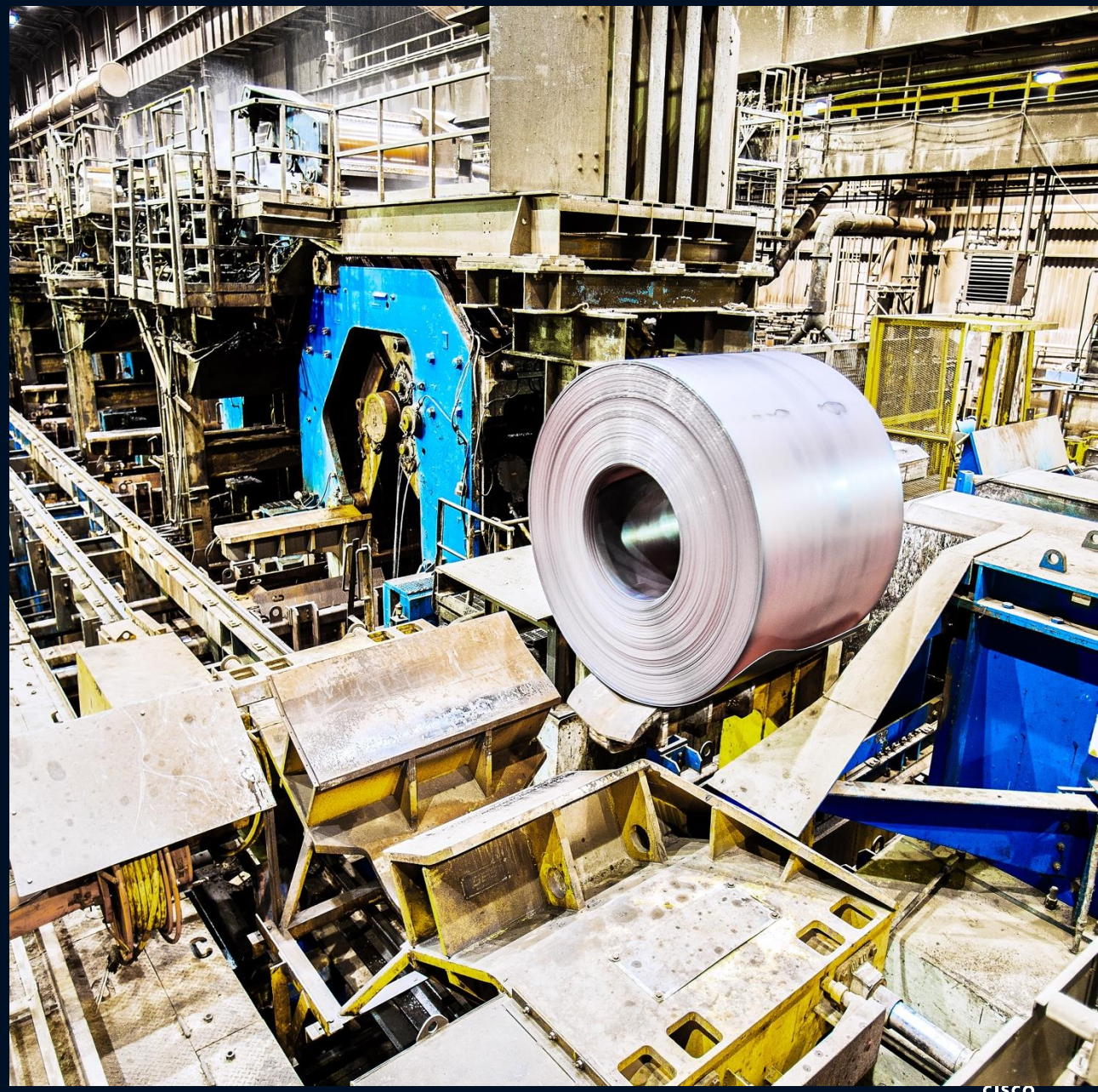
CISCO Engage | Tech Day

Modernizing Industrial networks for cybersecurity and AI

Andrew Usankin, Industrial IoT Solutions Engineer

October 9, 2025

Cisco has worked with over 52,000+ manufacturing customers and organizations, in 139 countries worldwide for more than 20 years



Cisco has been driving **industry digitization and innovation** for over 20 years

March 2003
First Cisco industrial switch

Today
Comprehensive range of advanced industrial networking solutions

Guiding OT migration to IP
Defining new industrial networking standards and reference architectures to help digitize industries

Championing OT specificities
Full support of OT protocols and architectures such as PROFINET, Ethernet/IP, HSR/PRP/DLR, and more

Enabling OT/IT partnership
Making IT innovations in management, security, and scalability seamlessly available to OT

Market-leading industrial networking, purpose-built to support today's operations

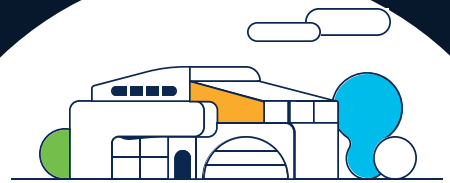
Networks are extending beyond carpeted spaces

Enterprise Operations

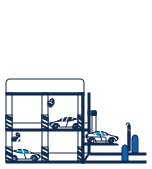
Extending the IT network beyond traditional climate-controlled spaces to non-carpeted areas.

