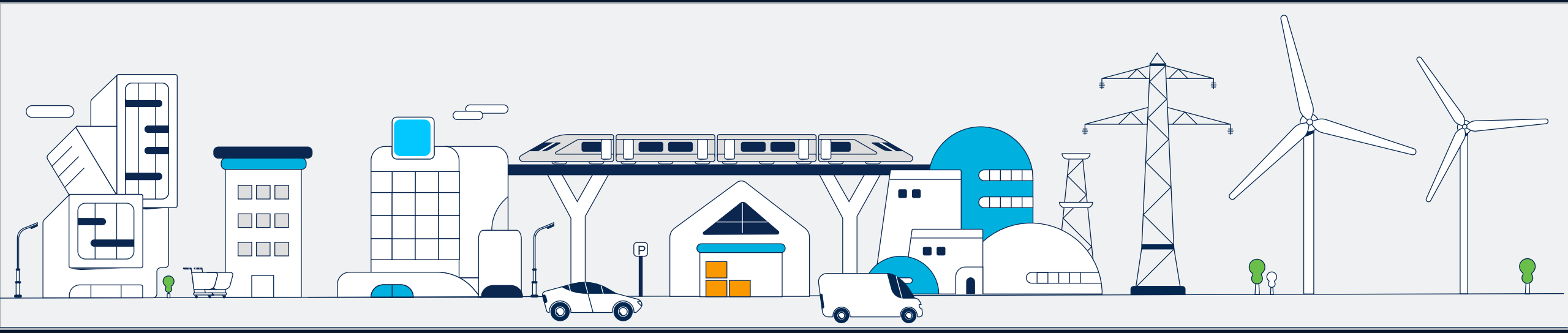
Bez viditelnosti není bezpečnost: Jak chránit industriální sítě před moderními hrozbami

Cisco Cyber Vision

Stanislav Kraus, Cisco SE
stakraus@cisco.com

June 2026

Securing industrial operations starts with OT visibility



Inventory OT assets and their communications

Spot vulnerabilities to patch or mitigate

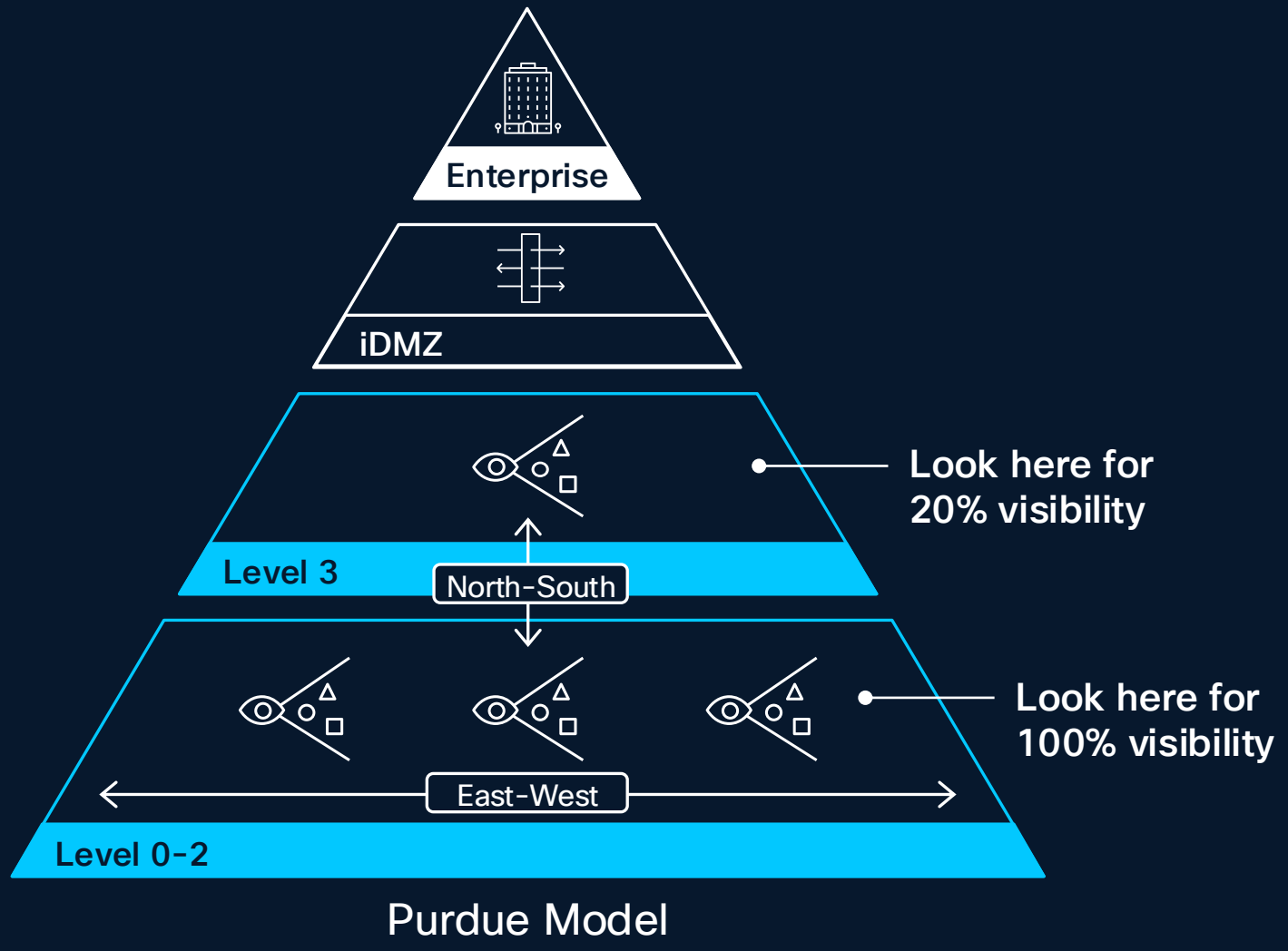
Create access policies to segment networks

