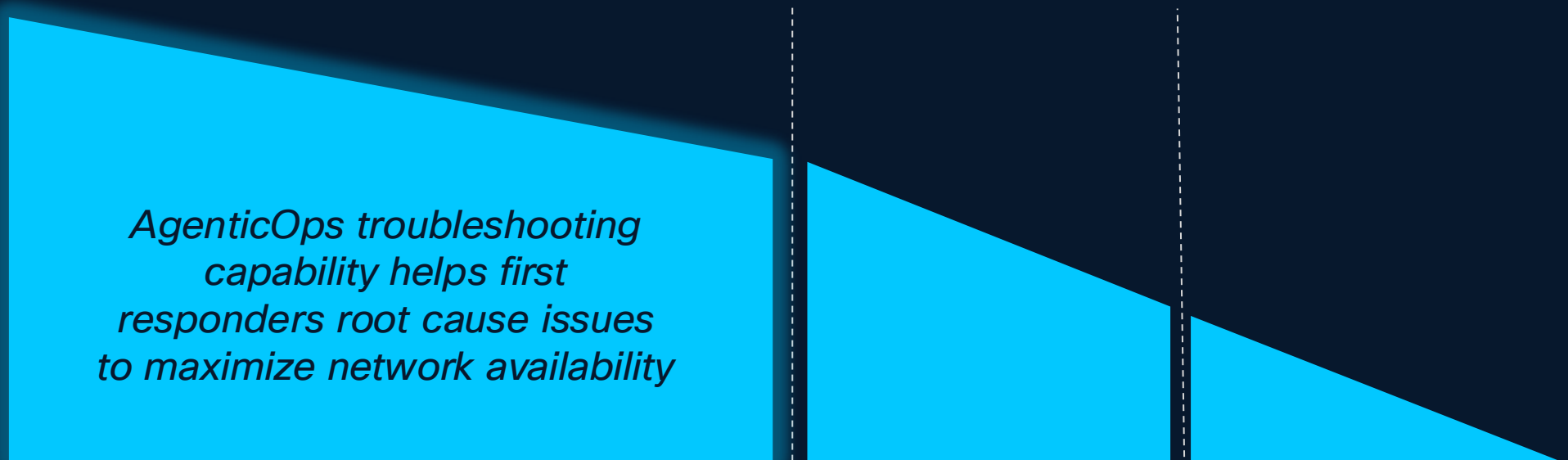
Today



With AgenticOps troubleshooting capability



Volume



Cisco's solution for industrial digital resilience

Addresses your top 4 priorities



Securing your OT
network



Move to Artificial
Intelligence



Reliable connectivity
for automation



Bring IT
skill to OT

Customers need wireless that can do more



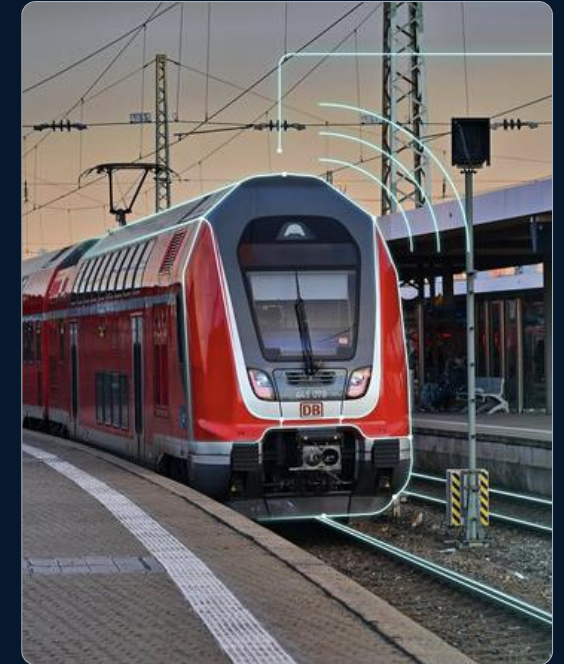
Automated guided vehicles (AGV) and Autonomous mobile robots (AMR) in plants



Wireless backhaul where fiber or cellular are unavailable or too expensive



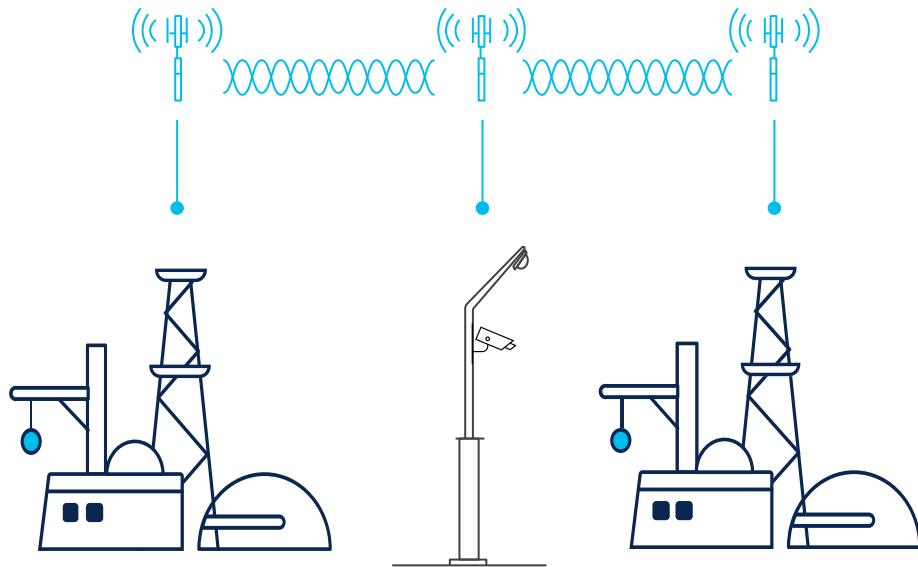
Tele-remote operations in mines and ports