Industrial Operations

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



Enterprise Solutions


Parking

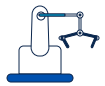

Roadways


Transportation


Renewables


EV chargers


Utilities


Manufacturing


Oil & Gas


Mining


Warehouses


Airports


Seaports

Connecting outdoor and industrial environments

cisco

Cisco’s solution is bringing the best of IT and OT together

Industrial Grade

Purpose built for operations

+

Enterprise IT Grade

Best of IT innovations

Catalyst Center

Catalyst SDWAN

Cisco IOS® XE

Enabling OT modernization has become an IT priority

Cisco is the Industrial Networking Market Leader

#1 Market Share
Global Industrial Edge

Industrial Switching

24% Layer 2 | 37% Layer 3

#1 Market Share

Industrial Routing

34%

#1 Market Share

Industrial Wireless

57%

#1 Market Share

Source: OMDIA, calendar year 2024

TrustRadius TOP RATED 2022

FORRESTER® WAVE LEADER 2024 Operational Technology Security Solutions

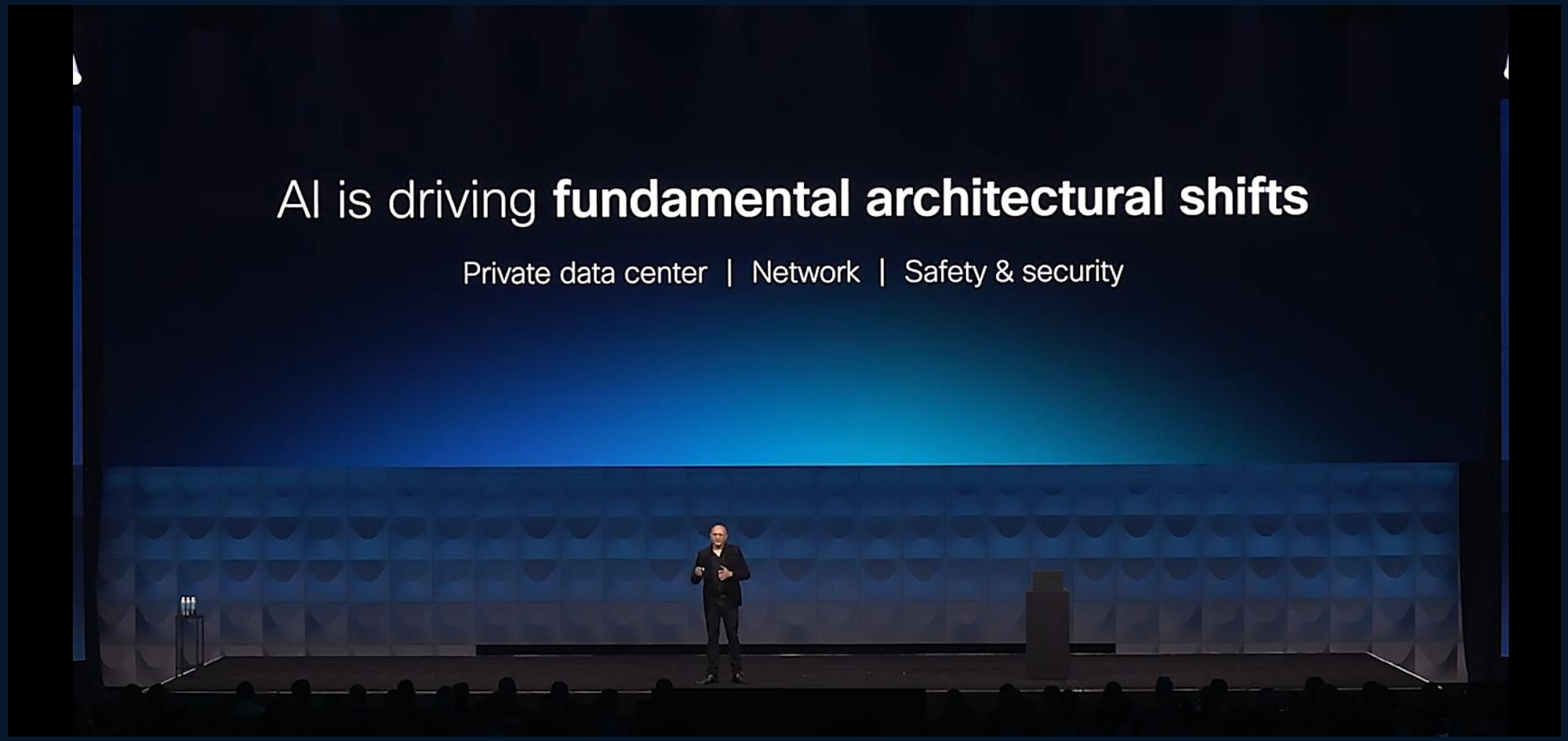
IoT BREAKTHROUGH AWARDS
Industrial IoT
Company of the Year 2025

Extending IT to operational environments

Campus & Branch

- Warehouses
- Distribution Center
- Parking Lots
- Airport
- Port
- Manufacturing
- Utility Substations
- Roadways
- Oil & Gas Refinery
- Mines