Detect bypass or leaks in the IDMZ

Drive compliance and governance

OT context and insights are foundational to securing industrial networks

Security starts with visibility, but where you look matters

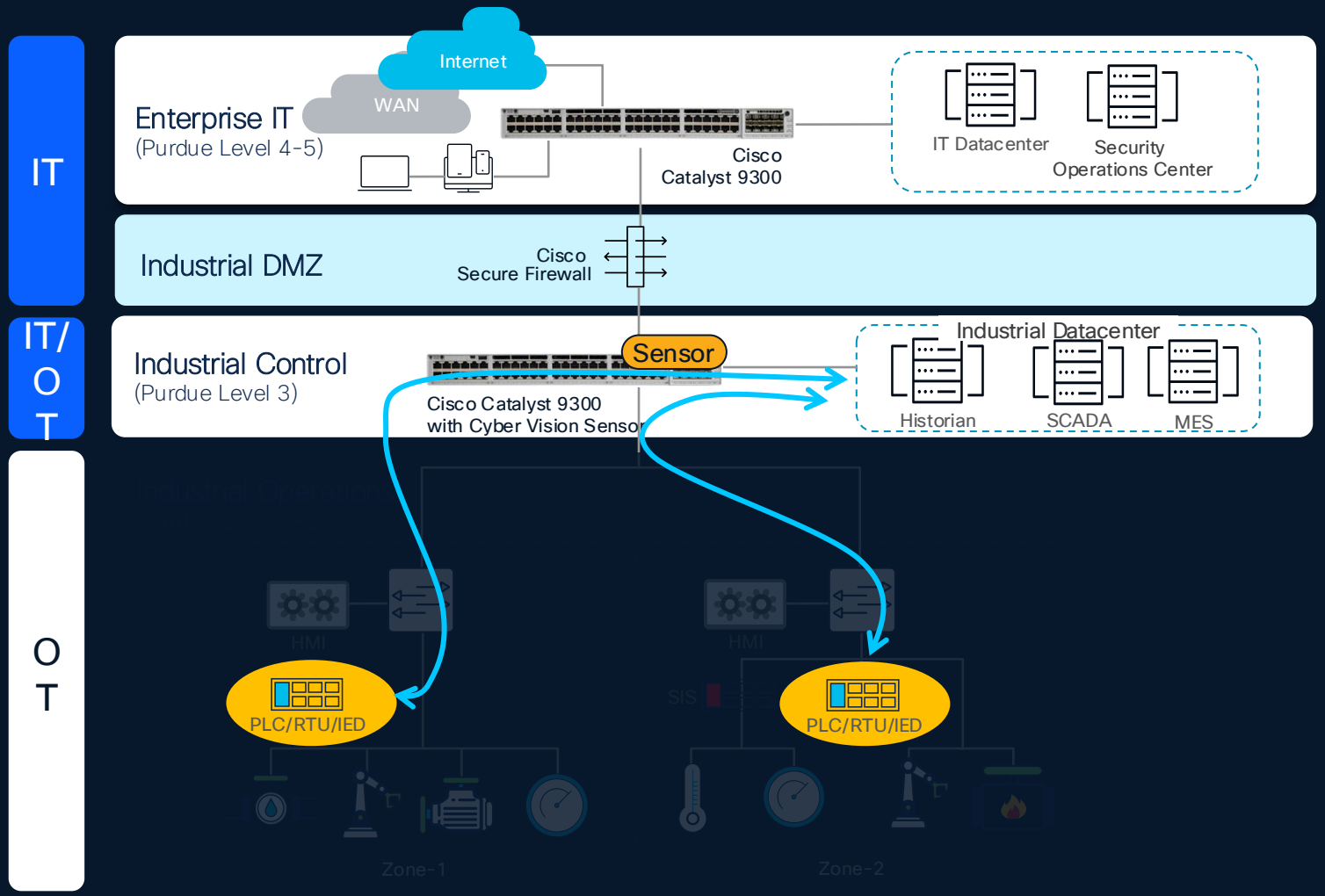


Purdue Model

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

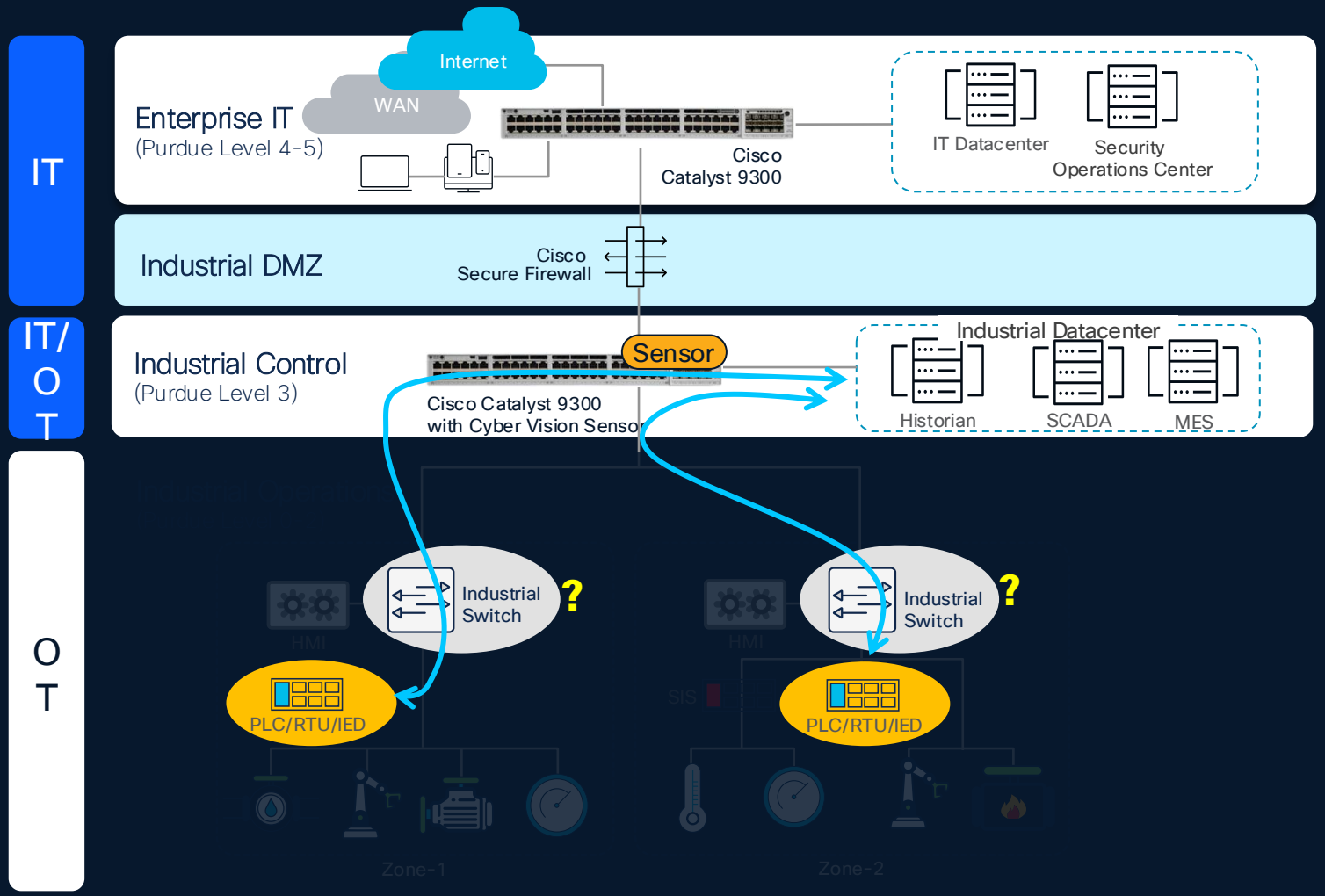
Gaining visibility at the aggregation layer sees very little as most OT traffic is local to the production cell

Your Catalyst switches let you turn on the lights



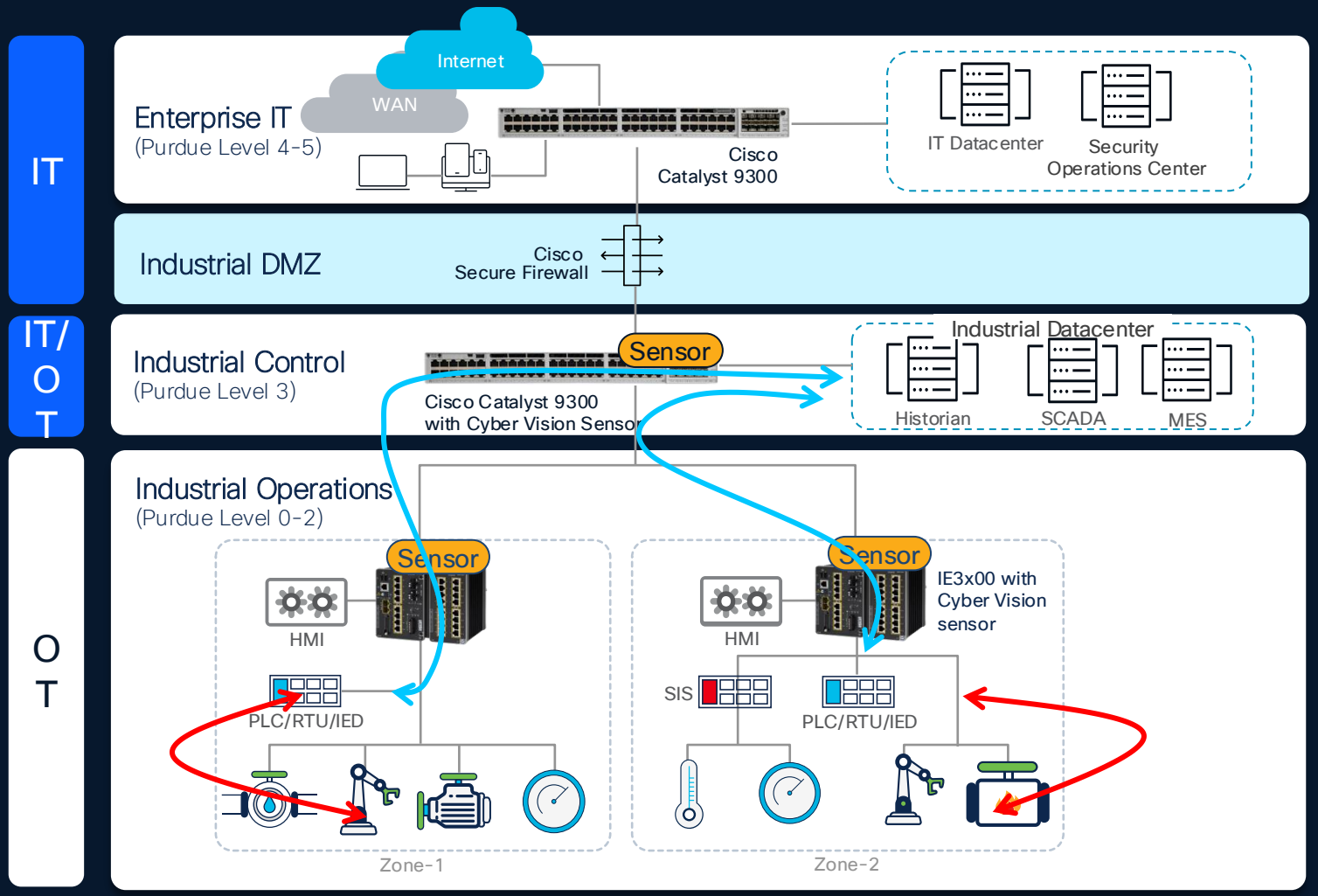
Step-1: Cyber Vision Sensor on Catalyst 9300 and IE9300 in your IDF gives you visibility to North-South communications to identify key assets