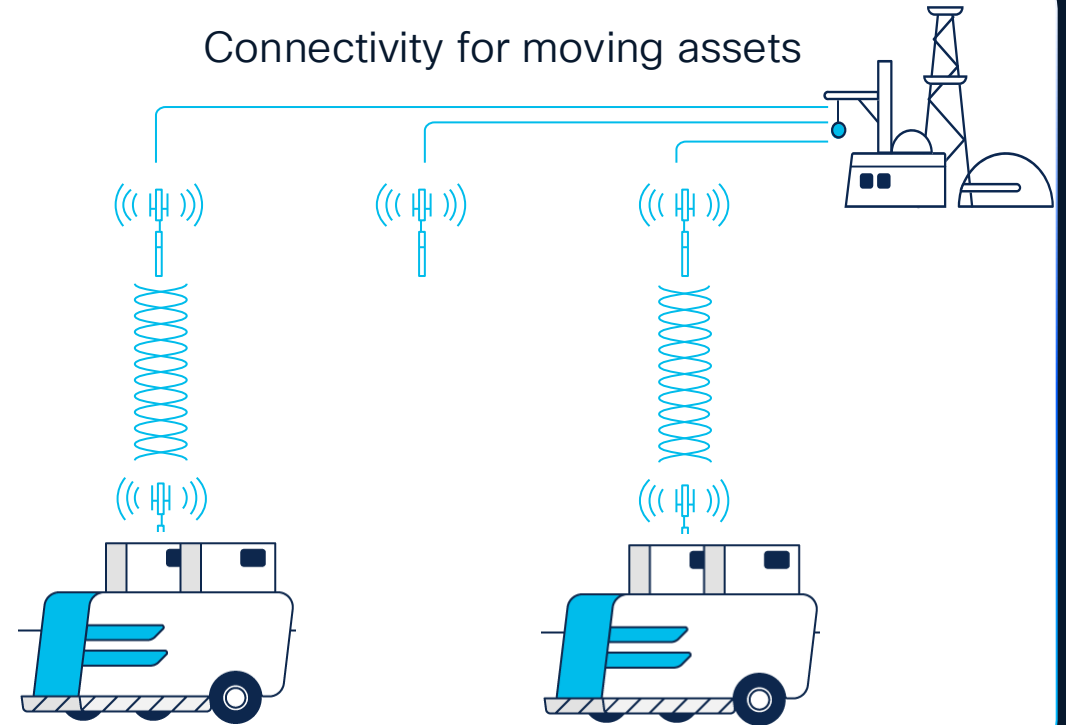
Communications-based train control (CBTC) in rail