Consistent Network Architecture



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

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

OT modernization has become an IT priority

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

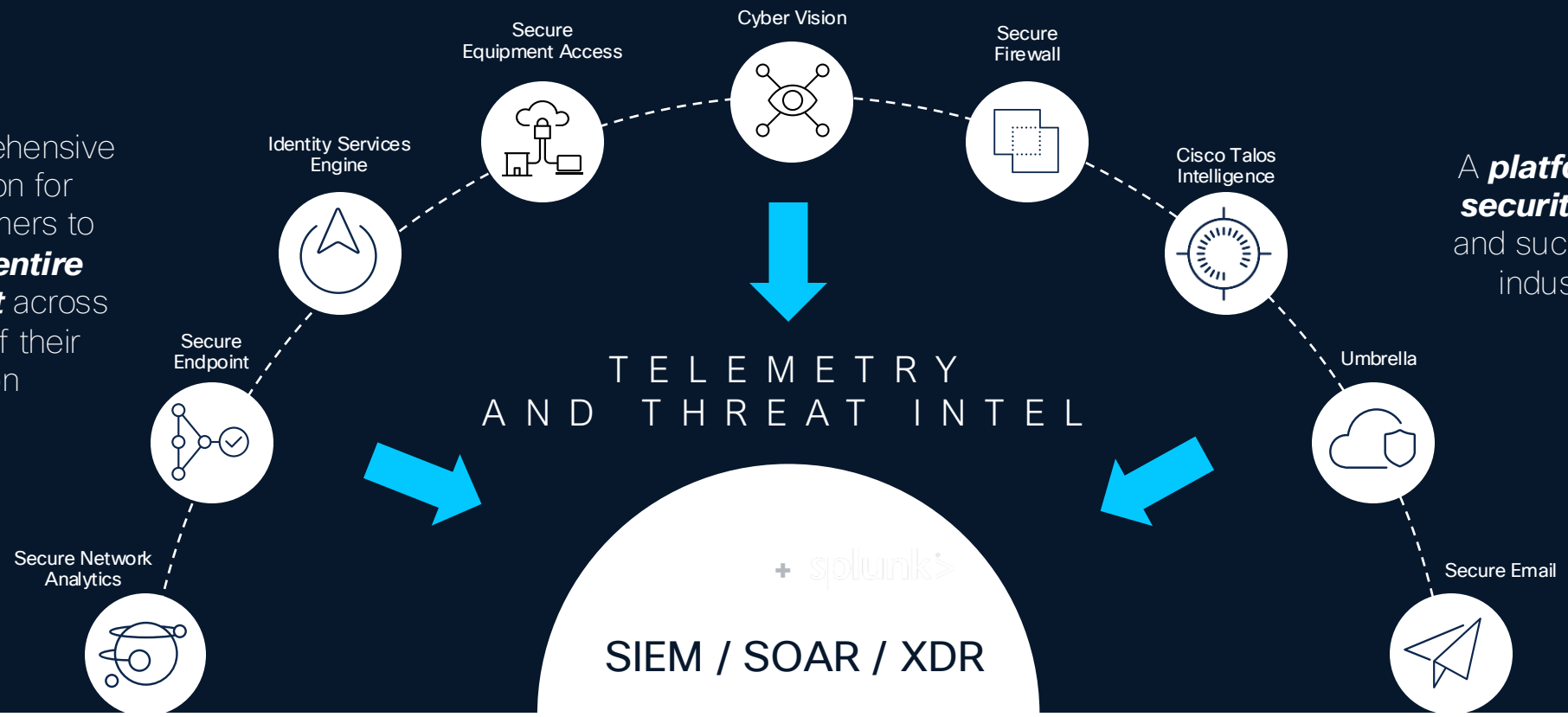
Cybersecurity urgency and AI readiness are driving OT network modernization

Leaders are accelerating IT/OT collaboration for success

Early movers are seeing significant operational and financial benefits

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

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

Cisco Trustworthy solutions for Tamperproof Security

- **Unalterable device identify**
  with SUDI (Secure unique device identifier)
- **SW image authentication during bootup**
  with Secure boot and Image signing
- **Secure storage and Cryptographic services**
  with TAM (Trust Anchor module)
- **OS protection from vulnerabilities at runtime**
  with runtime defenses

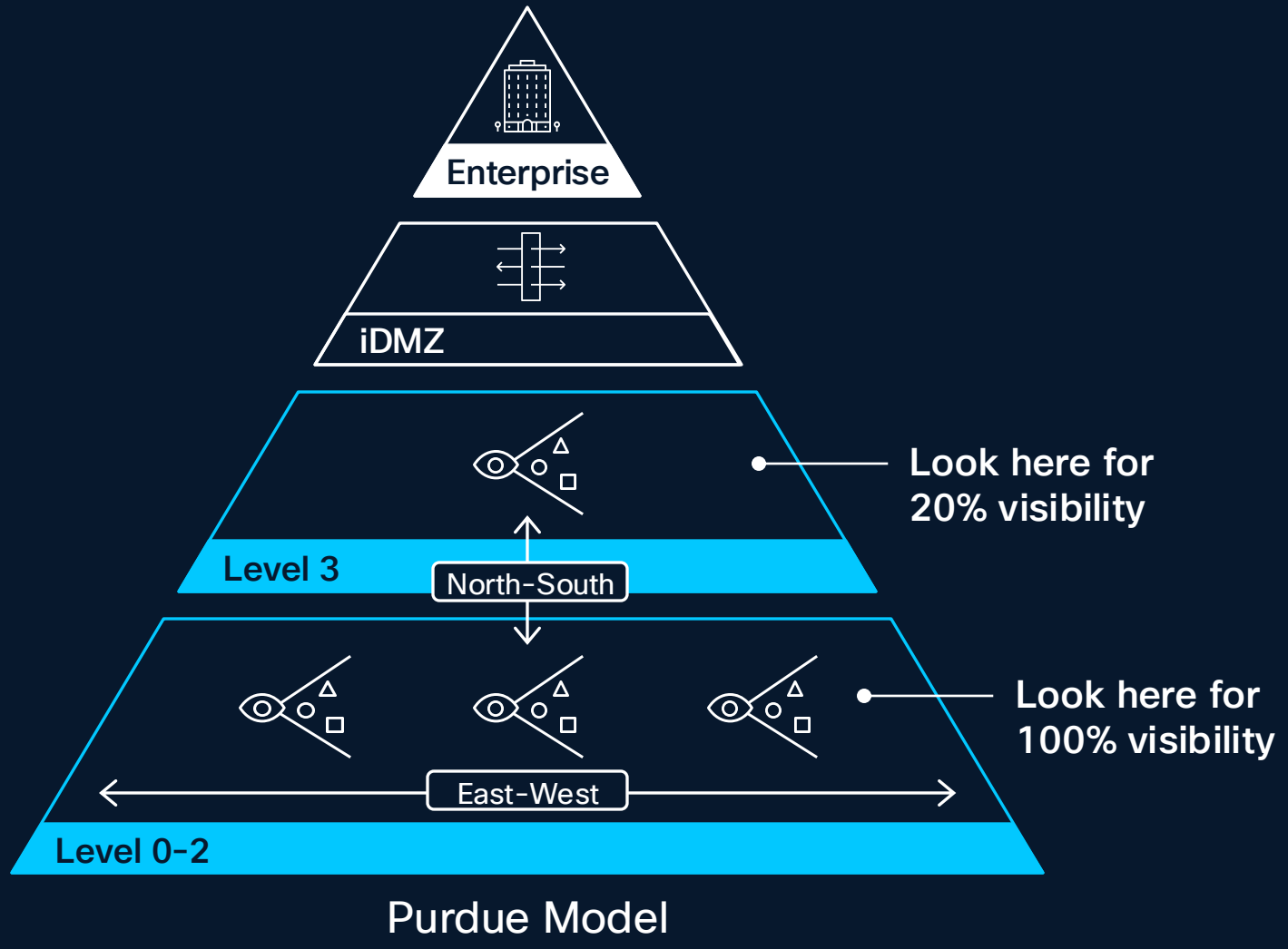
Delivering uncompromised security & reliability consistently, everywhere

