L'industrie de demain, les enjeux sécuritaires d'aujourd'hui

Exploiter la collaboration IT OT et les technologies de sécurité pour construire des opérations industrielles cyber résilientes

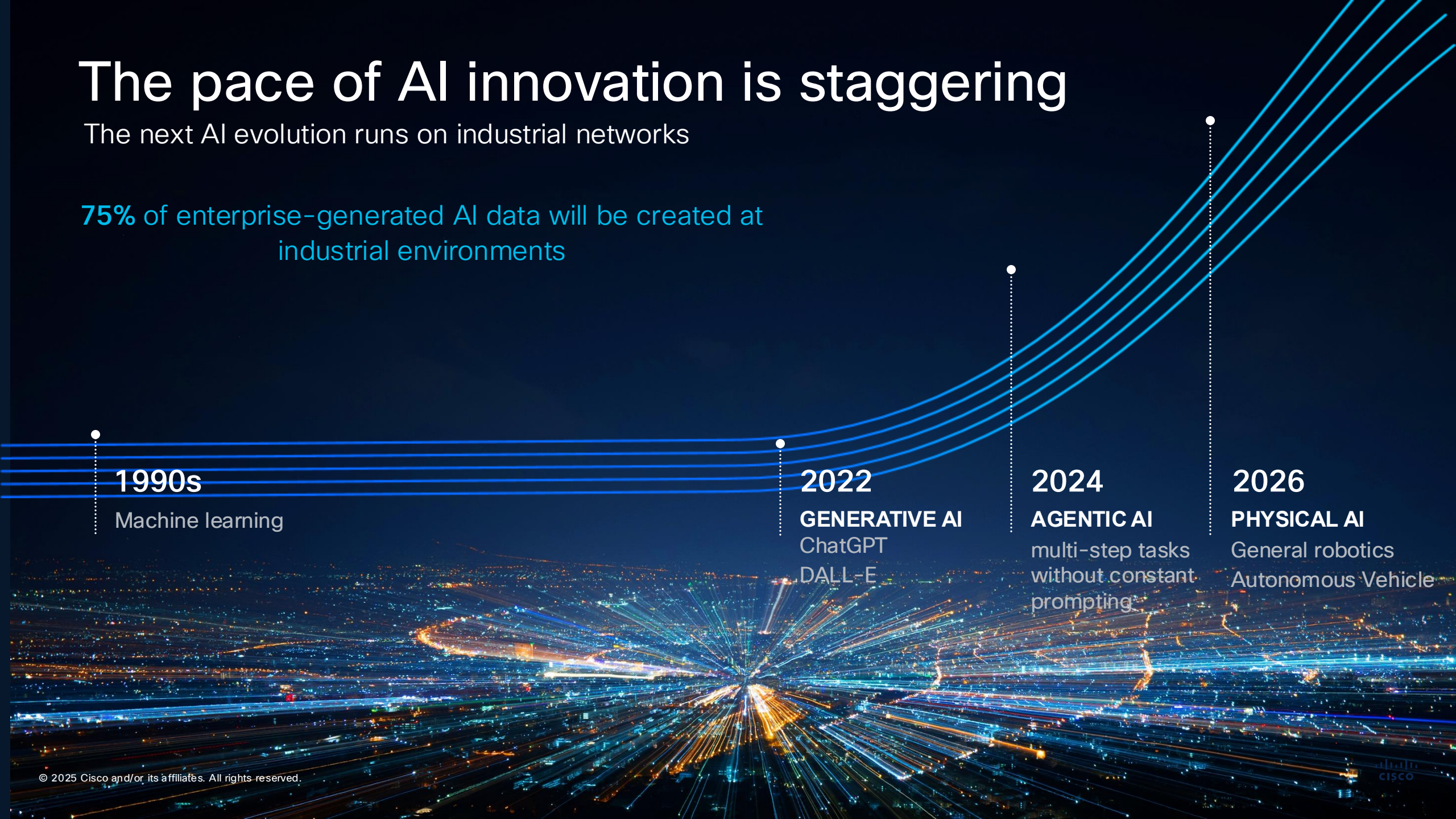
Sarah-Louise Justin, Cisco Account Executive Industrial IoT

September 16, 2025

The pace of AI innovation is staggering

The next AI evolution runs on industrial networks

75% of enterprise-generated AI data will be created at industrial environments



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

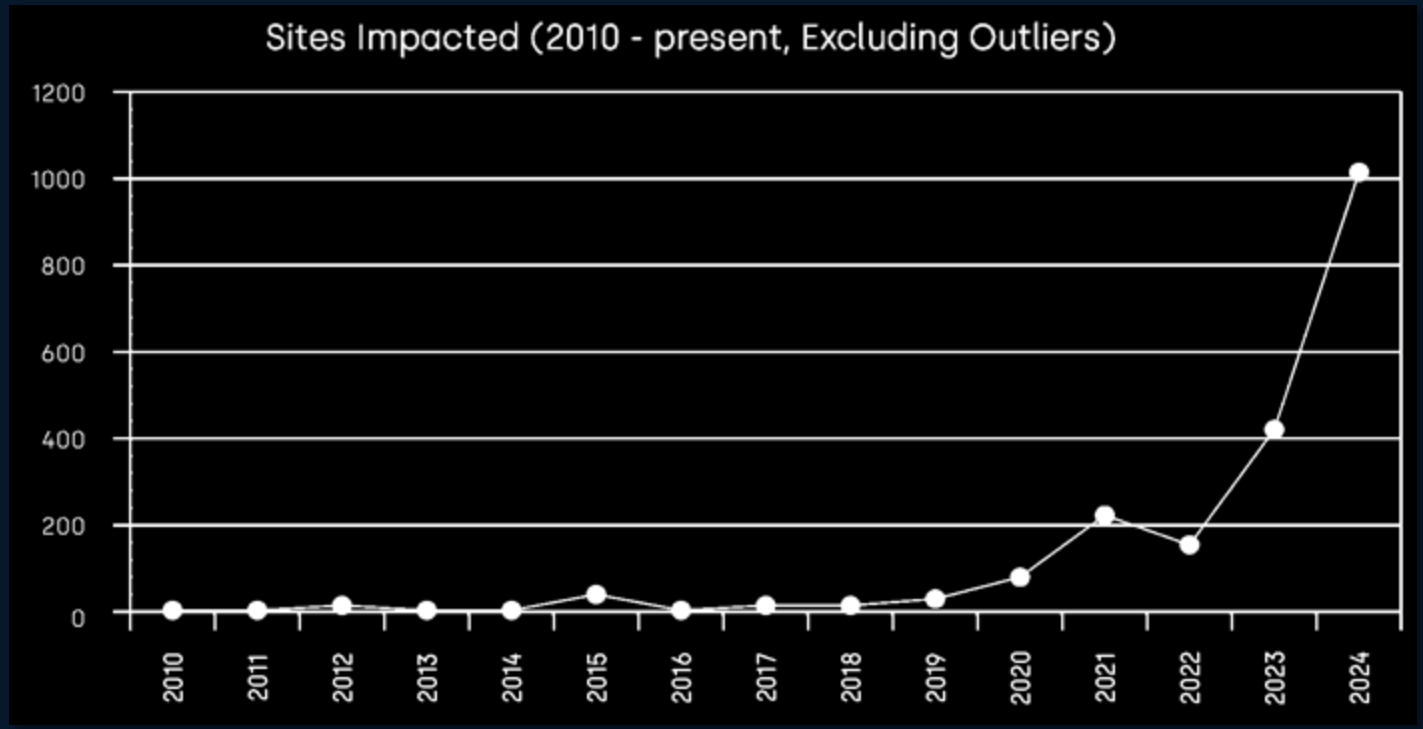
Cisco GSX

The reality of industry digitization

Increased connectivity results in more cyberattacks

2024 saw:

- At least one cyberattack every week against OT assets caused physical consequences in 2024
- 146% increase in sites impacted by cyberattacks with physical consequences
- Nation state attacks have tripled

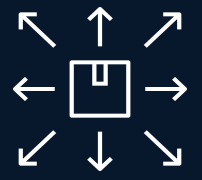


Waterfall 2025 OT Cyber Security Threat Report

Bringing our portfolio together

One Cisco Vision

Hybrid Mesh Firewall



Universal Zero Trust Network Access (ZTNA)

SOC of The Future

Accelerated by Cisco AI

Context

Identify Context Across the Network

Users

Devices

IoT / Things

Policy Decisions

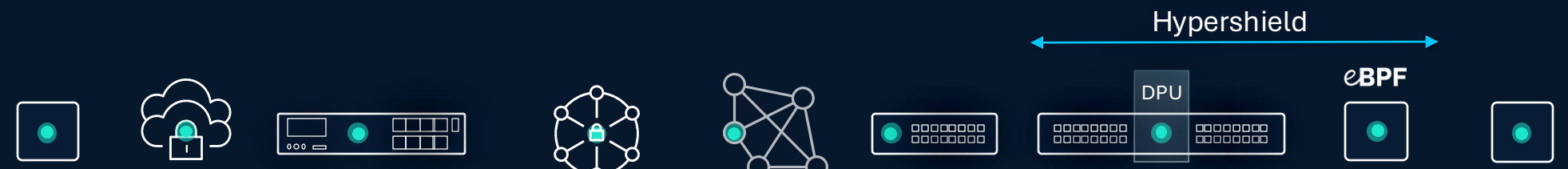
Decide on policy based on the context

Security Cloud Control

ISE

Policy Enforcements

Enforce policy Across the Network



AI Security

Multi Cloud Defense

Secure Firewall

Secure Access

ACI

Secure Router

Smart Switches

Isovalent

Secure Workload

The journey to secure industrial networks

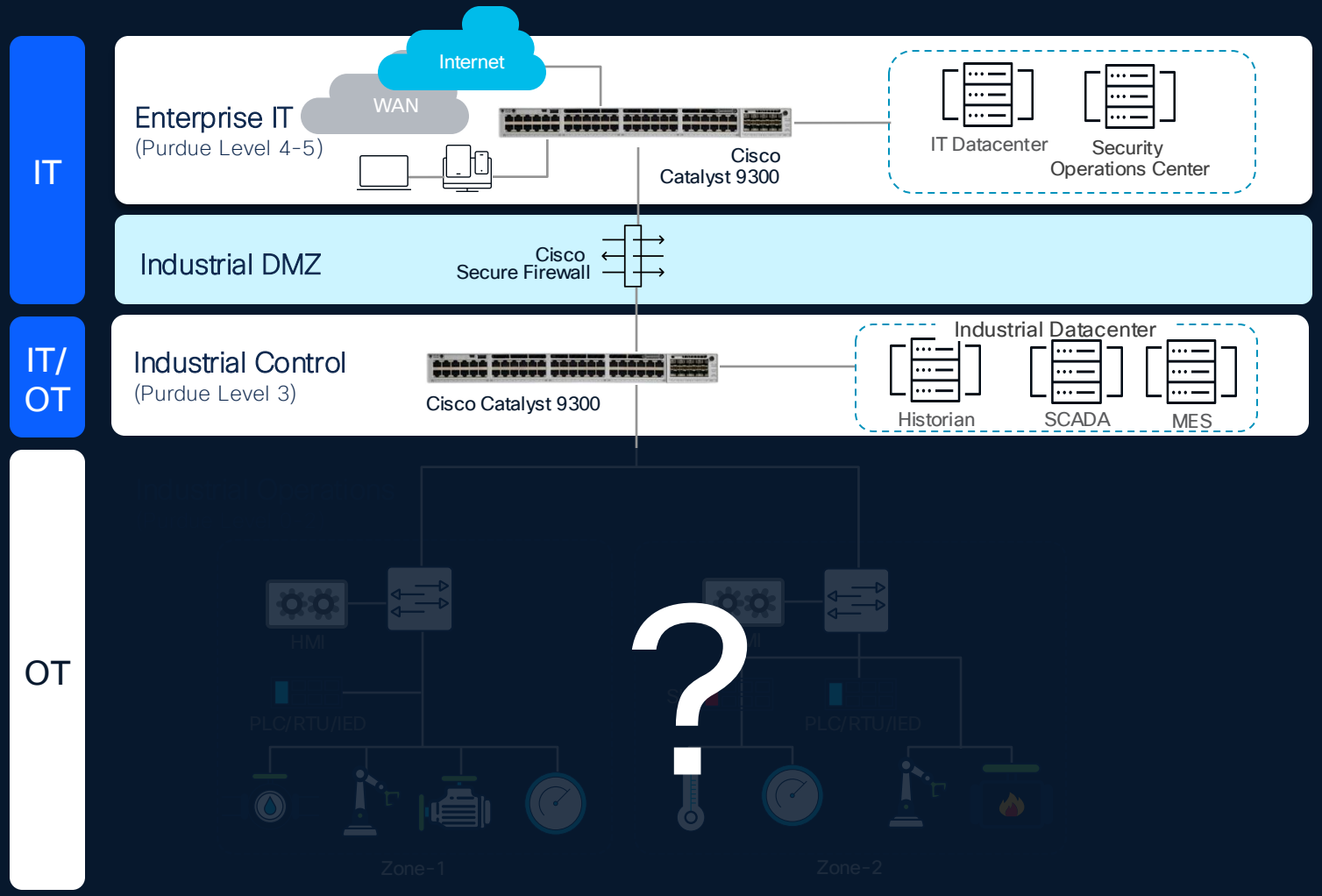
Understand the OT security posture with OT visibility