URWB: Reliable fiber-like wireless connectivity, anywhere

Connectivity where fiber isn't available or is too costly



Connectivity for moving assets



End-to End Overlay



Make-before-break handoff



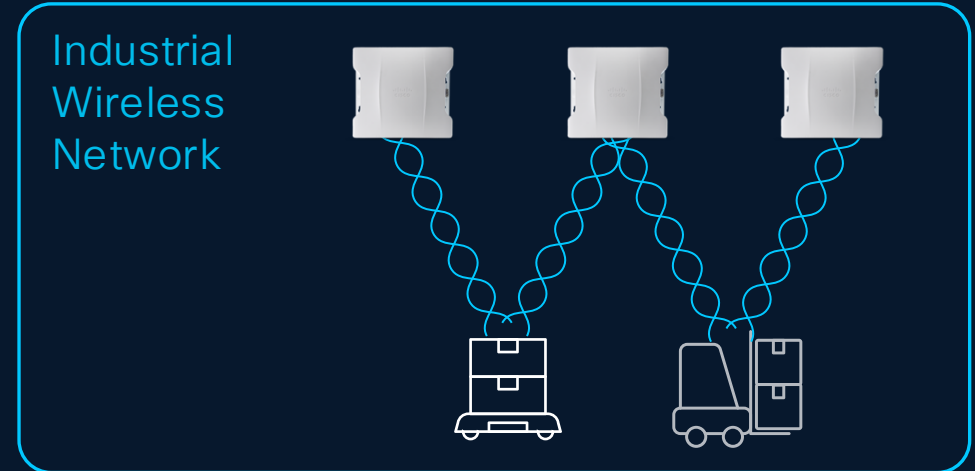
Multipath operation



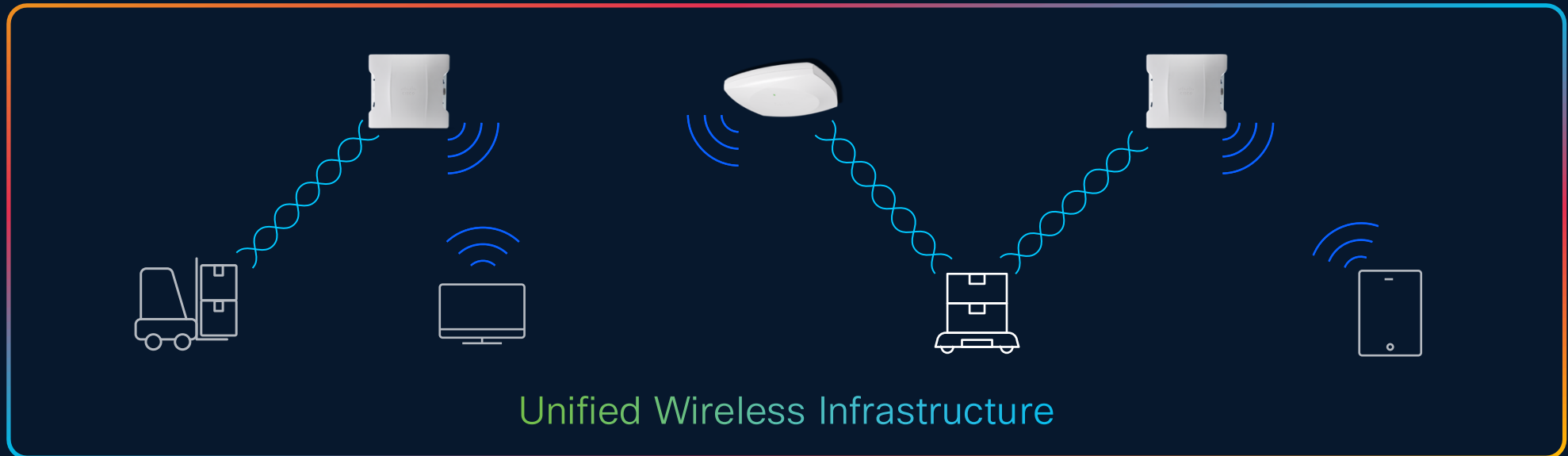
Ultra-fast failover
Carrier-grade availability