Helps you start a dialogue with OT



Step-2: Work with OT to identify the critical industrial switches that connect these key assets

Helps you get a footprint into OT

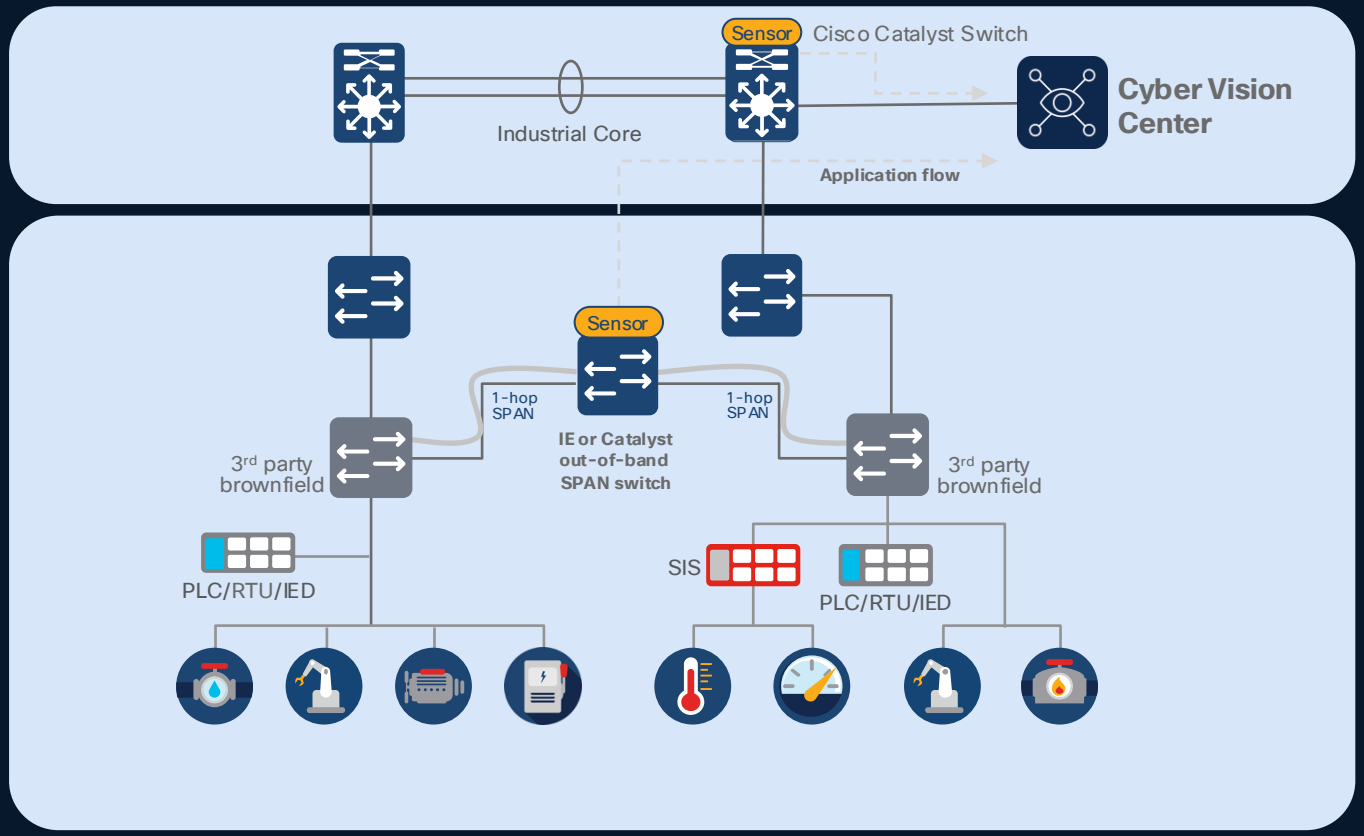


Cyber Vision
is licensed per endpoint,
not per sensor!

Step-3: Replace critical switches with Cisco IE3x00 running Cyber Vision sensor to see the entire OT network

Note: You don't need to replace all industrial switches, just the ones connecting to PLC's

Out-of-Band Collection

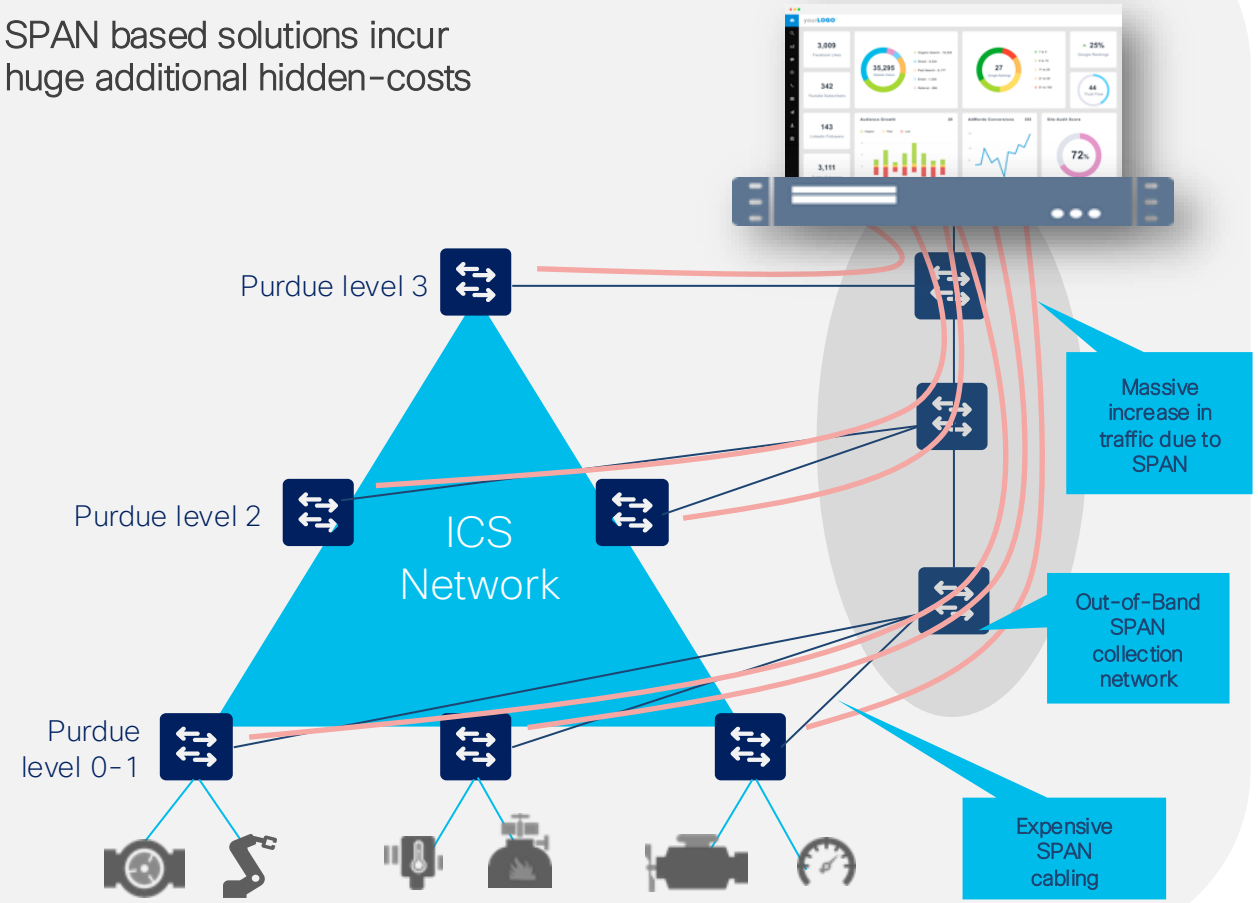


- Embedded Sensor on IE3400 and Catalyst 9300 can be leveraged as out of band sensor
- Enables aggregation of multiple SPAN sessions from across infrastructure
- Environment and scale are deciding factors for IE3400 or Catalyst 9300
- Unlike other solutions that require SPAN all the way to the monitoring appliance, the Cyber Vision solution for brownfield has lower TCO because it leverages the existing network and only requires 1-hop of SPAN traffic