Limit blast radius with network segmentation

Control risks from remote access to OT assets

Monitor OT networks in the SOC

Securing industrial operations starts with OT visibility

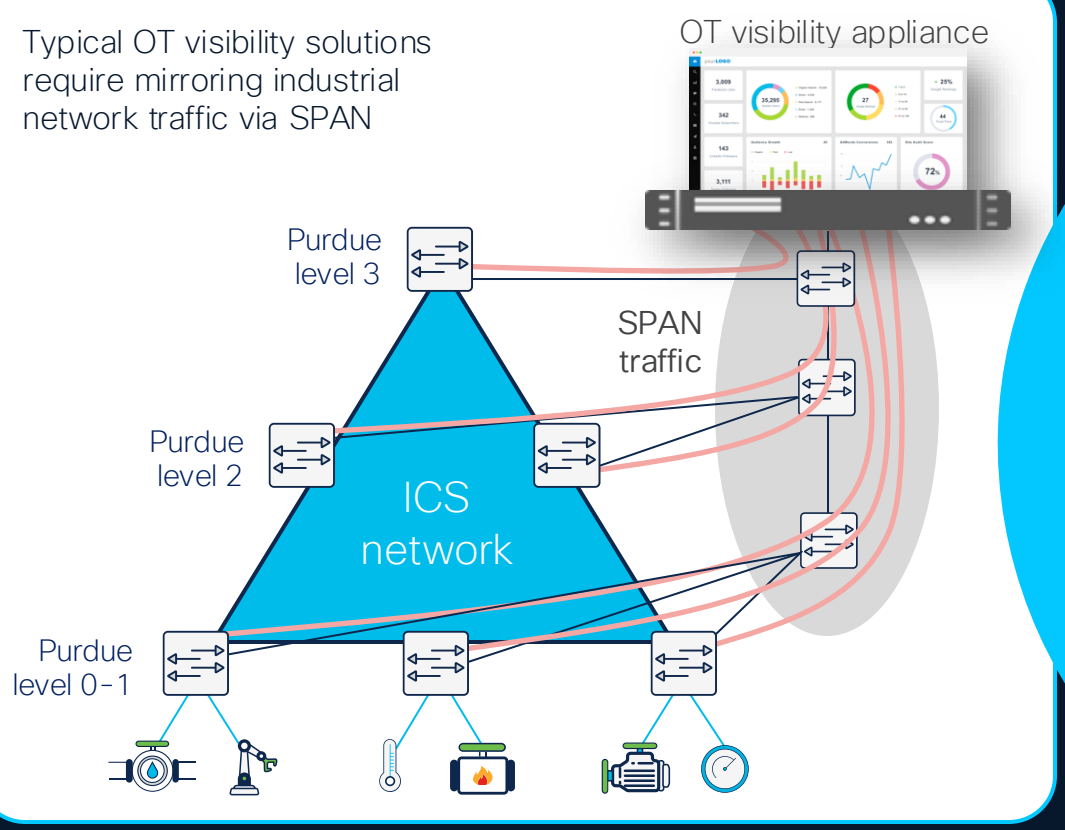


How can IT leverage network equipment it owns to gain visibility into OT environment?

Most OT visibility solutions cannot be deployed at scale

Beware of hidden costs!

Typical OT visibility solutions require mirroring industrial network traffic via SPAN

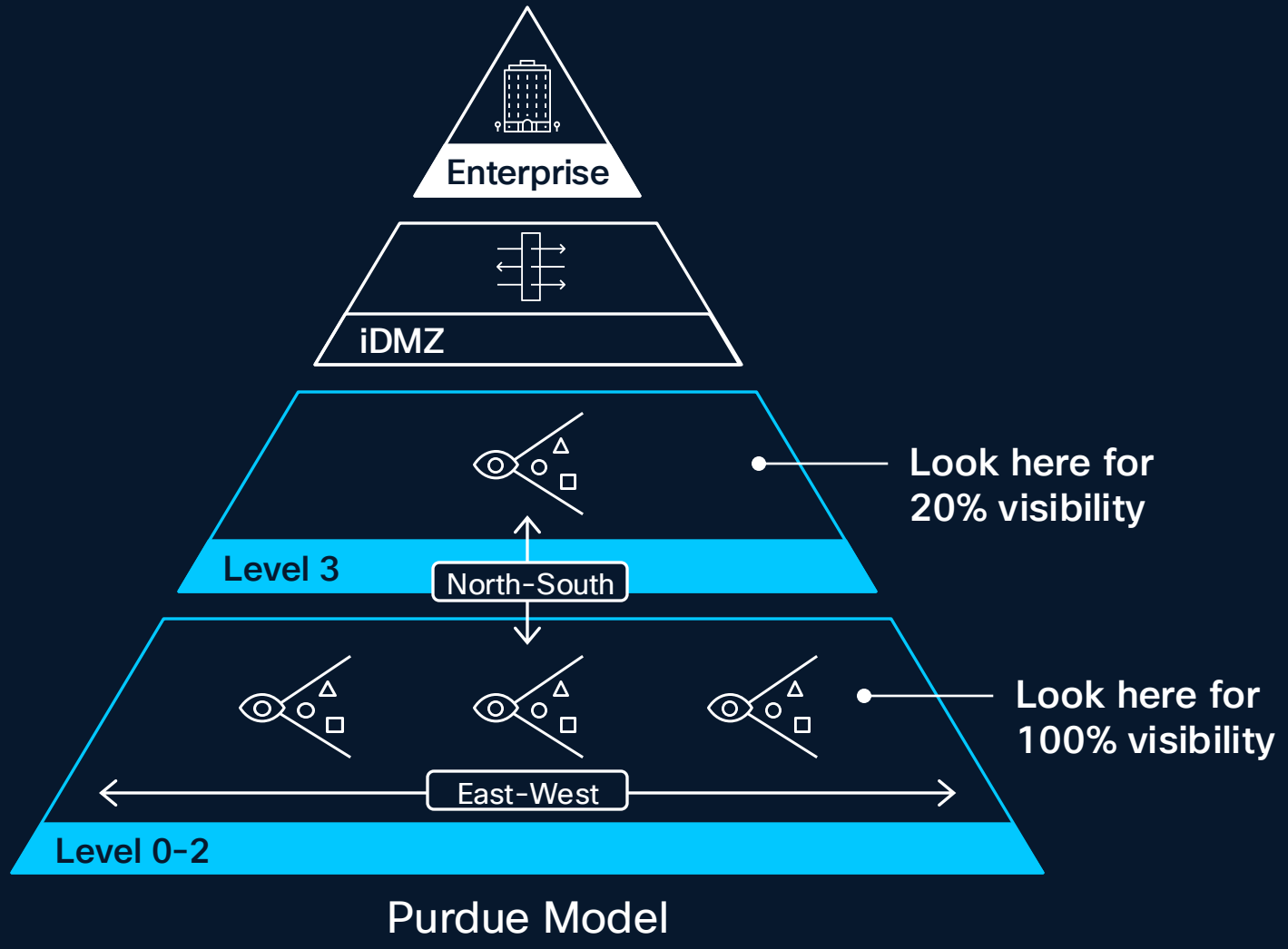


Additional switches for SPAN collection

Expensive cabling for collection network

Exponential traffic increase due to SPAN

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

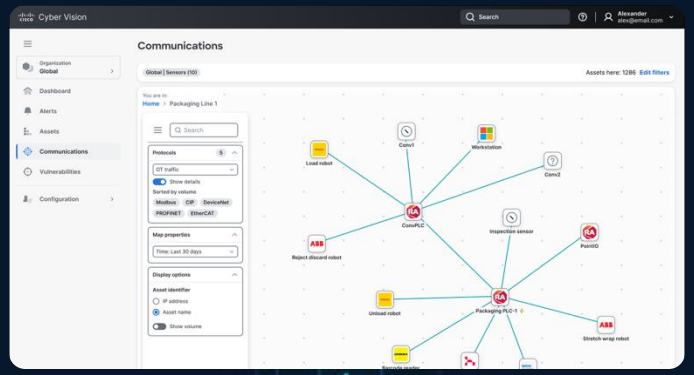
Gaining visibility at the aggregation layer sees very little as most OT traffic is local to the production cell