Introducing Wi-Fi and URWB unified infrastructure

Before



Now



Cisco's solution for industrial digital resilience

Addresses your top 4 priorities



Securing your OT
network



Move to Artificial
Intelligence



Reliable connectivity
for automation



Bring IT
skill to OT

Enterprises are connecting “things” in uncarpeted spaces



Security cameras



Outdoor Wi-Fi



Mobile assets



Gate access control



ATMs



Wireless backhaul for non-wired locations



Private mobile wireless on campus



Building management systems



Outdoor digital signage



Emergency call buttons

These non-climate-controlled spaces require an environmentally hardened network

Introducing Cloud management for Cisco rugged switches

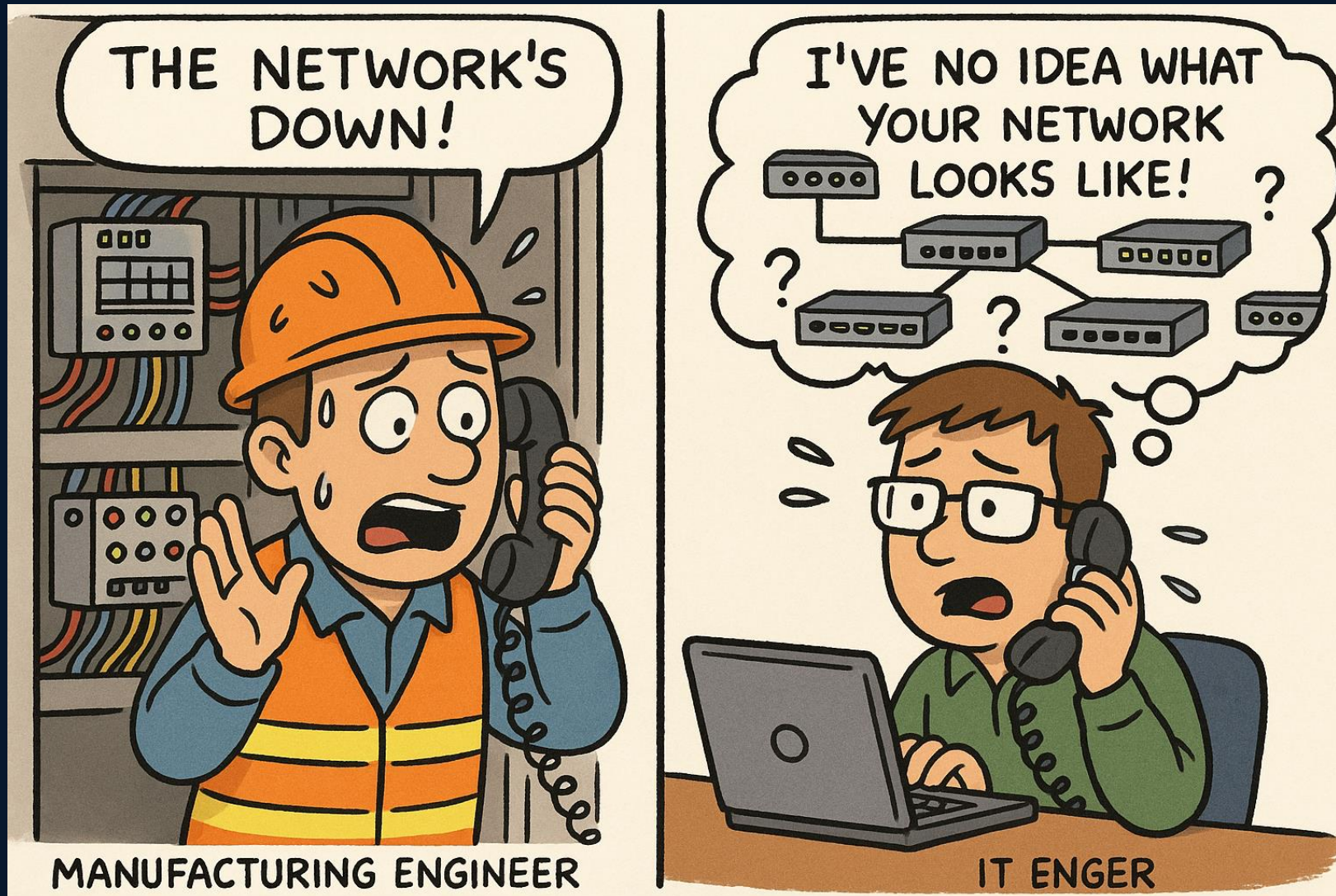
- A single dashboard to manage enterprise and rugged switches
- Easily extend enterprise networks to outdoor and uncarpeted spaces
- Allow IT teams to enforce consistent security policies and maintain control

Seamlessly manage enterprise and rugged networks from a single cloud dashboard

The screenshot displays the Meraki cloud management interface for a specific device, 'Parking Lot IE-3500-8U3X'. The interface is organized into several sections:

- Navigation:** A left sidebar contains menu items for Network IIOT, Network-wide, Assurance, Switching (highlighted), Cameras, and Organization. A search bar is located at the top right.
- Device Overview:** The main header shows the device name 'Parking Lot IE-3500-8U3X' with an 'Online' status and 'Configuration source: Cloud'. Below this is a map showing the device's location in Mandalay Bay, Las Vegas, with nearby landmarks like Ruby Blue, Lux Vegas, and W Las Vegas.
- Summary and Port Status:** A 'Summary' tab is active, showing a grid of port status indicators. Ports 1/4 through 1/11 are listed, with some showing green status and others grey. A 'Port key' dropdown is visible below the grid.
- Historical Device Data:** A section titled 'Historical device data' (Last 2 hours) contains two charts:
 - Connectivity:** A horizontal bar chart showing a continuous green line, indicating stable connectivity over the period from 16:50 to 18:13.
 - Usage:** A line chart showing network usage in Kb/s over time. The usage fluctuates between approximately 0.5 and 1.5 Kb/s from 16:45 to 18:15.
- Device Details:** A vertical list of device attributes is shown on the left side of the main content area, including:
 - Device uptime: 12d 4h 54m
 - Last device boot: Aug 6 13:52:49 (PDT)
 - Configuration: Up to date (last fetched 39 minutes ago)
 - Firmware: Not running configured version
 - LAN IPv4: 192.168.1.146
 - Type: Via DHCP
 - Interface: Vlan 1
 - Public IP: 67.188.193.285
 - Gateway: 192.168.1.1
 - DNS: 192.168.1.1