Building a **scalable** IoT/OT security architecture

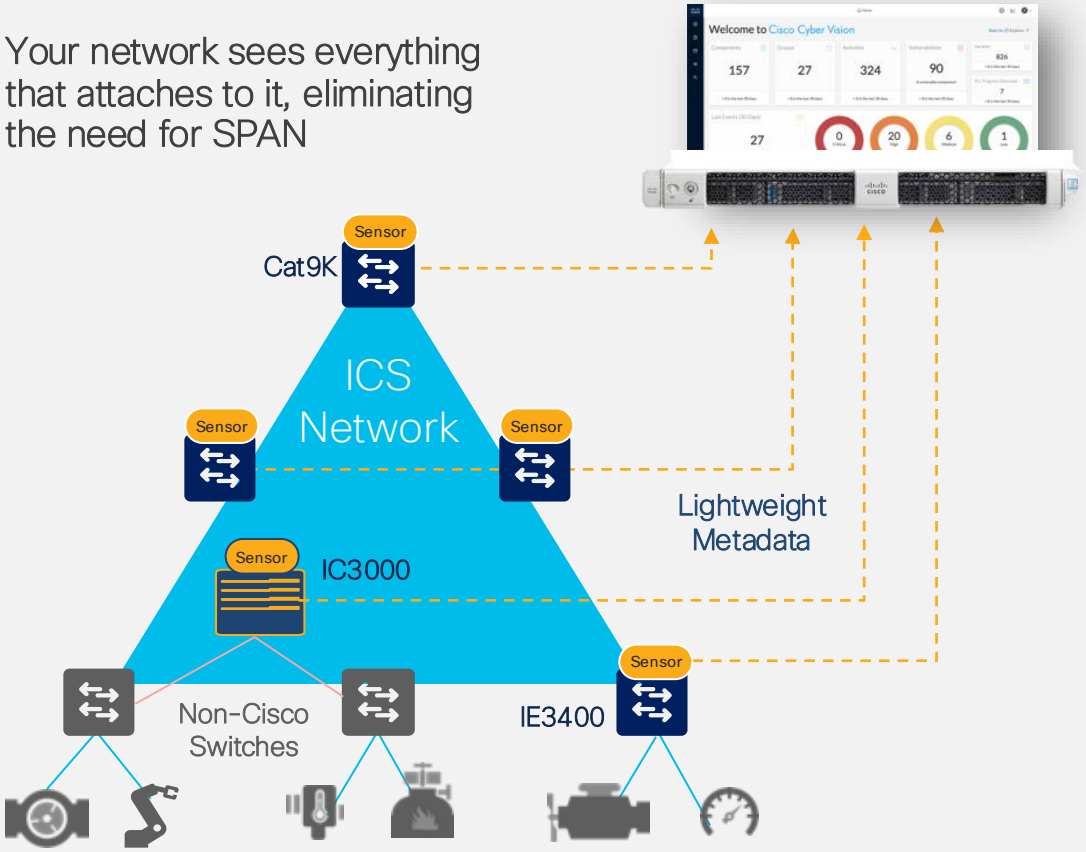
Other solutions

SPAN based solutions incur huge additional hidden-costs



Cisco Cyber Vision

Your network sees everything that attaches to it, eliminating the need for SPAN

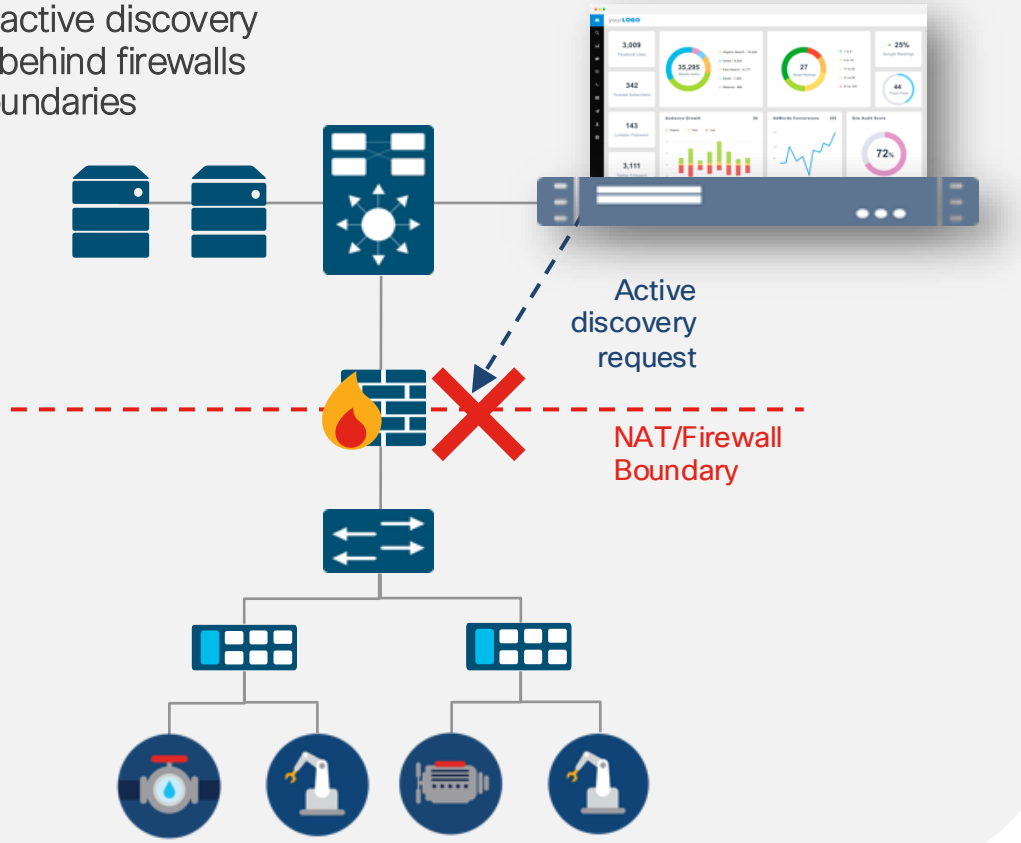


Distributed edge discovery sees more

Silent devices, FWs

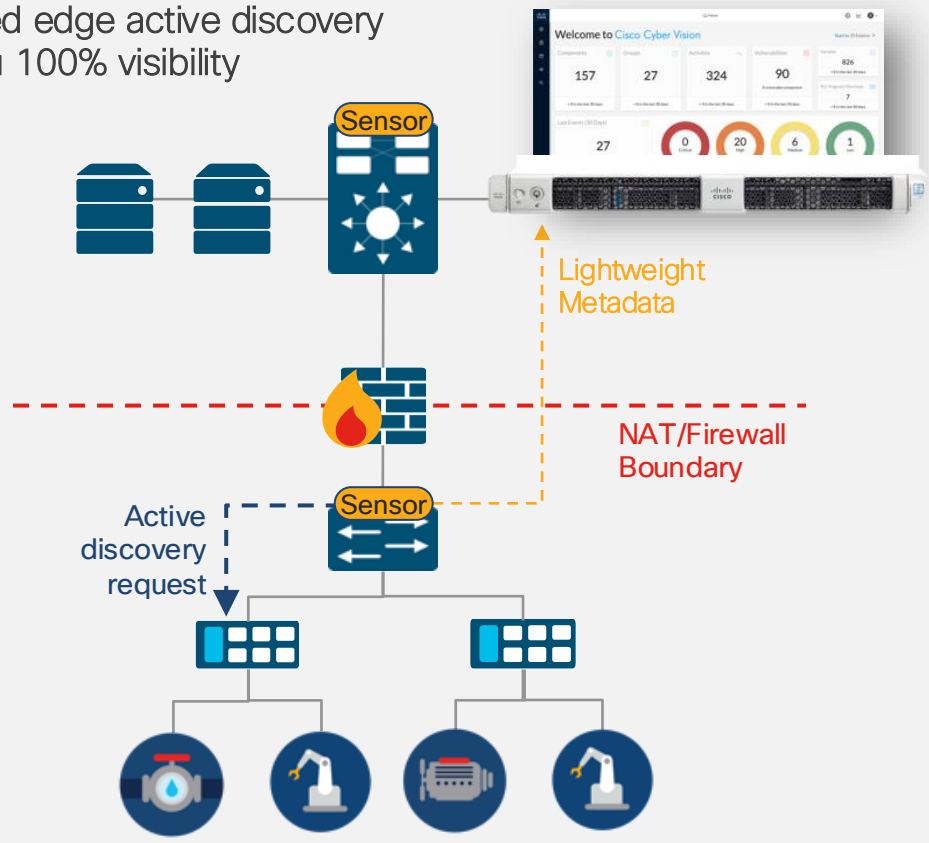
Other solutions

Centralized active discovery cannot see behind firewalls and NAT boundaries