Cisco Named a Leader in OT Security

FORRESTER®
WAVE LEADER 2024
Operational Technology Security Solutions

The 15 Providers That Matter Most And How They Stack Up

Security starts with visibility, but where you look matters

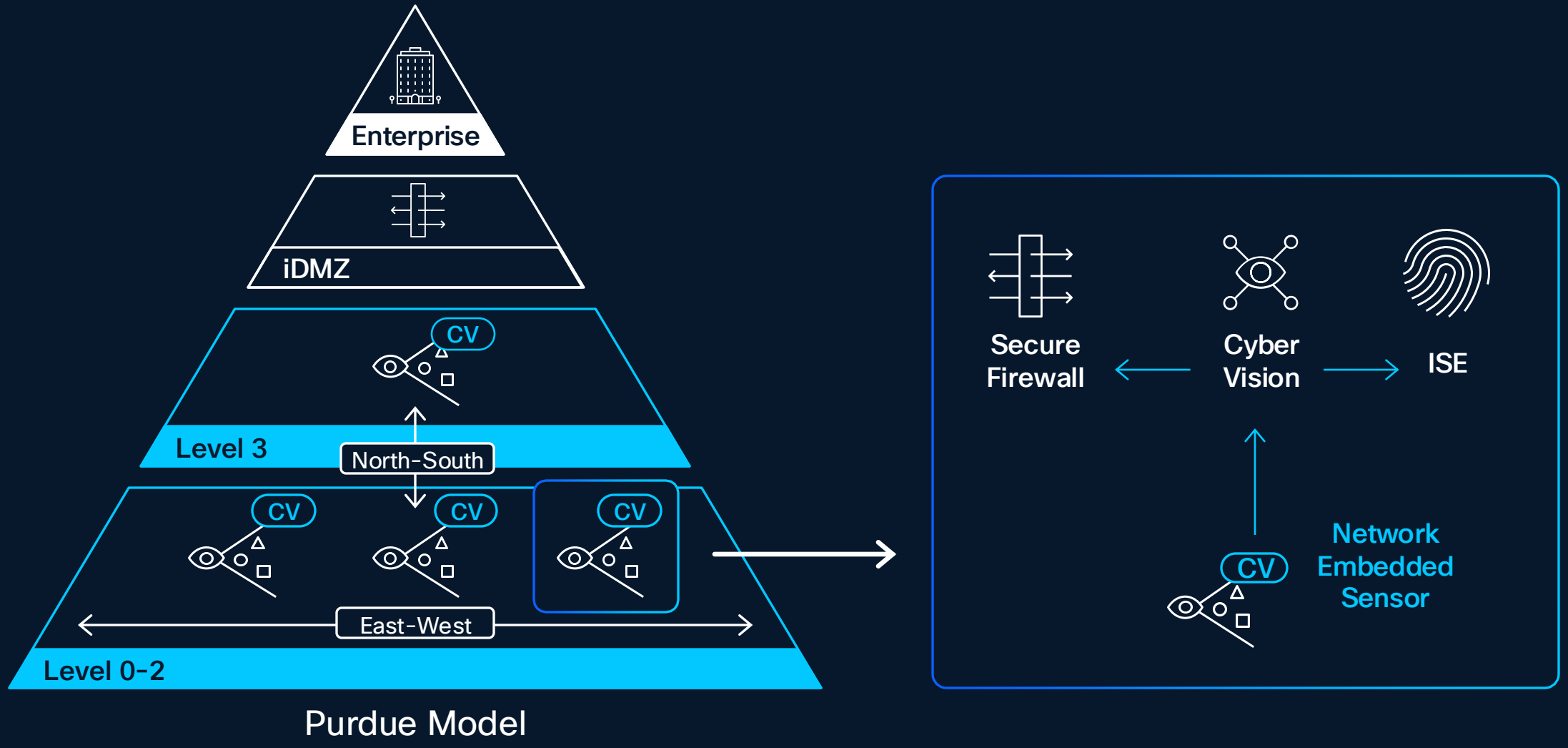


Purdue Model

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

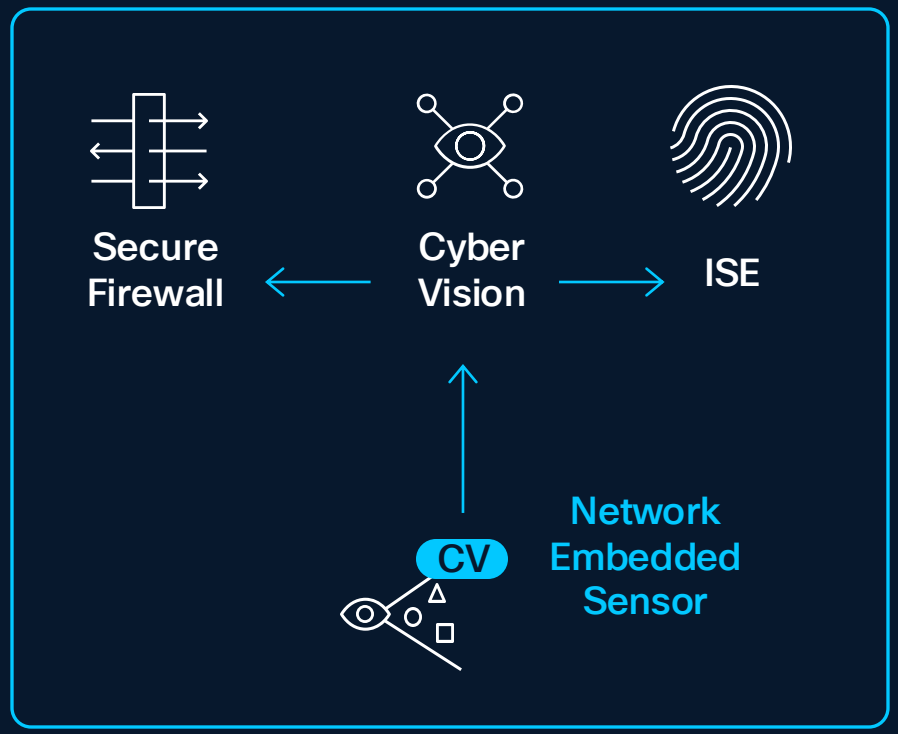
You run the risk of downtime if you try to segment Level 0-2 without 100% visibility

Visibility driven adaptive segmentation



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

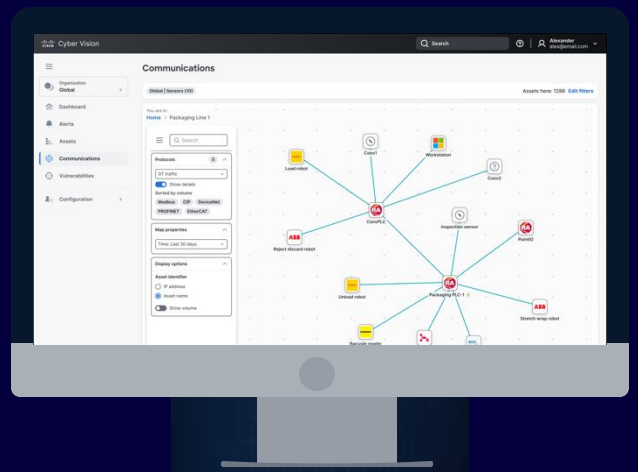


Cyber Vision

Visibility built-in, not bolted on

- Visibility of connected assets