Cisco Cyber Vision

Visibility built-in, not bolted on

Cisco industrial network sees everything, so you gain visibility at scale

Cyber Vision Center



Lightweight Metadata

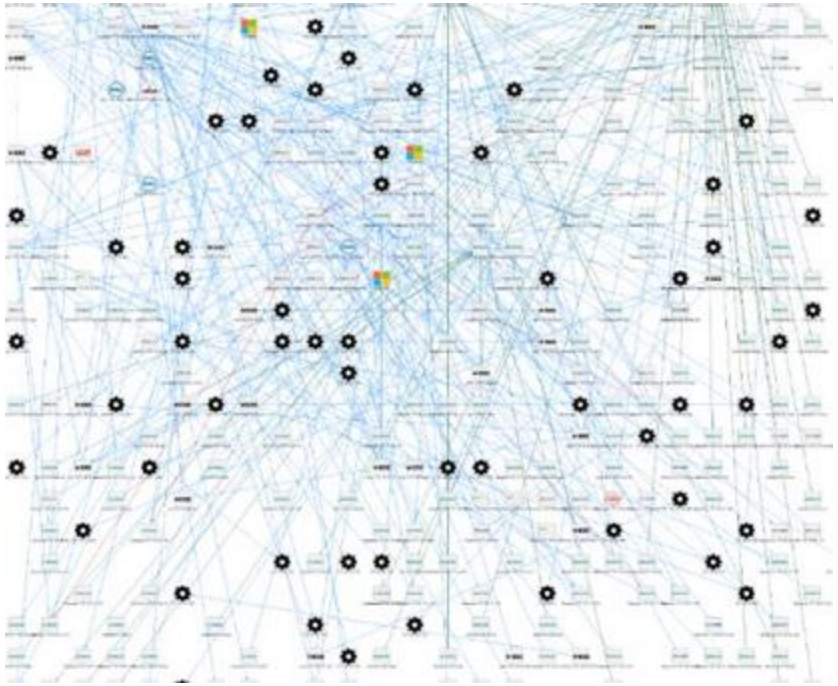
Cyber Vision Sensors

Deep Packet Inspection & Active Discovery built into your network infrastructure

Cisco Cyber Vision

Starting an OT Visibility project ... The reality

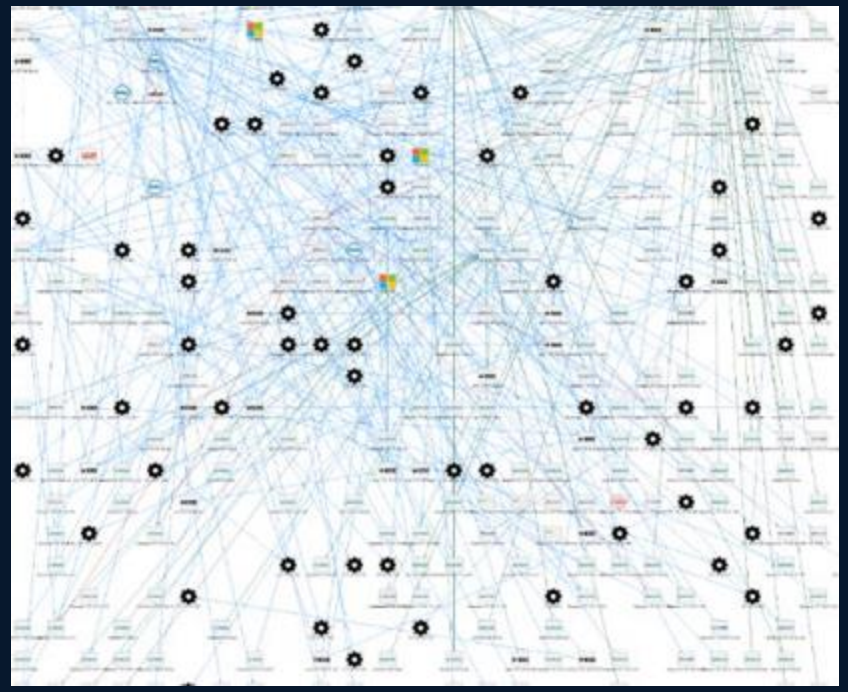
Your actual OT assets & their communications



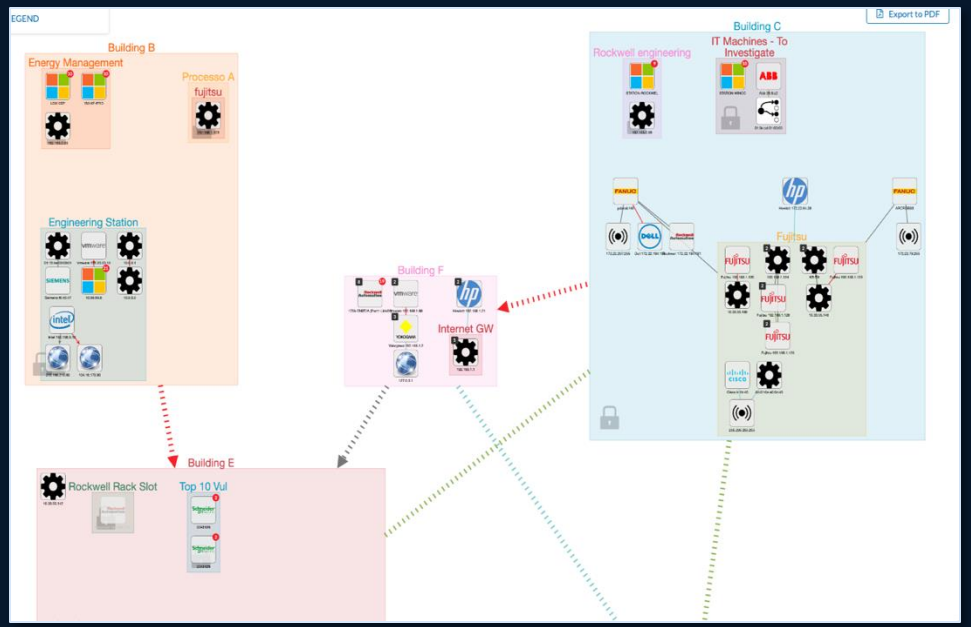
Introducing AI-driven Network Segmentation for OT