How IT & OT Have Worked Together Historically



This is your therapist saying... **It can get better**



Catalyst Center

Leverage your IT investments to gain efficiencies in OT

Catalyst Center

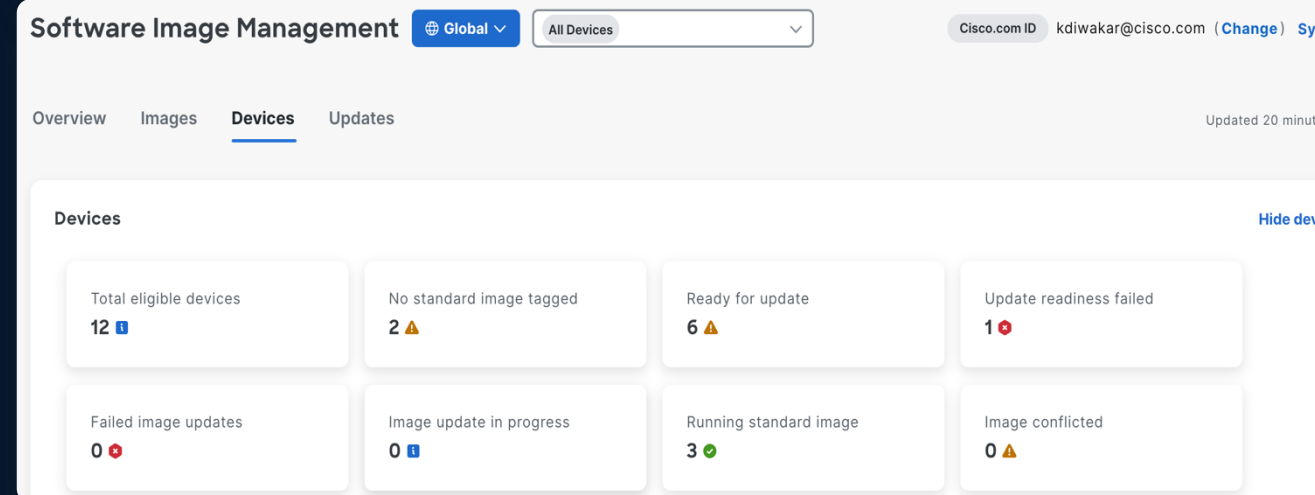
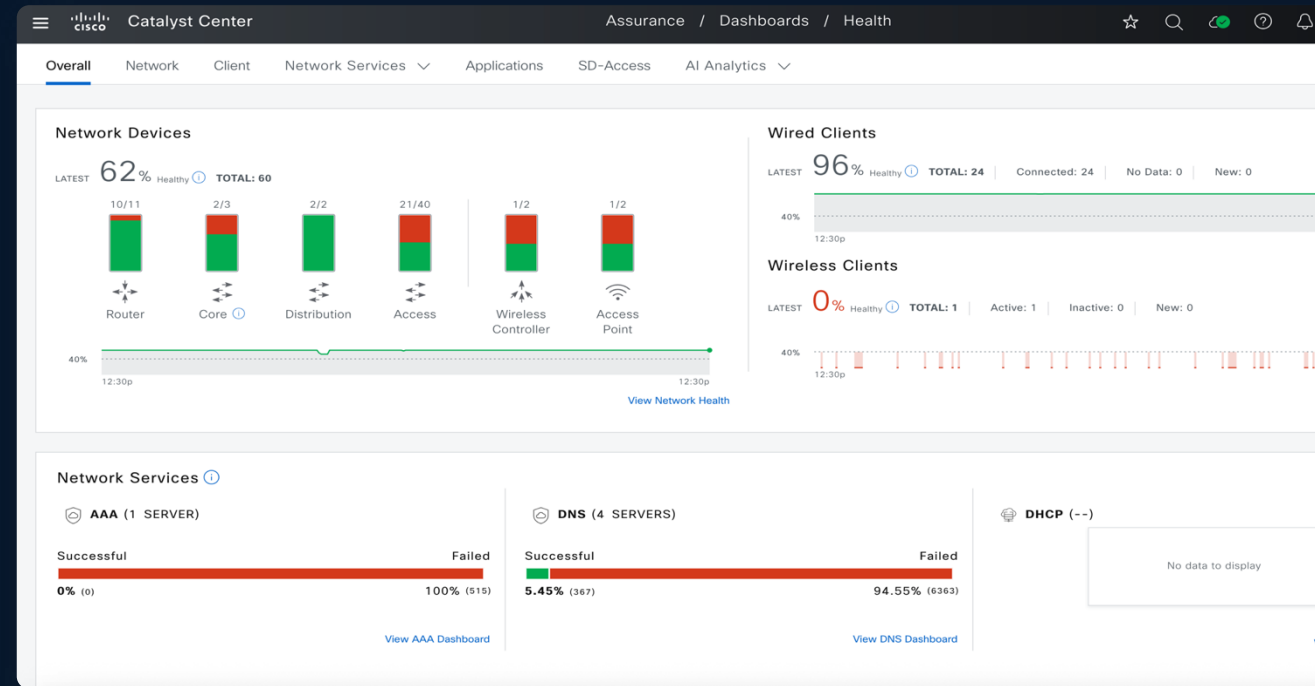
Network Snapshot

As of Jun 1, 2025 12:56 AM

- Sites**: 51
DNS Servers : 1
NTP Servers : 1
[Add Sites](#)
- Network Devices**: 61
Unclaimed: 3
Unprovisioned: 8
Unreachable: 22
[Find New Devices](#)
- Network Profiles**: 7
Switching: 5
Wireless: 2
Routing: 0
Assurance: 0
WAN: 0
[Manage Profiles](#)
- AI Endpoint Analytics**: 48 Total Endpoints
Fully Profiled Endpoints: 15%
Partially Profiled Endpoints: 83%
Unprofiled Endpoints: 2%
Trust Score Alerts: 0
AI Proposed Rules: 0
[View Details](#)
- Software Images**:
Success: 14
Progress: 0
Failure: 17
[Manage Images](#)
- Cisco Licensed Devices**: 12
Switches: 10
Routers: 0
Wireless: 2
[Manage Licenses](#)
- Images**: 1
As of Jun 1, 2025
- EoX Status**: 7
Last Scan: May 2025

What can Catalyst Center do for OT networks?