Cisco Cyber Vision

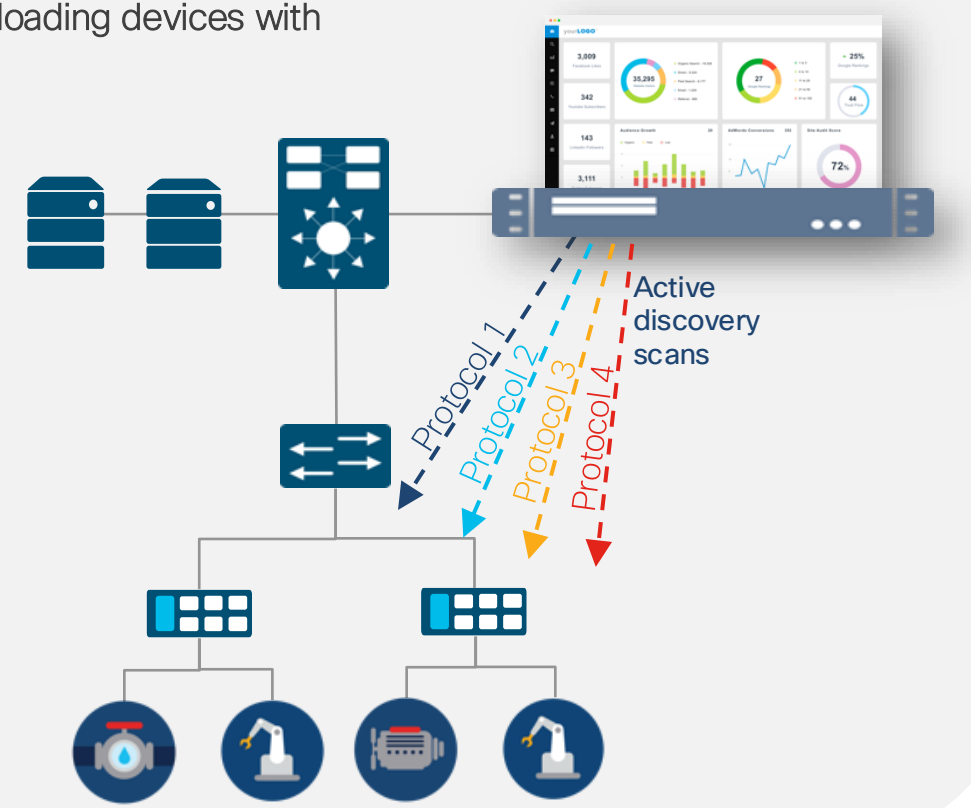
Distributed edge active discovery gives you 100% visibility



Closed-loop control makes active discovery safe

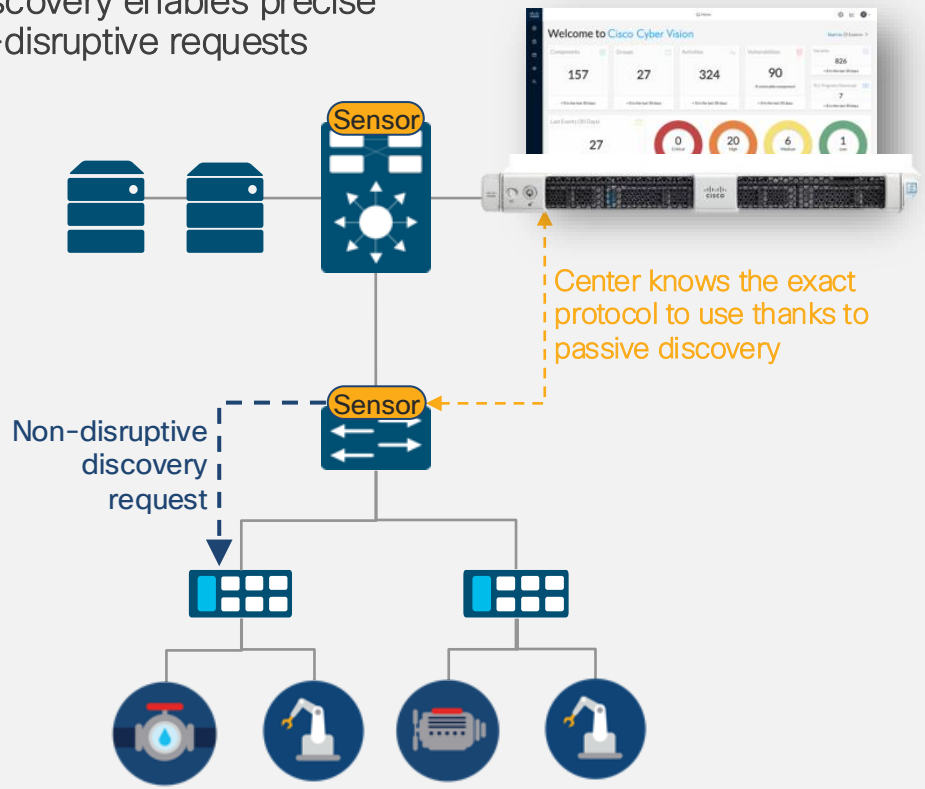
Basic active discovery solutions scan networks overloading devices with ARP requests

Other solutions

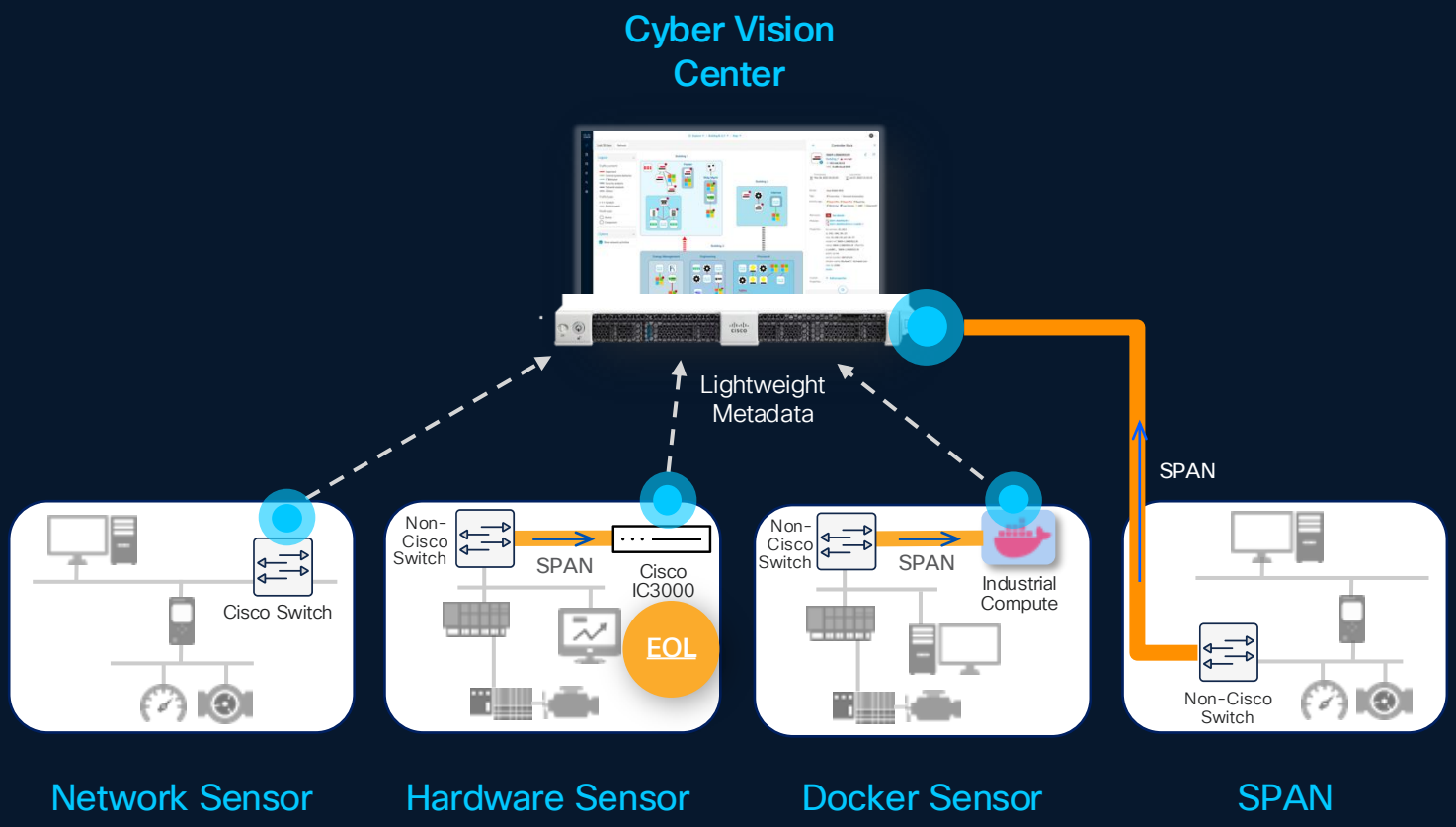


Closed-loop between passive and active discovery enables precise and non-disruptive requests