- Identify and track vulnerabilities
- Track your risk exposure
- Stop Leaks
- Detect malicious intrusions
- Measure Progress
- Asset grouping for security policy

Cyber Vision Center



Cyber Vision Sensors

Deep Packet Inspection & Active Discovery built into your network infrastructure

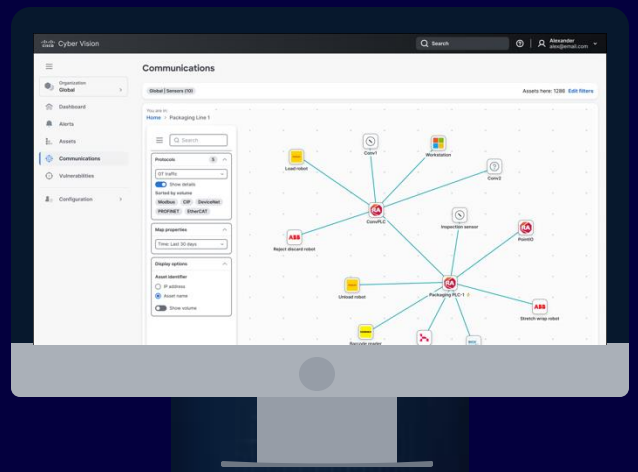
Cyber Vision

Visibility built-in, not bolted on

Key Outcomes:

- Up to date list of industrial assets
- Understanding of risks to industrial devices and measure of improvement over time
- Reduce risk with easy to deploy micro-segmentation
- Faster detection of and response to threats in industrial systems
- Improved NIS2 and IEC62443 compliance