- Manage networks with automation and assurance
- Secure operations by applying consistent policies and SW versions
- Reduce downtime with AI-driven problem identification and resolutions



Lean-IT collaborating with OT

Challenges

- 15+ Production sites and rapidly expanding
- Lean IT team supports OT network in growing breakthrough drug production
- Highly reliable OT network needed for precision drug manufacturing

Solutions

- **IE3300** access switch with IOS-XE to leverage existing IT knowledge and investments
- **Catalyst Center** for Zero Touch Provisioning to reduce deployment time from days to hours
- Catalyst Center configuration, software updates, and PSIRT monitoring for compliance

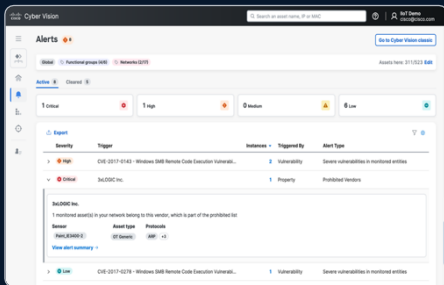


✓ Catalyst IE3300

✓ Catalyst Center

Cisco's solution for industrial digital resilience

Addresses your top 4 priorities



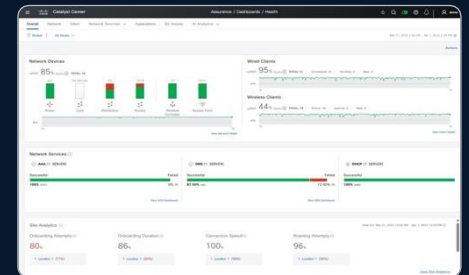
Cyber Vision and SEA



Comprehensive Hardware Portfolio



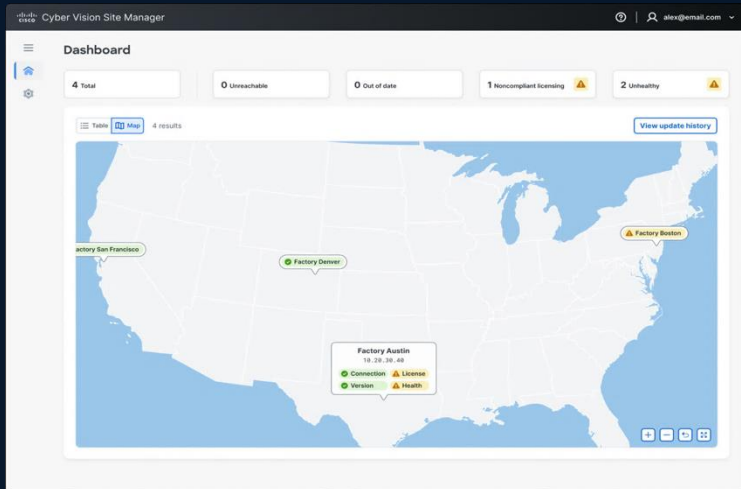
Cisco Wireless with URWB



Catalyst Center and Cloud Management

New Innovations to Drive Operational Simplicity in OT

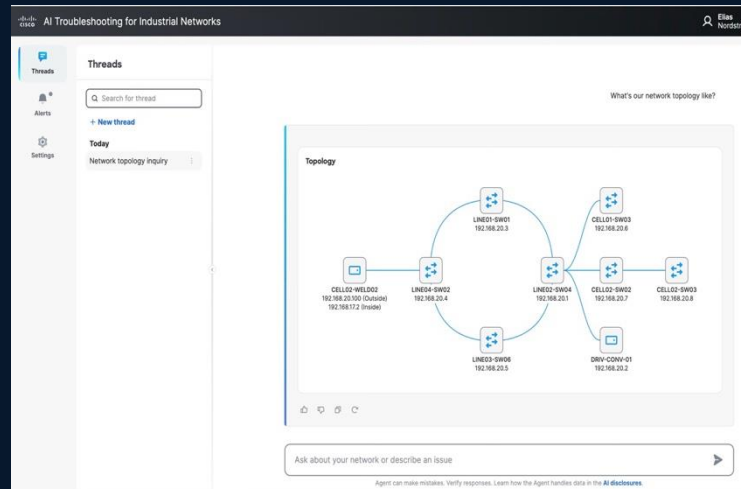
NEW!