Turning Complex OT Traffic into Actionable Insights

Your actual OT assets & their communications

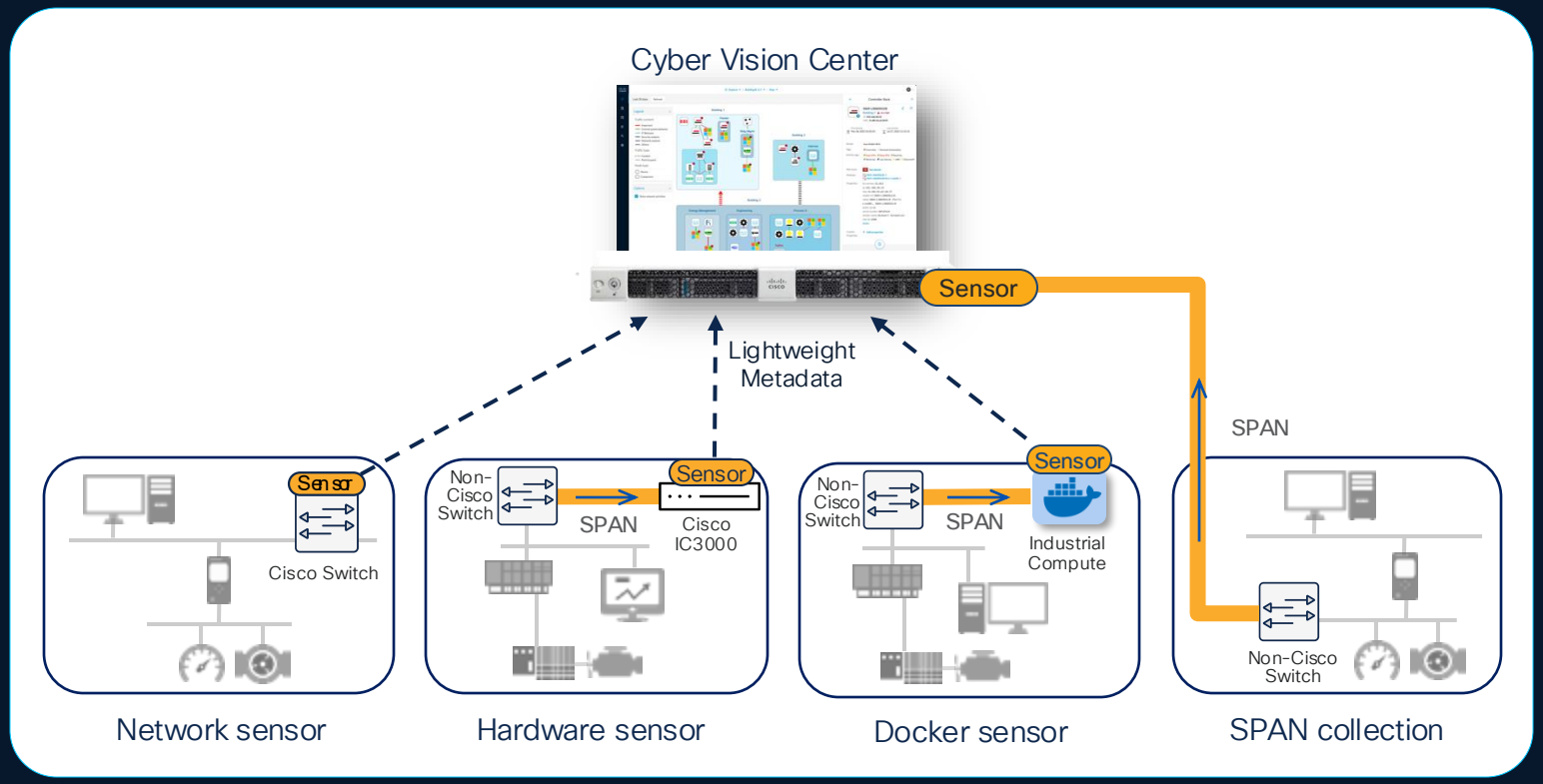


converted into information that drives actions



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

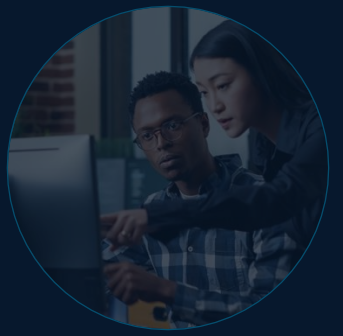
Scales across brownfield and greenfield environments