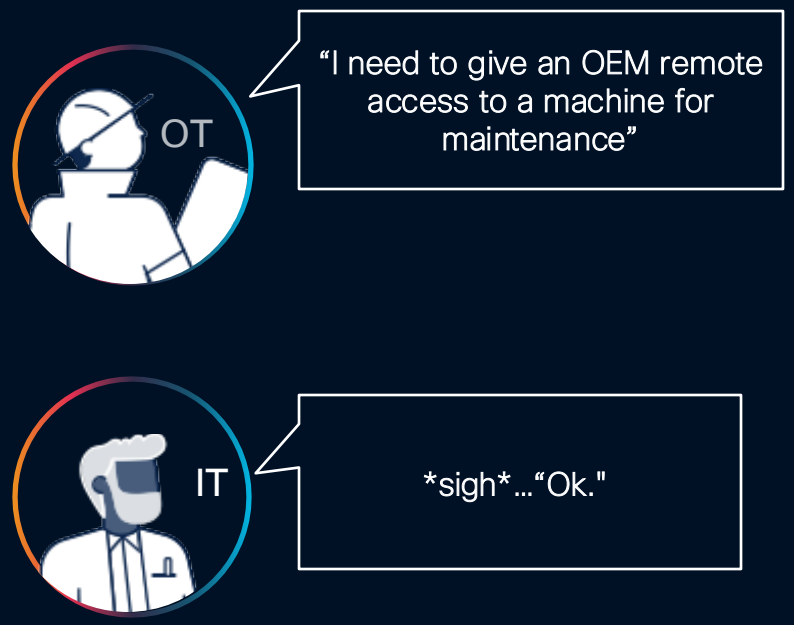
Cyber Vision Center



Cyber Vision Sensors

Deep Packet Inspection & Active Discovery
built into your network infrastructure

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



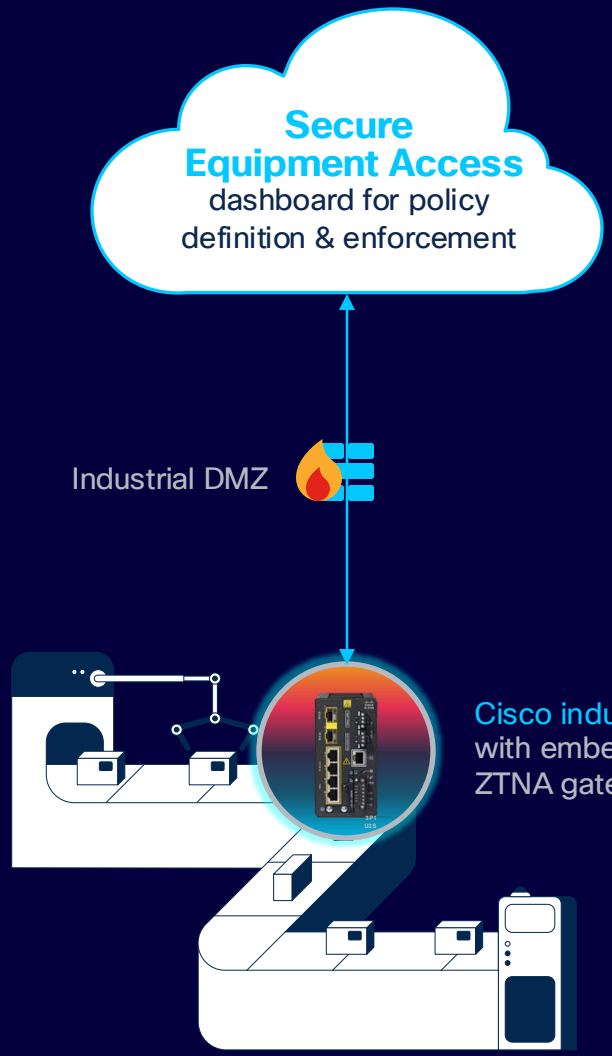
- **Add user account to the VPN**
- MFA is an optional add-on!
- Create policies for VPN user so they cannot access network
- Give user credentials to the jump server
- Add network policies to jump server to stop lateral movement
- Setup WebEx call so I can watch remotely
- Remember to close all policies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



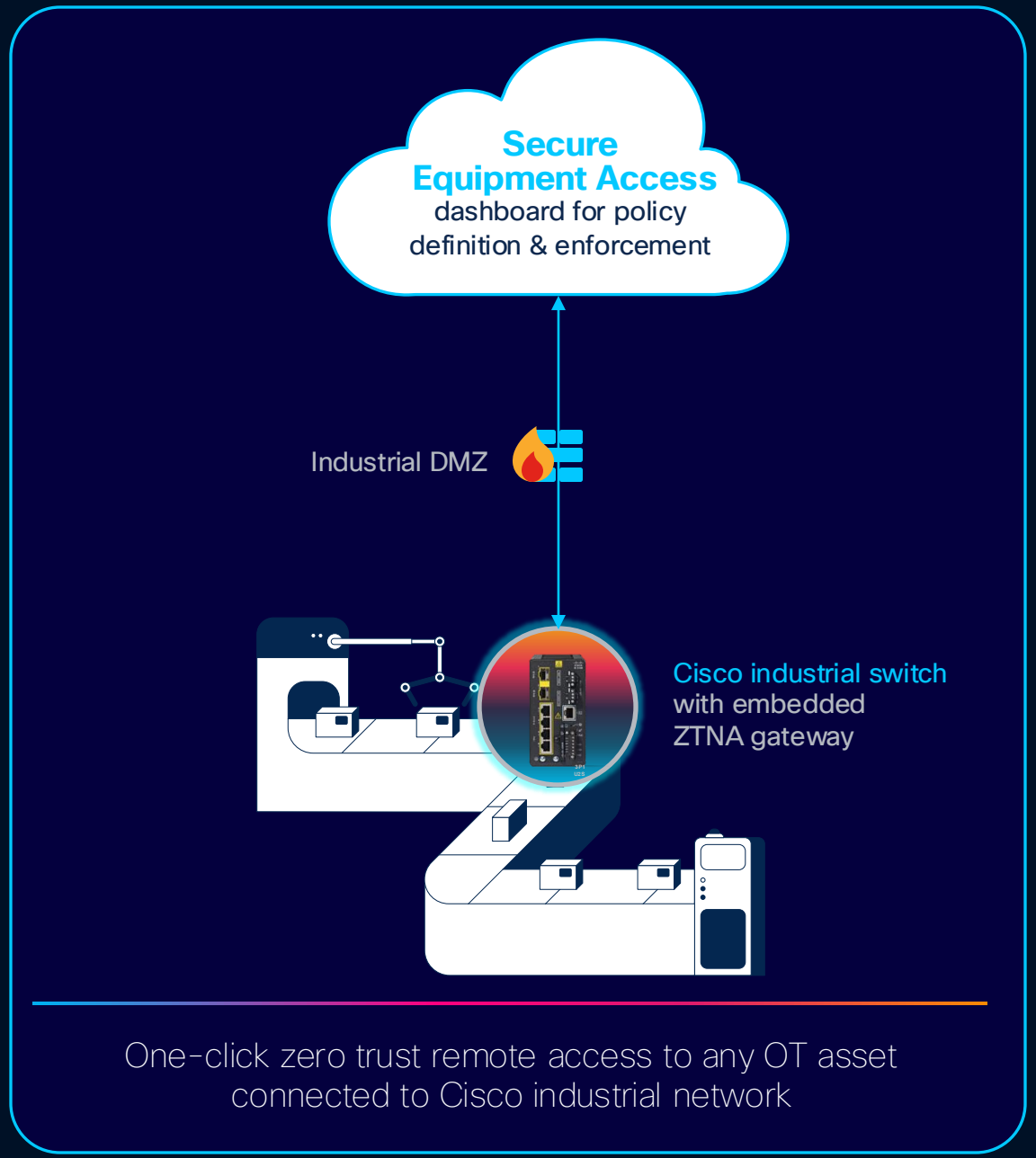
One-click zero trust remote access to any OT asset connected to Cisco industrial network