Cisco Cyber Vision



Flexibility to mix and match sensor types



- 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

Cisco Cyber Vision portfolio

Center

Hardware Appliance

UCS based servers with Hardware RAID

CV-CNTR-M8N
- 32 core CPU
- 192 GB RAM
- 3.2TB or 6.4TB drives

Software Appliance

Virtual Machines

VMWare ESXi OVA

HyperV VHD

Nutanix HAV

Minimum requirements
x386 server CPU, 10 cores
32GB RAM and 1TB SSD
1 or 2 network interfaces

Amazon Web Services

Microsoft Azure

Google Cloud

Minimum requirements
x386 server CPU, 10 cores
32GB RAM and 1TB SSD
1 or 2 network interfaces

Sensors

IE3300, IE3400, and IE3500 Switches

IE3400HD and IE3500HD IP67 Switch

Catalyst IR1101 Cellular Router

Catalyst IR1800 Cellular Router

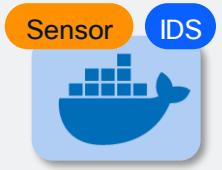
Catalyst IR8300 Multiservice Router

Catalyst IE9300 Rugged Switches

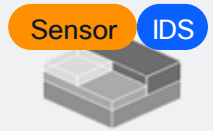
Catalyst 9300/9350/9400 Aggregation Switches

Network Sensors

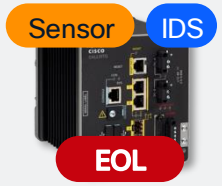
DPI and active discovery built into network-elements eliminating the need for SPAN



x86 or ARM64 Compute running Docker



x86 Compute running VMWare



Cisco IC3000 Industrial Compute

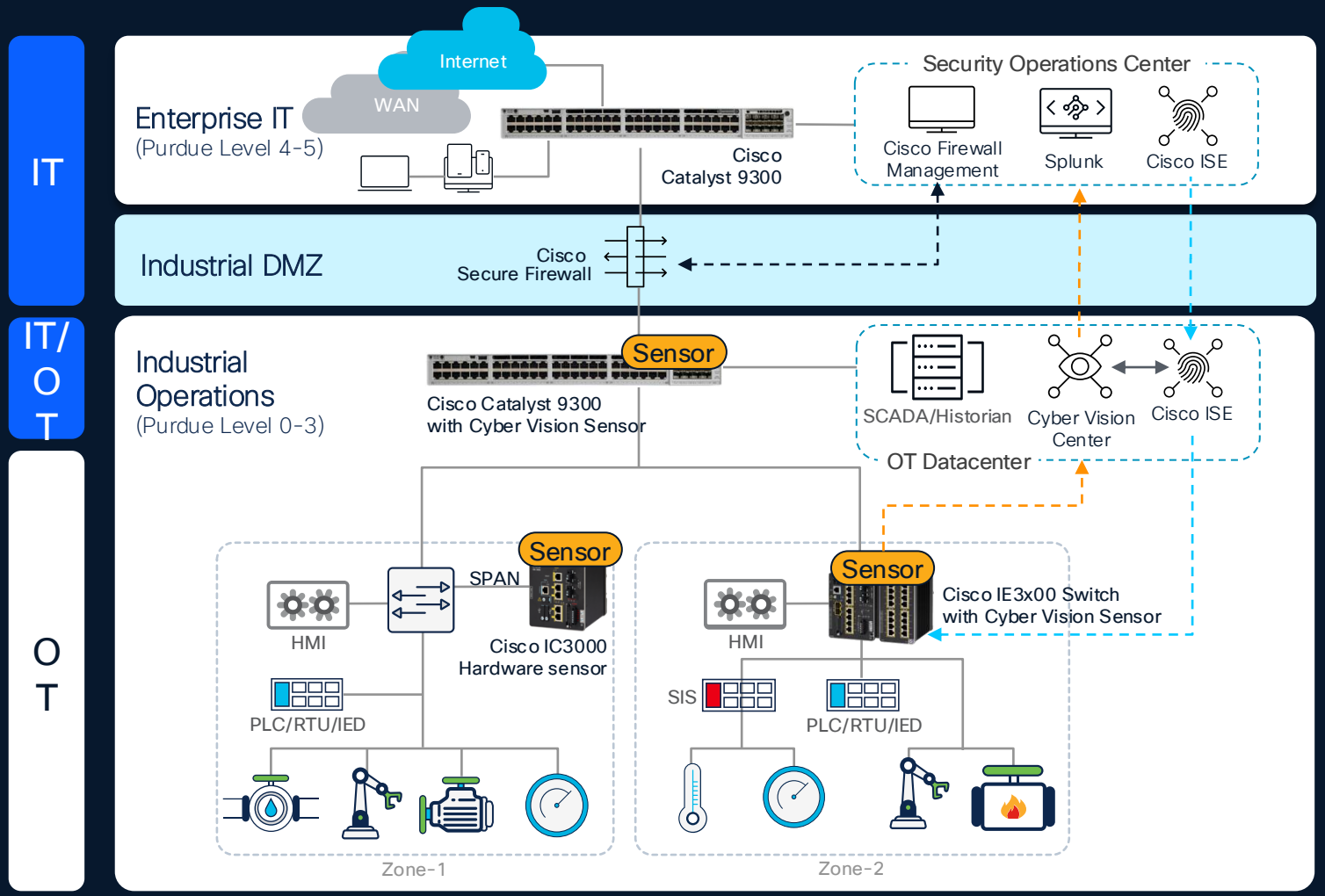
Compute Sensors

DPI and active discovery via SPAN to support brownfield

Cyber Vision VM Sensor – Technical Summary

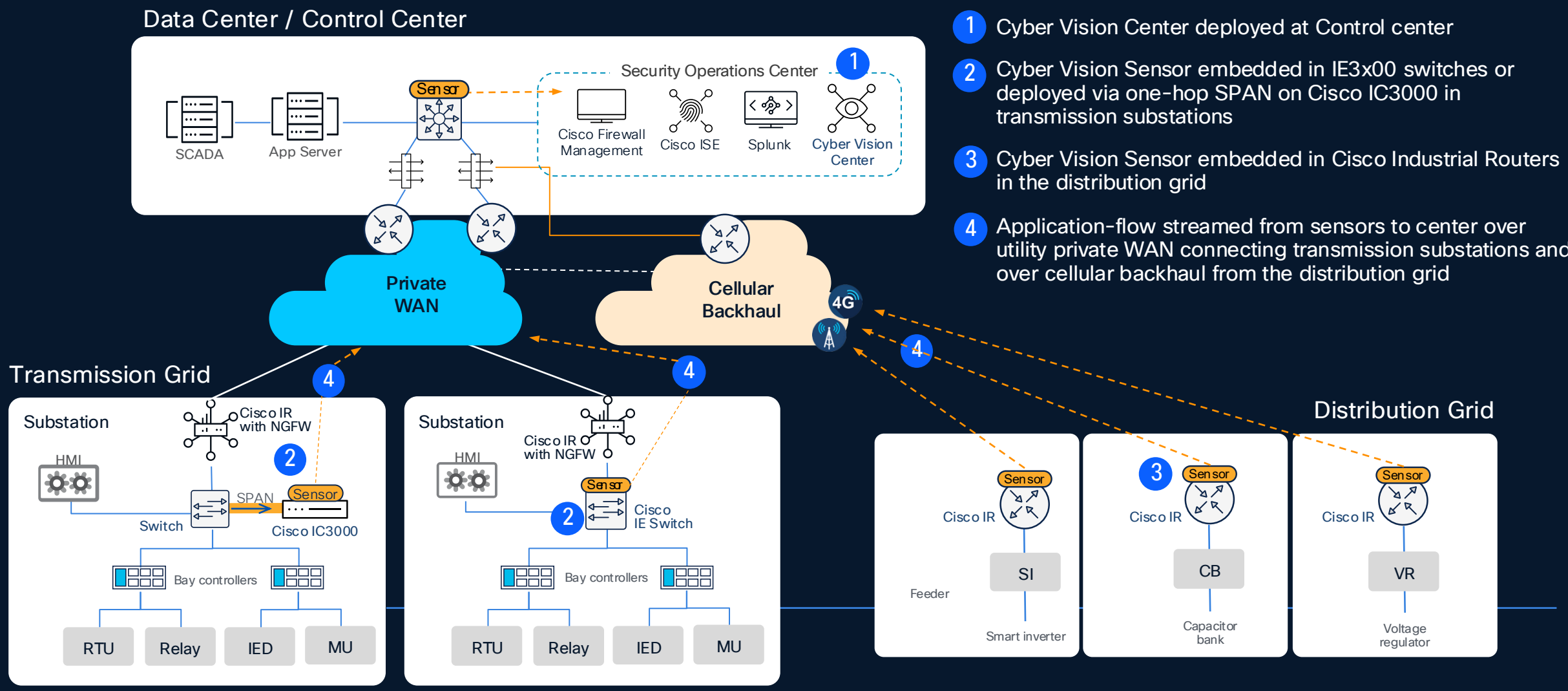
- Compatible with x86-64 devices
  - VMWare v6.x required
  - Minimum of 4GB dedicated memory required (8GB recommended)
  - Minimum of 2 dedicated CPU cores required
- Required network communication
  - Host to CV Center ports: 443/80
  - VM instance to Center ports: 5671, 10514
- Storage allocation of instance will grow over time