Step #2: Segment the industrial network

Understand the OT security posture with OT visibility

Limit blast radius with network segmentation

Control risks from remote access to OT assets

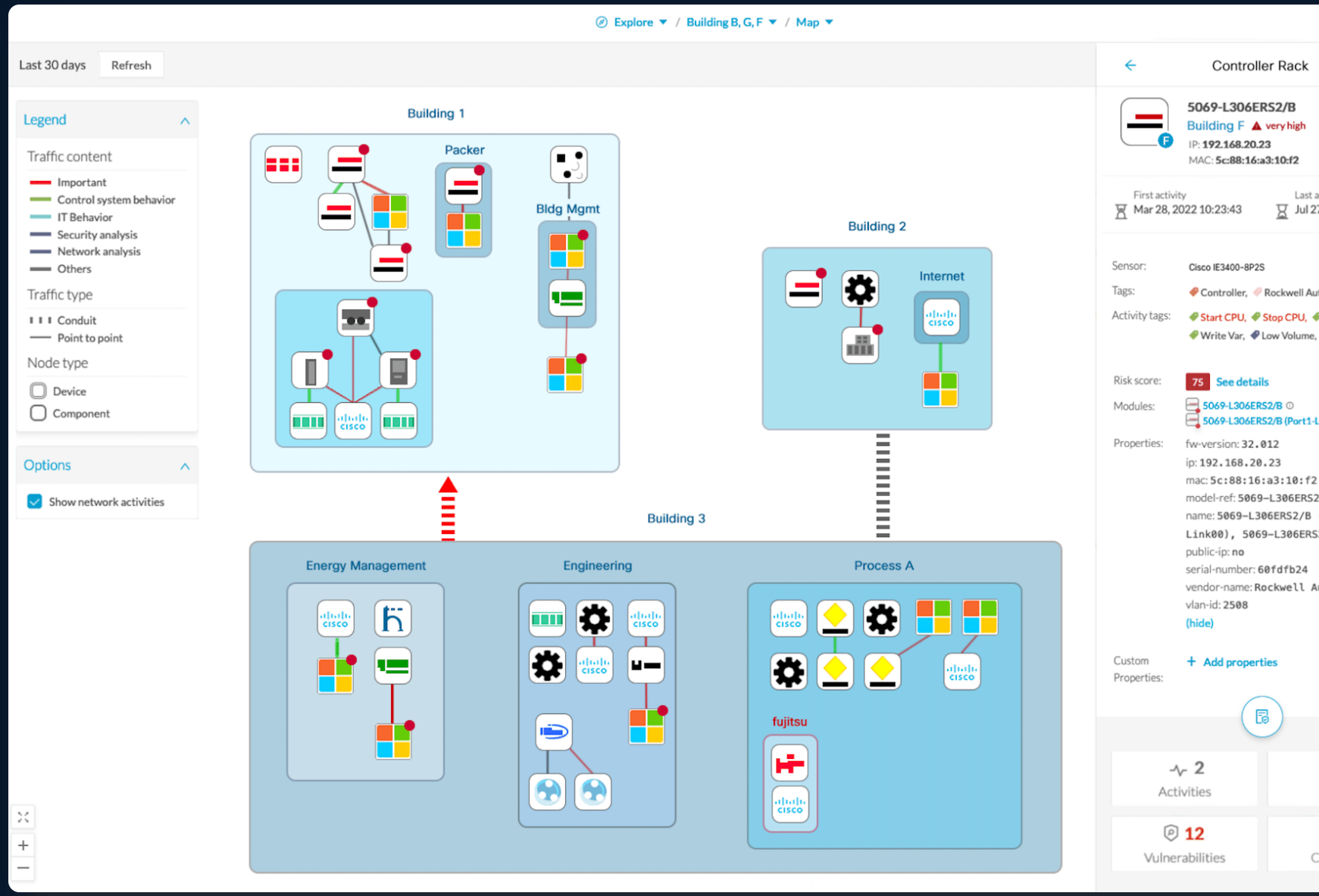


Monitor OT networks in the SOC

Cyber Vision

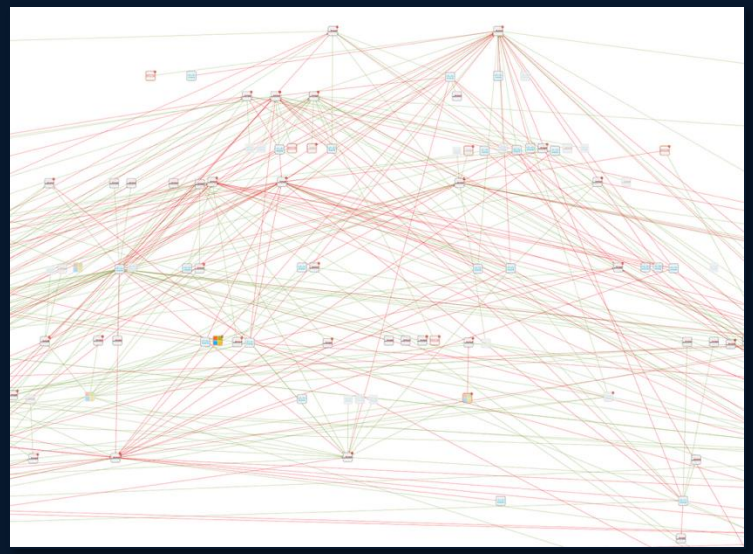
IEC-62443 segmentation made simple

- 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



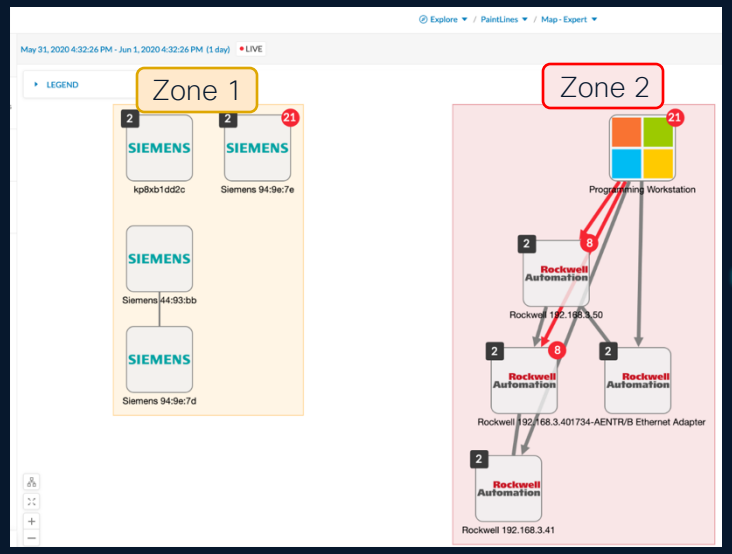
Using visibility to drive OT segmentation at scale

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

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

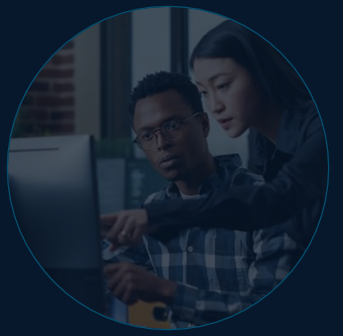
Using the network to shrink the zones of trust and protect operations at scale

Step #3: Secure Remote Access to OT Assets

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

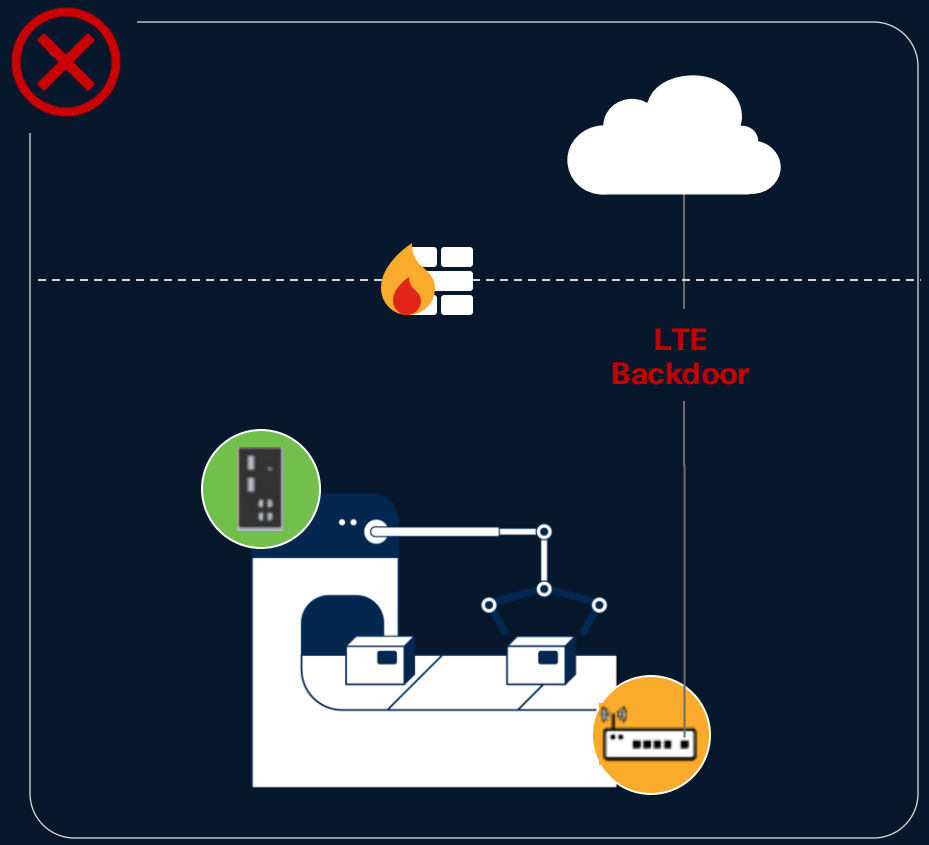
Increased Cyber Risk with more remote users accessing your OT assets

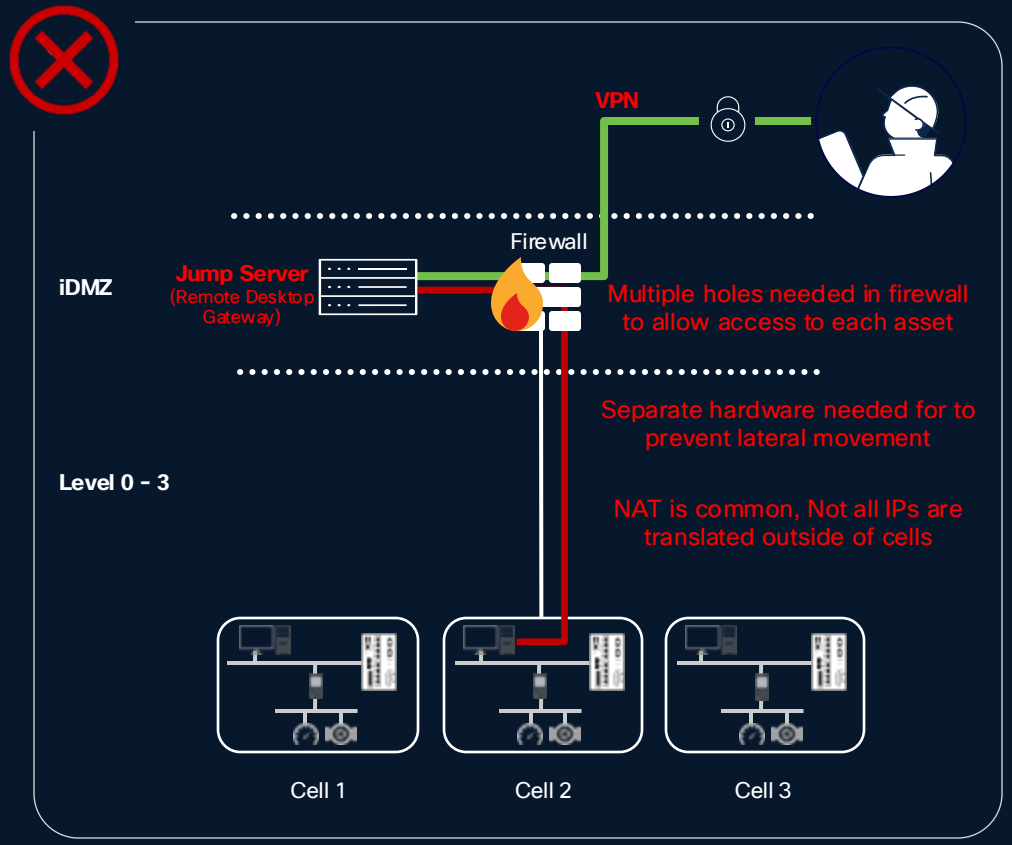
Remote Users

Machine Builders,
System Integrators,
Remote Workforce

NIS2 makes it a priority to implement Zero-Trust access control policies

Existing remote access solutions are either security backdoors or come with many trade-offs