Secure Equipment Access

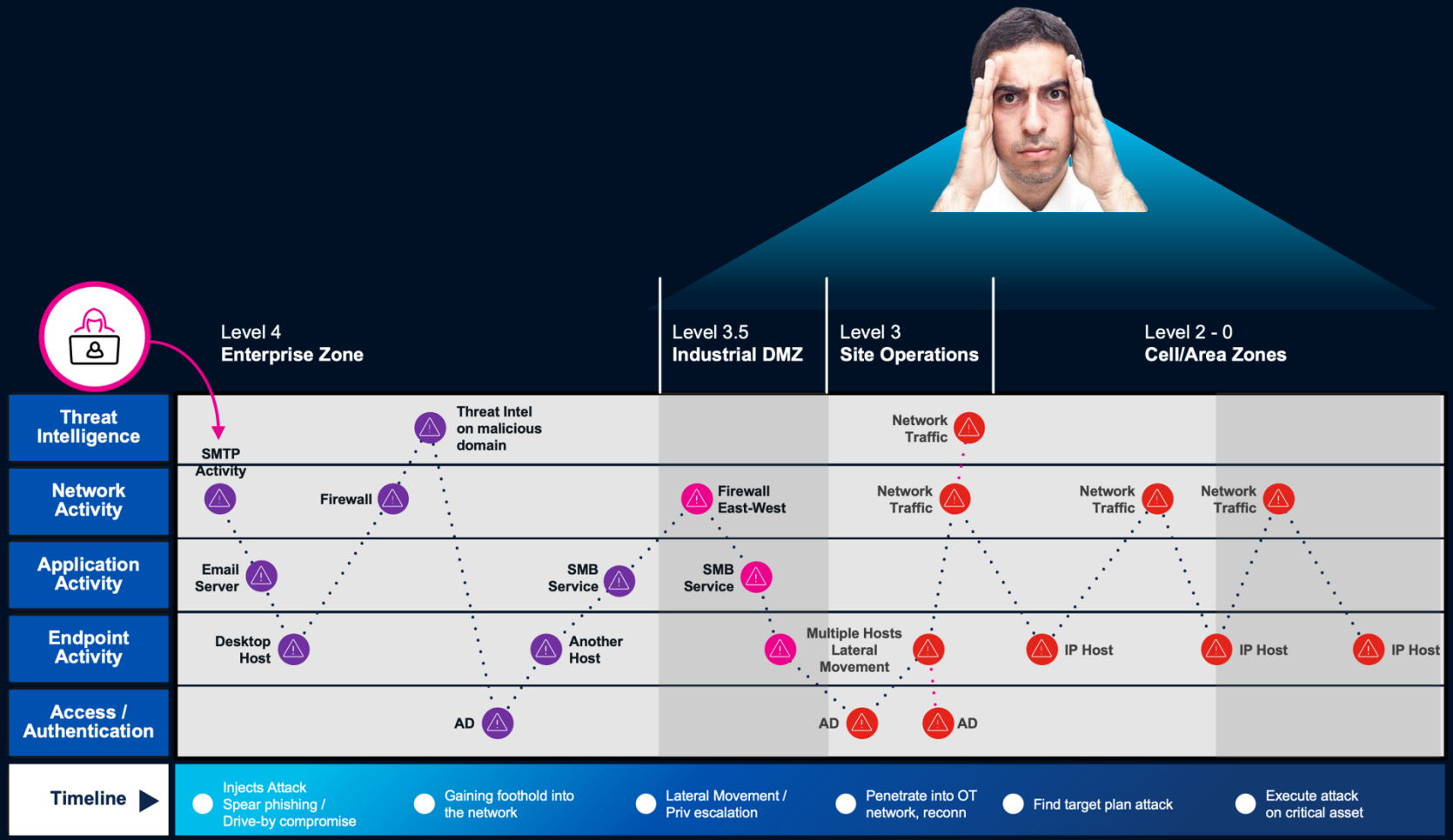
OT self service based on IT defined zero trust remote access

Key Outcomes:

- Improved production uptime with secure access for experts and vendors to resolve production issues
- Improved IT/OT collaboration with tools both teams use
- Improved NIS2 and IEC62443 compliance