Security Architecture in Manufacturing



1. Visibility built into your industrial network to identify OT assets, vulnerabilities, assess security posture and detect threats
2. Prevent propagation of threats with industrial firewall IDMZ and network micro-segmentation
3. Enable SOC to investigate industrial threats with enrichment and orchestrate response with playbooks

Security Architecture in Electric Utilities



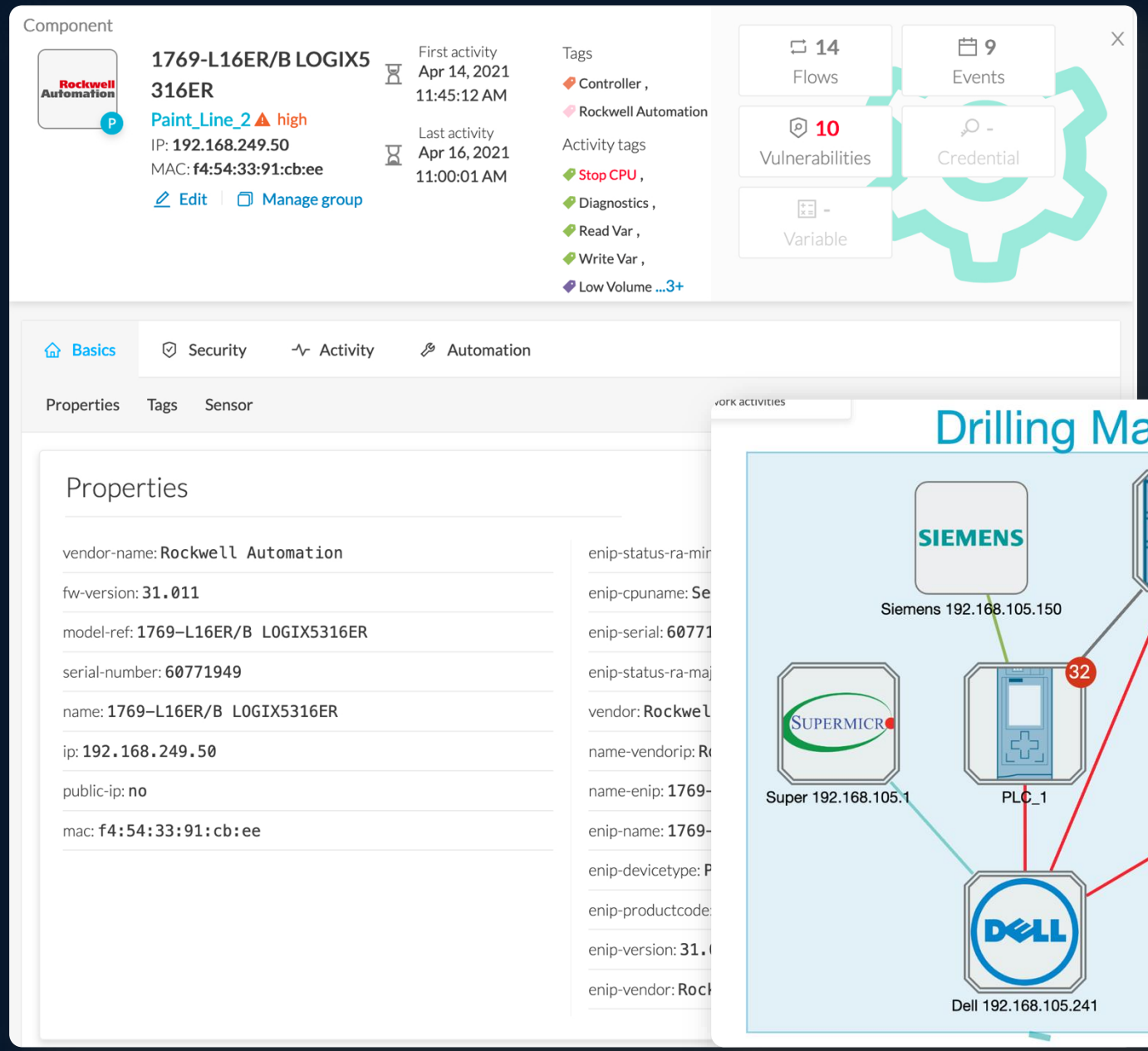
1. Cyber Vision Center deployed at Control center
2. Cyber Vision Sensor embedded in IE3x00 switches or deployed via one-hop SPAN on Cisco IC3000 in transmission substations
3. Cyber Vision Sensor embedded in Cisco Industrial Routers in the distribution grid
4. Application-flow streamed from sensors to center over utility private WAN connecting transmission substations and over cellular backhaul from the distribution grid

Key Features

Cyber Vision

Visibility into connected industrial assets

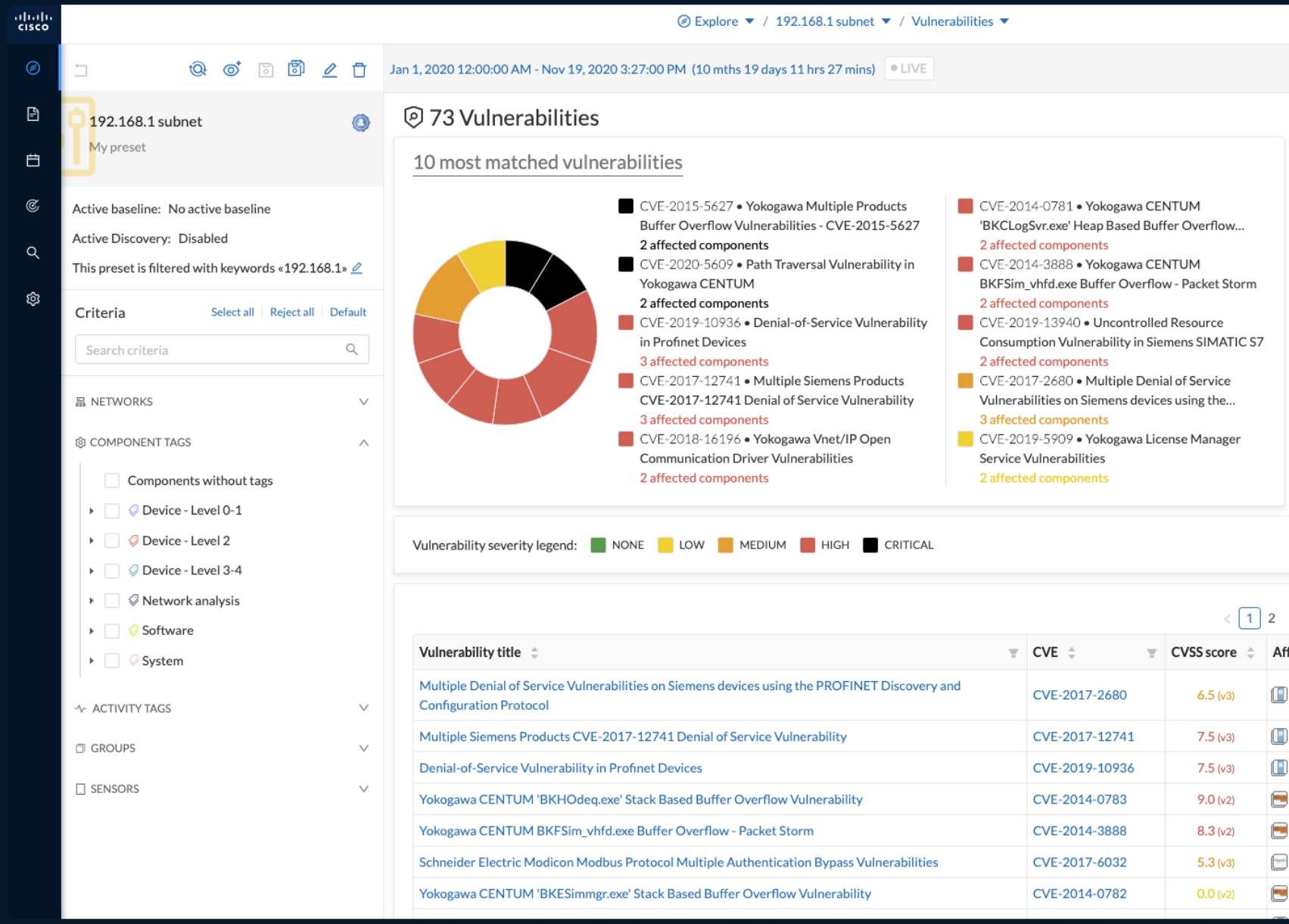
Understand the identity of all assets in the environment gain insight into network communications