Multi-site OT Threat Intelligence Distribution

Simplifying OT threat intel deployment and security infrastructure management

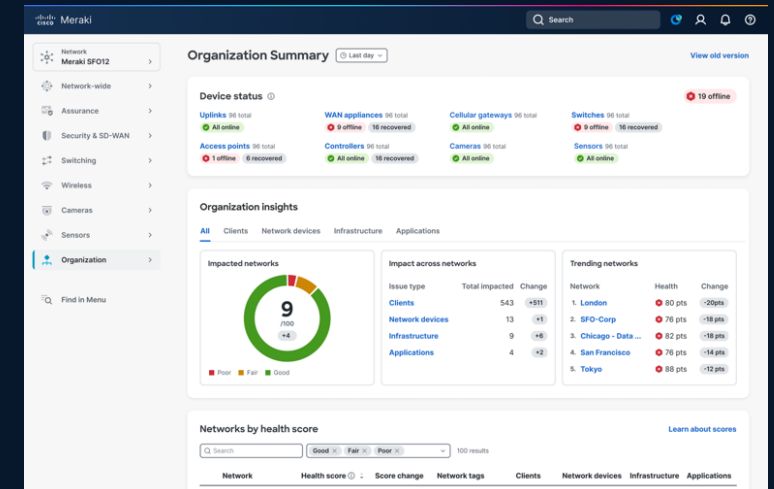
NEW!



AgenticOps for Industrial Networks

Simplifying troubleshooting for OT teams to maximize network availability

NEW!



Cloud Management for Rugged Networks

Simplifying management across IT and rugged networks with the Meraki dashboard

Cisco validated design for Industrial Systems

Technical blueprints and architectures, tested, and proven - enabling seamless standardization



Faster deployments



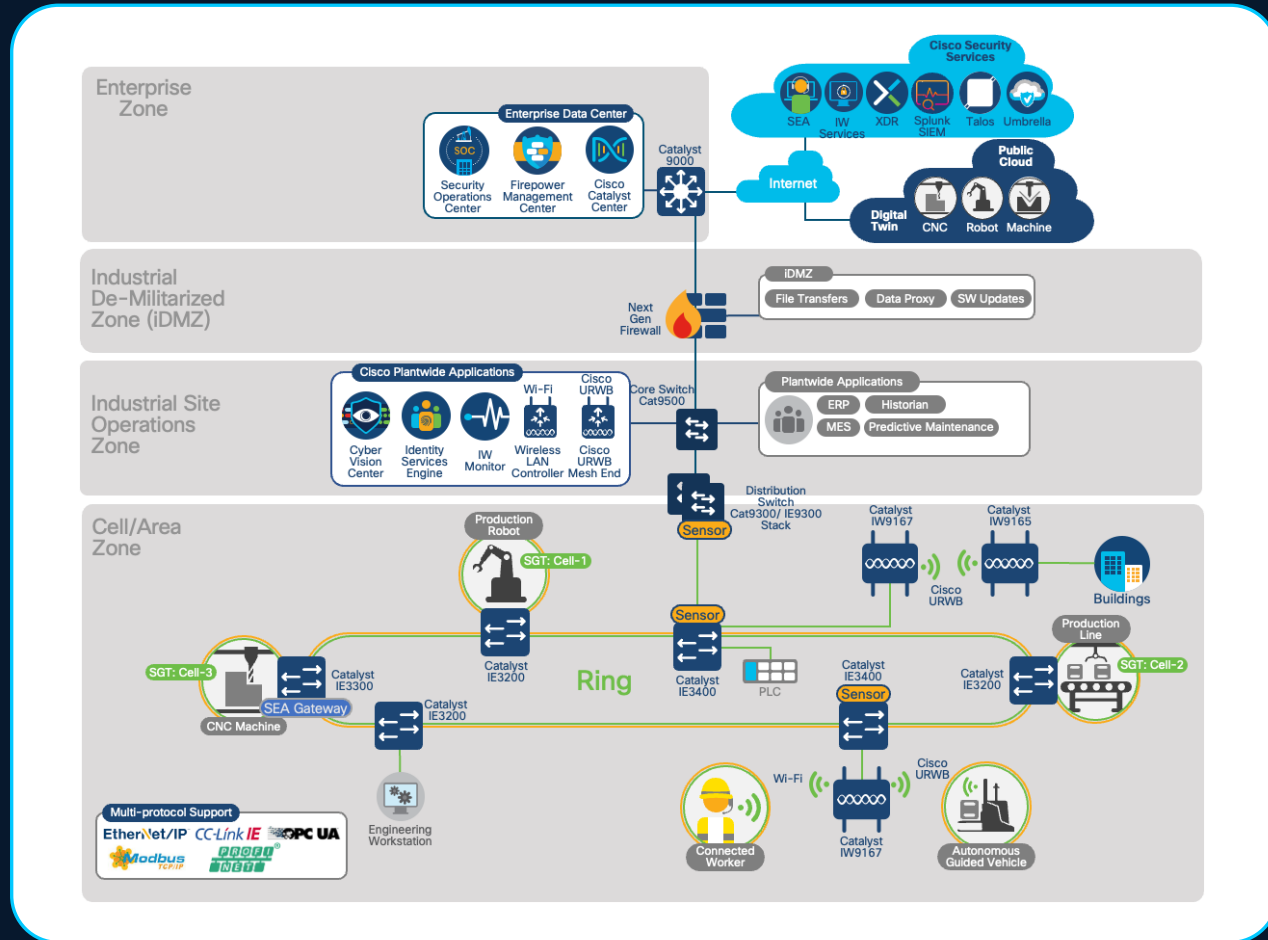
Less Risk



Increased predictability



End-to-end designs



Proven to work with:



Introducing New Validated Designs for Manufacturing

- Seamless standardization
- Faster deployments
- Less risk
- Increased predictability
- End-to-end designs



Three vertical cards are displayed within a blue-bordered container. The first card, "AI MACHINE VISION", features a central icon of a person with a magnifying glass and a gear, surrounded by document and camera icons. Below it, the text reads "BUILDING THE INDUSTRIAL NETWORK THAT MAKES IT HAPPEN". The second card, "INDUSTRIAL CONTROL VIRTUALIZATION", features a central icon of a gear with a key, surrounded by icons for a PLC, HMI, and robot. Below it, the text reads "DUAL FABRIC PLATFORM FOR VIRTUAL PLC, HMI, AND ROBOT CONTROL". The third card, "INDUSTRIAL NETWORK MANAGEMENT", features a central icon of a person with a gear, surrounded by icons for a document, folder, and hourglass. Below it, the text reads "DESIGN GUIDANCE TO EXTEND CATALYST CENTER TO THE OT SPACE WITH RBAC".

www.cisco.com/go/iotcvd

Simplifying OT networks with proven technical blueprints and architectures

Leverage the best of Cisco's decades of experience



**Industry-leading
networking**

Industrial IoT Portfolio

- Comprehensive wired wireless and security portfolio
- Ruggedized and purpose built for OT industrial use cases



**Cybersecurity and
incident response**

Cisco Industrial Threat Defense

- OT visibility embedded in the network
- Zero Trust Network Access for OT
- Segmentation



**Best practices to
design and deploy**

Cisco Validated Designs

- Faster deployments
- Decreased risk
- End-to-end designs

Learn more

The screenshot shows the Cisco Industrial IoT solutions landing page. The header includes the Cisco logo, navigation links for Products and Services, Solutions, Support, Learn, Why Cisco, and Partners, and a search bar for trials and demos. The main content area features a large image of a worker in a hard hat and safety vest using a tablet in an industrial setting. The headline reads "Build resilient industrial networks today to innovate tomorrow". Below this, a sub-headline states "Cisco Industrial IoT solutions". A paragraph describes the comprehensive range of high-performance, rugged networking solutions for industrial AI. The page is divided into sections: "Overview" and "Resources". The "Overview" section includes a video player titled "Future-proofing industrial networking for cybersecurity and AI" with a 01:25 duration. Below the video are four key benefits: "Industry-leading solutions to simplify and scale IT for industrial networks", "Rely on tougher, smarter networking solutions that bring IT and OT together, enhance efficiencies, secure operations, and pave the way for industrial AI.", "Get networking designed for OT" (Enjoy the power of a comprehensive portfolio that's built for operational technology (OT), supports industrial control protocols, withstands tough environmental conditions, and lets you choose from fiber, cellular, and wireless connectivity options.), "Protect operations against cyberthreats" (Secure your industrial network at scale and maintain production uptime with networking equipment that provides visibility into connected assets, enables zero-trust remote access, and enforces segmentation policies.), "Build future-proof networks" (Get ready for software-defined industrial automation and industrial AI), and "Automate tasks and improve network reliability" (Achieve agile and scalable...).

[Cisco IoT: cs.co/iot](https://cs.co/iot)

The screenshot shows the Cisco Industrial Threat Defense landing page. The header includes the Cisco logo, navigation links for Products and Services, Solutions, Support, Learn, Why Cisco, and a search bar for trials and demos. The main content area features a large image of a worker in a hard hat and safety vest using a laptop in an industrial setting. The headline reads "Tough security for tough environments". Below this, a sub-headline states "Cisco Industrial Threat Defense". A paragraph describes the comprehensive cybersecurity solution that's built into the industrial network and unifies IT and OT security. The page is divided into sections: "Overview" and "Resources". The "Overview" section includes a video player titled "Industrial Threat Defense OT cybersecurity solution" with a 01:13 duration. Below the video are four key benefits: "Security for critical infrastructures and industrial operations", "From OT visibility to adaptive segmentation to zero-trust remote access, get a comprehensive platform that unifies IT and OT cybersecurity and makes it simple to protect operations at scale.", "Uncover your industrial cybersecurity posture" (Easily inventory your OT/ICS assets and their behaviors with a solution that uses your network as a sensor to provide full visibility at scale—and the insights you need to reduce the attack surface.), "Protect operations" (Enforce ISA/IEC 62443 zones and conduits and prevent threats from spreading with a solution that empowers OT teams to define segmentation policies and employs your network as the enforcer.), "Control and secure OT remote access" (With easy-to-use zero-trust remote access built into network equipment, your OT team can manage assets from anywhere and you gain control over risks from remote users.), and "Find and block threats across IT and OT" (With OT insights in your IT security tools, you can detect, investigate, and resolve threats across IT and OT—all from a single console).

[IoT CVD: cisco.com/go/iotcvd](https://cisco.com/go/iotcvd)

Thank you