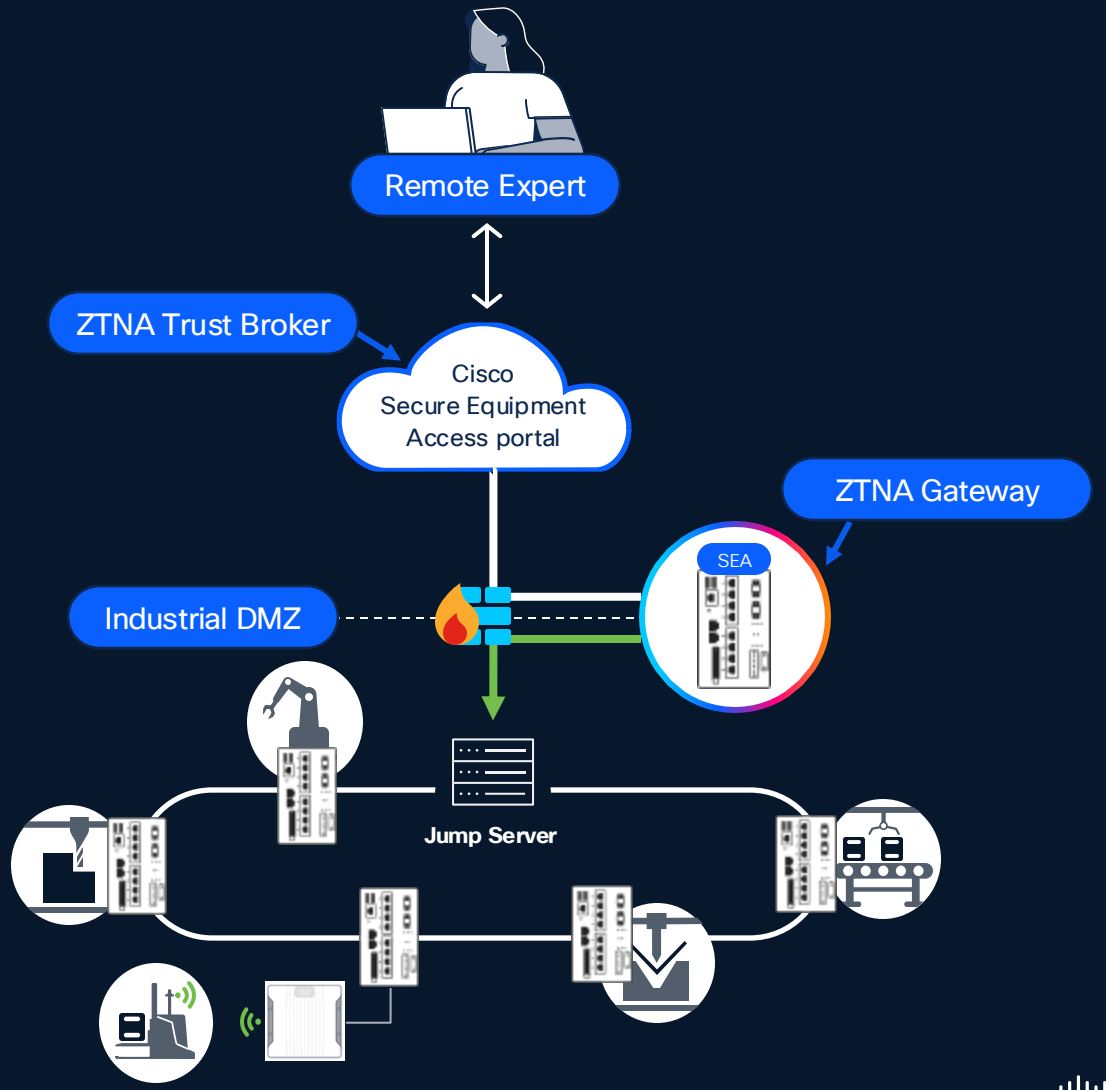
Universal identity makes Universal ZTNA possible

There is no universal zero trust without ubiquitous, shared identity across the enterprise

Enhance existing Jump Servers with Zero-Trust

Supercharge your existing remote access setup with modern security capabilities

- Keep existing jump servers to maintain workflows and simplify change
- Replace insecure VPNs and enforce robust access control with SEA ensuring only authorized users have access only at specific times
- Gain new control with SEA recording sessions or inspecting file transfer*
- Simplify operations with cloud-based policy management that OT can use



Step #4: Unify IT and OT visibility into the SOC

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

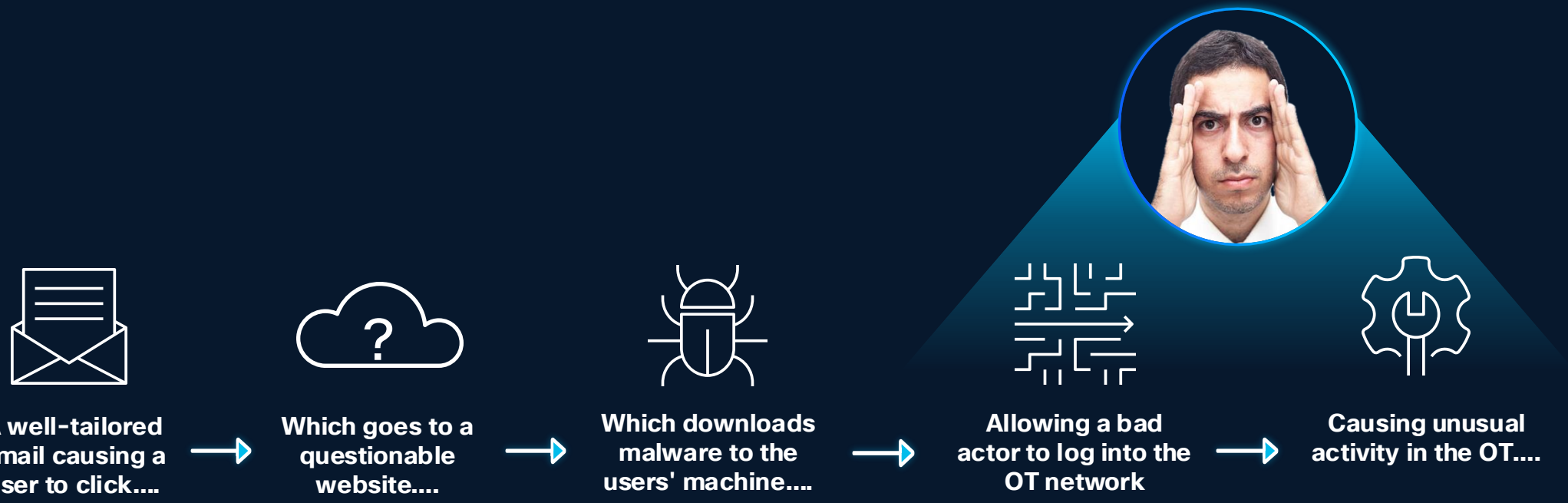
A siloed approach is not enough to secure OT