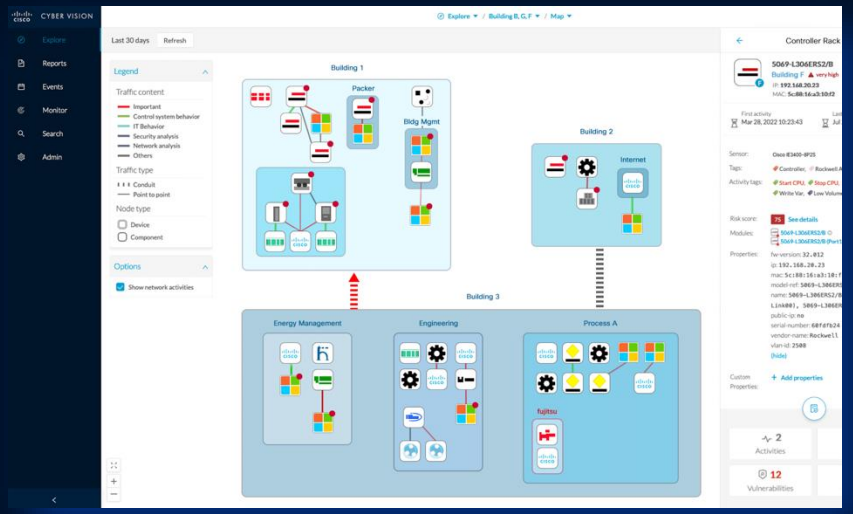
A siloed approach is not enough to secure OT



- 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

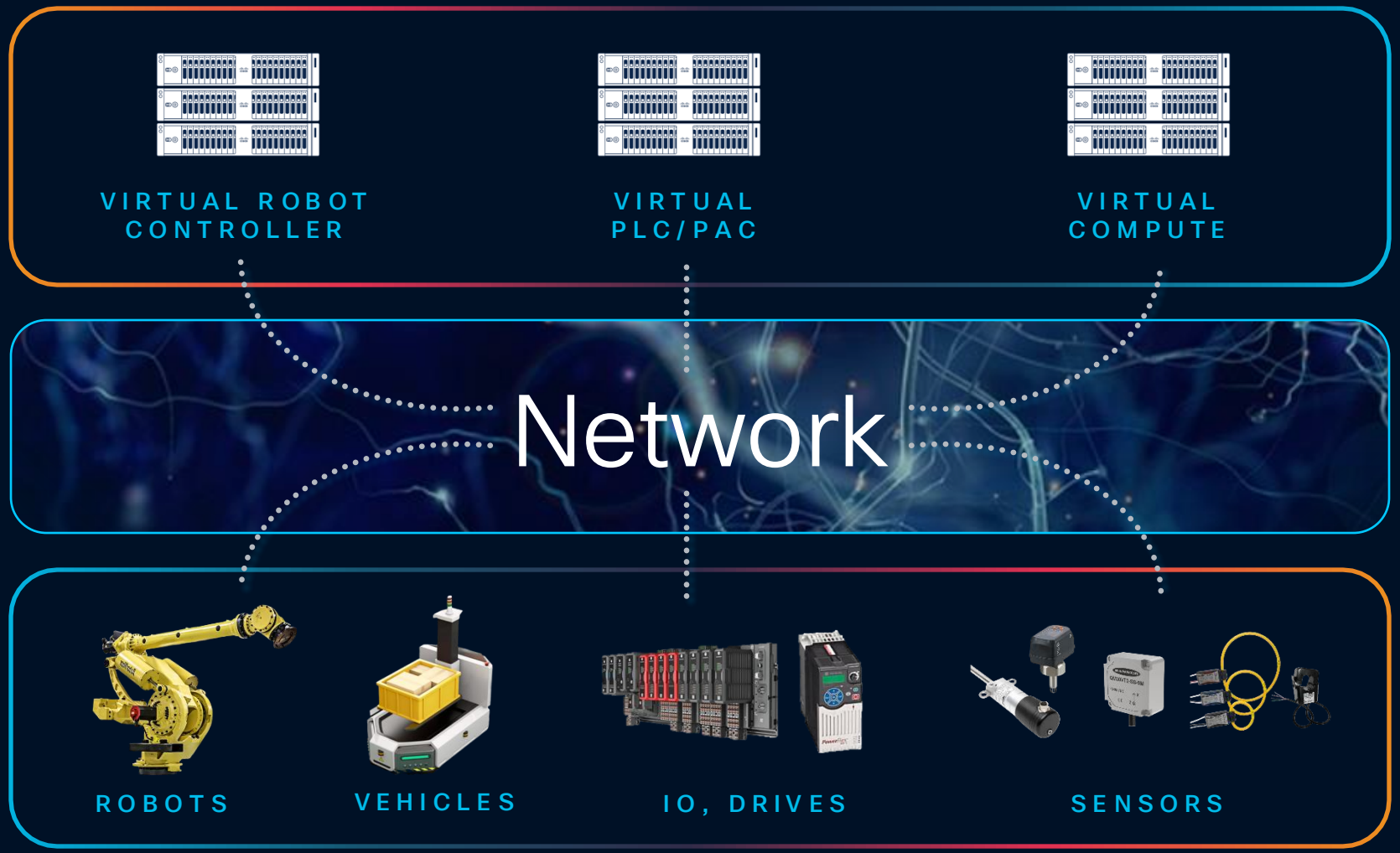
- Unified IT/OT security events management
- OT Asset Investigator
- OT Baselining
- Perimeter Monitoring
- Risk Based Alerting
- MITRE ATT&CK ICS correlation rules
- NERC-CIP compliance reports

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

Brains
in the data center

Nervous system
is the network

Physical components
on the factory floor



Thank you


CISCO