Detecting threats requires cross-domain visibility

OT, IT, and Cloud domains are increasingly **interconnected**

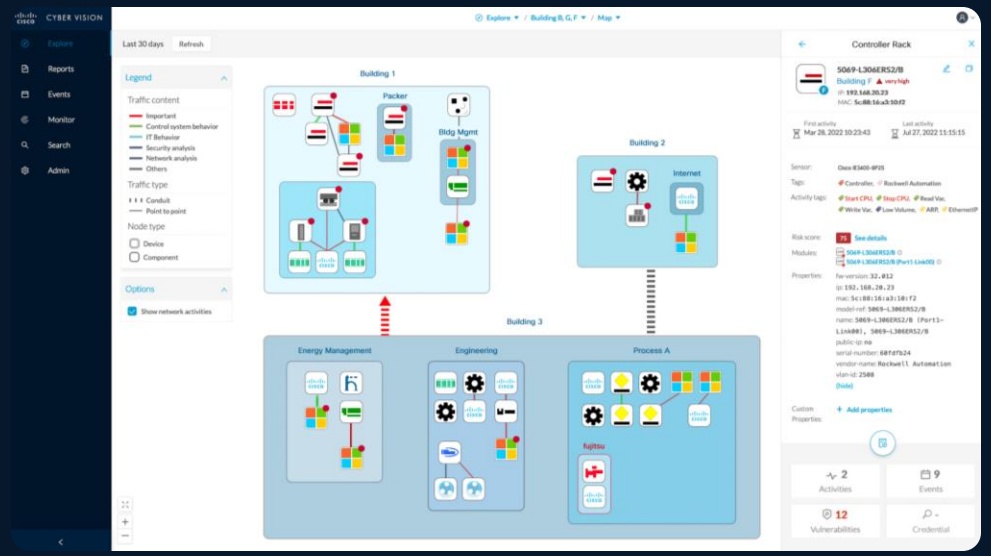
Attacks to OT almost always **originate from IT**, e.g. through a phishing email

Unified visibility across domains is key to detecting and stopping threats



Getting visibility to OT in the SOC

Cyber Vision

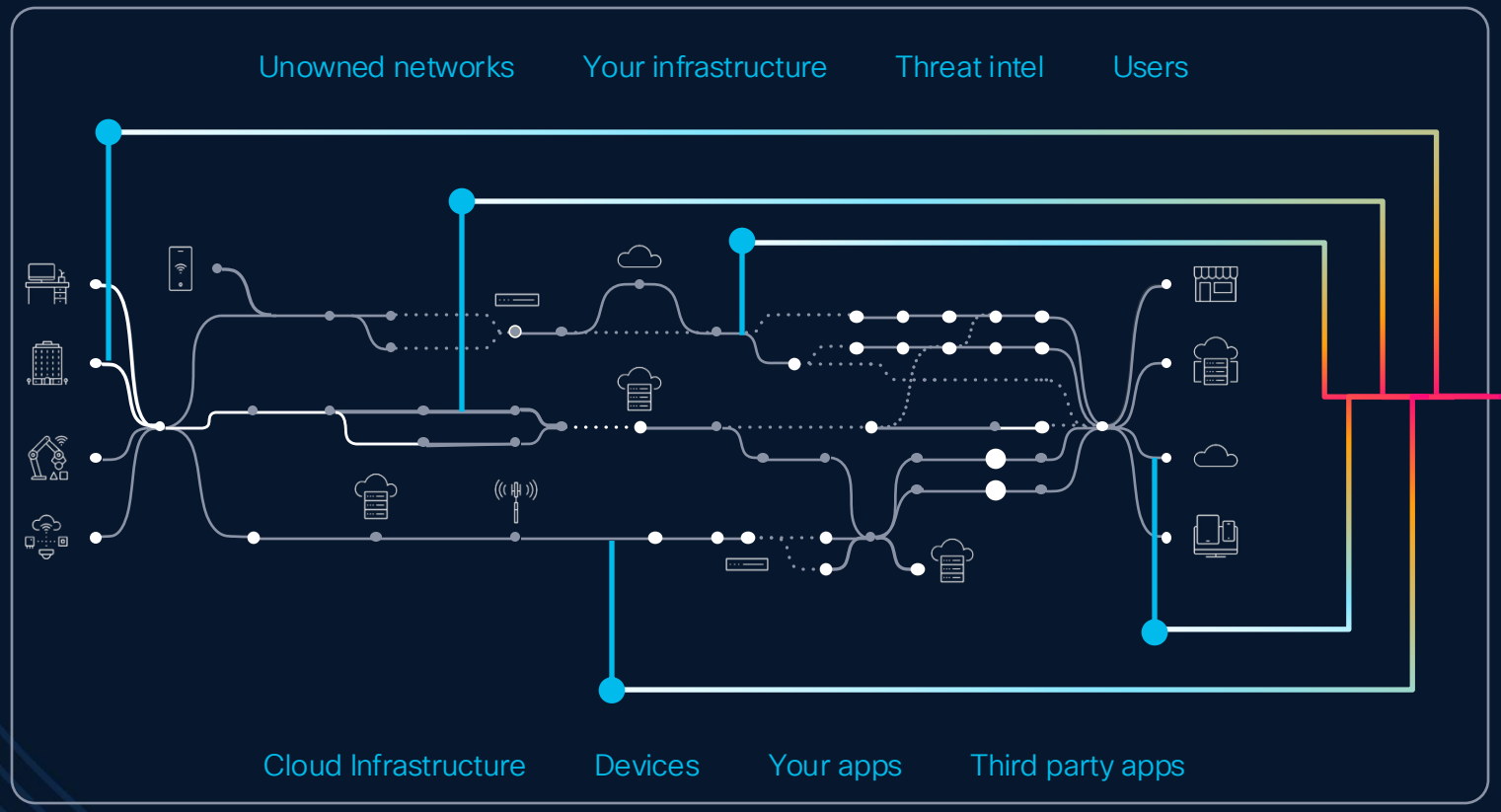


Cyber Vision
Add On for Splunk

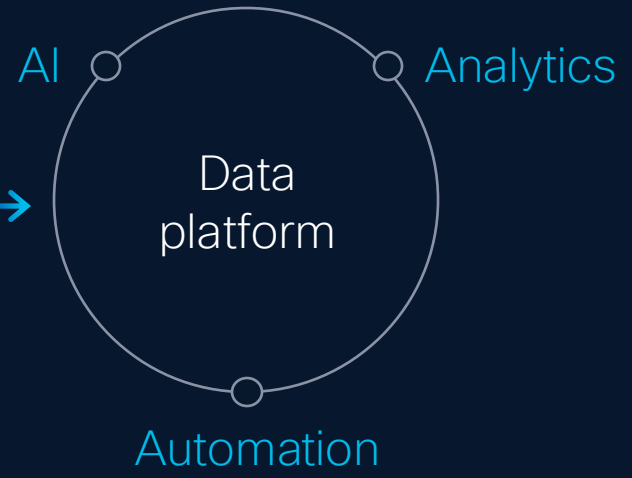
Splunk OT Security

Visibility across the entire chain

The power of Splunk and Cisco means you can unify data across the digital footprint to drive resilience and better outcomes



Data



Security | Assurance | Observability

Key takeaways

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

MERCI DE VOTRE ATTENTION !

Sondage de satisfaction

Merci de votre feedback

Scannez-moi

Cyberdefense


CISCO