Cyber Vision

Identify & Track Vulnerabilities

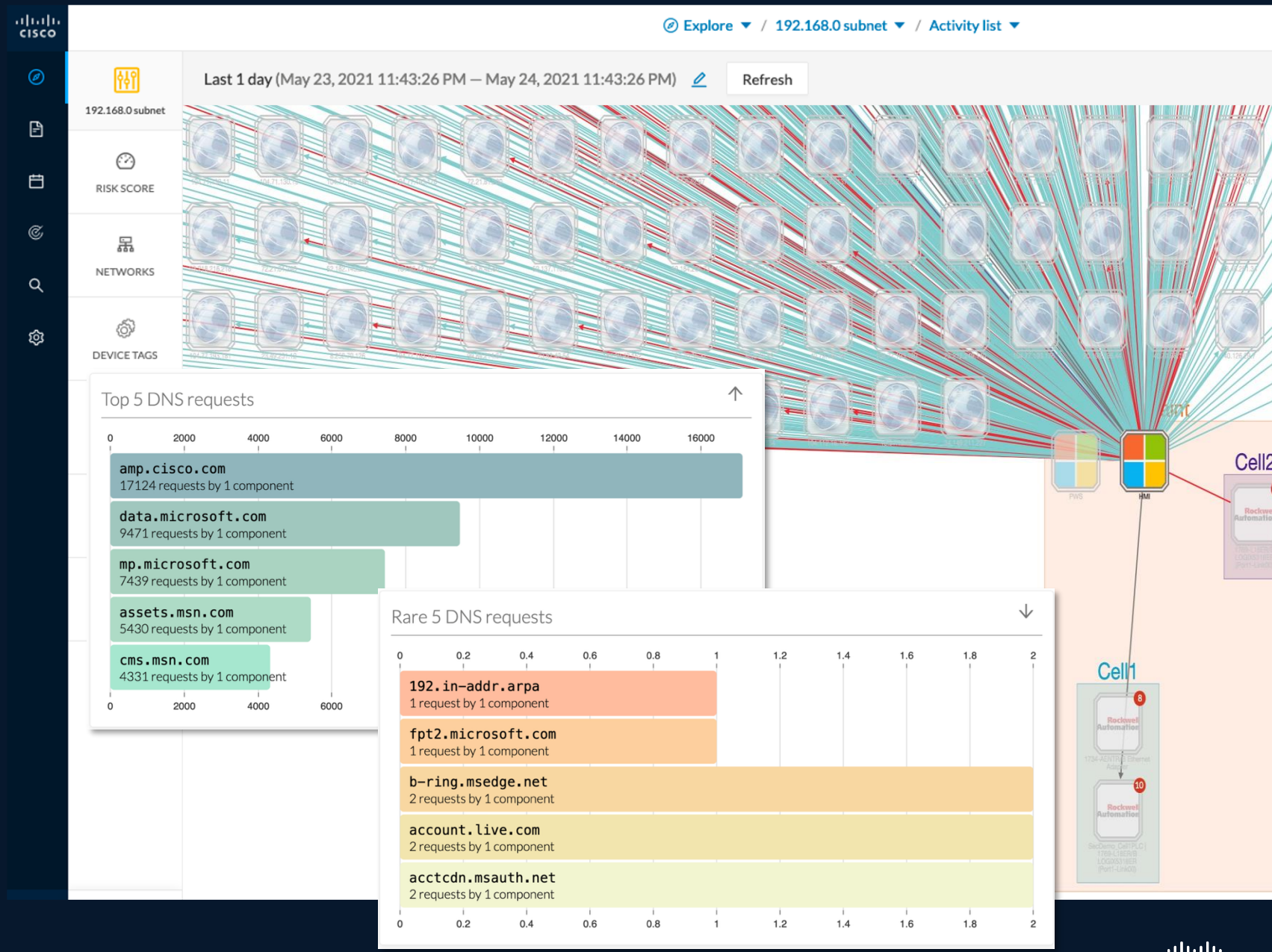
Identify known asset vulnerabilities so you can patch or protect them before they are exploited



Cyber Vision

Identify & Stop iDMZ Leaks

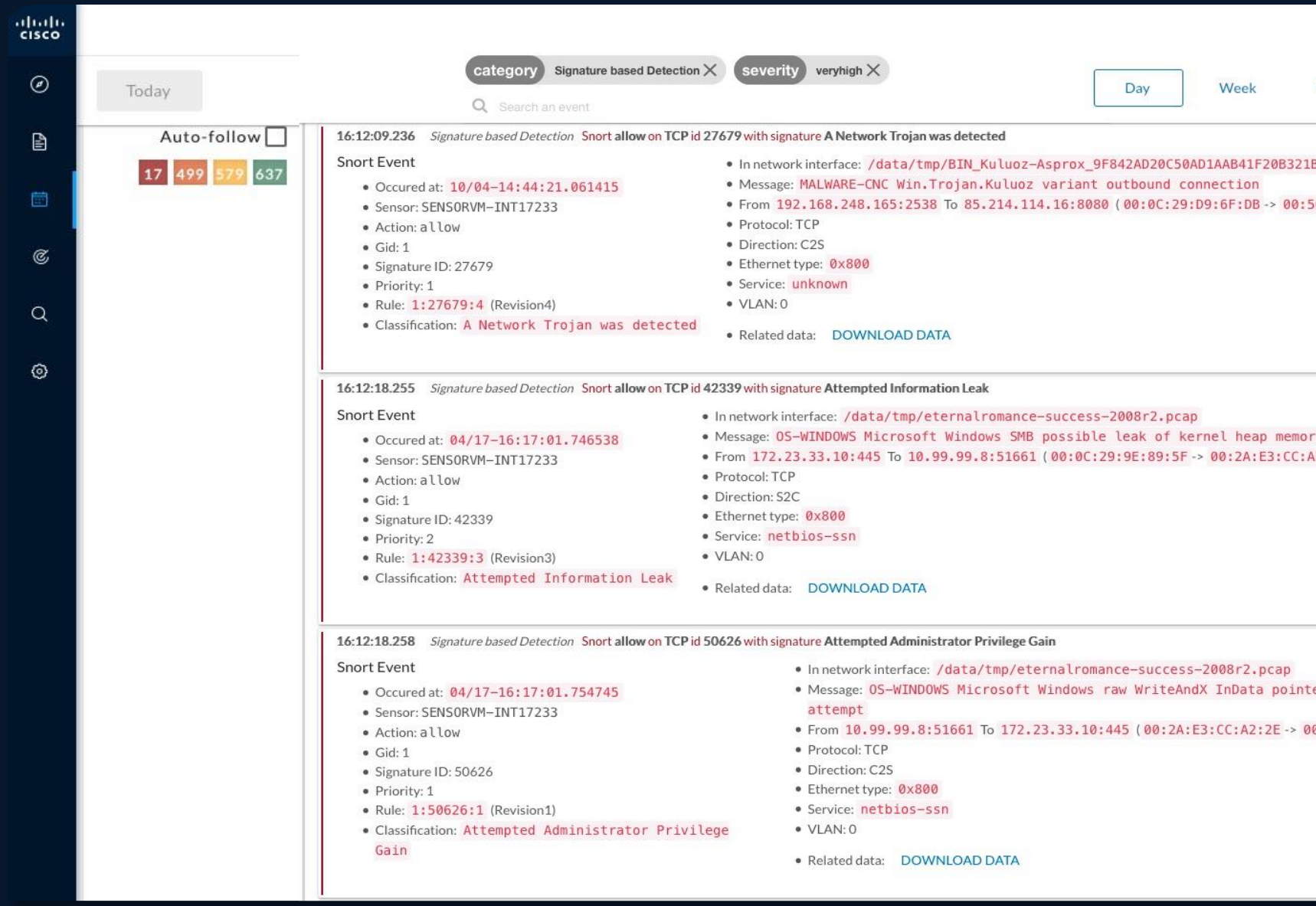
Filter subnets to identify traffic to external networks and stop unauthorized leaks past the DMZ



Cyber Vision

Detect Malicious Intrusions

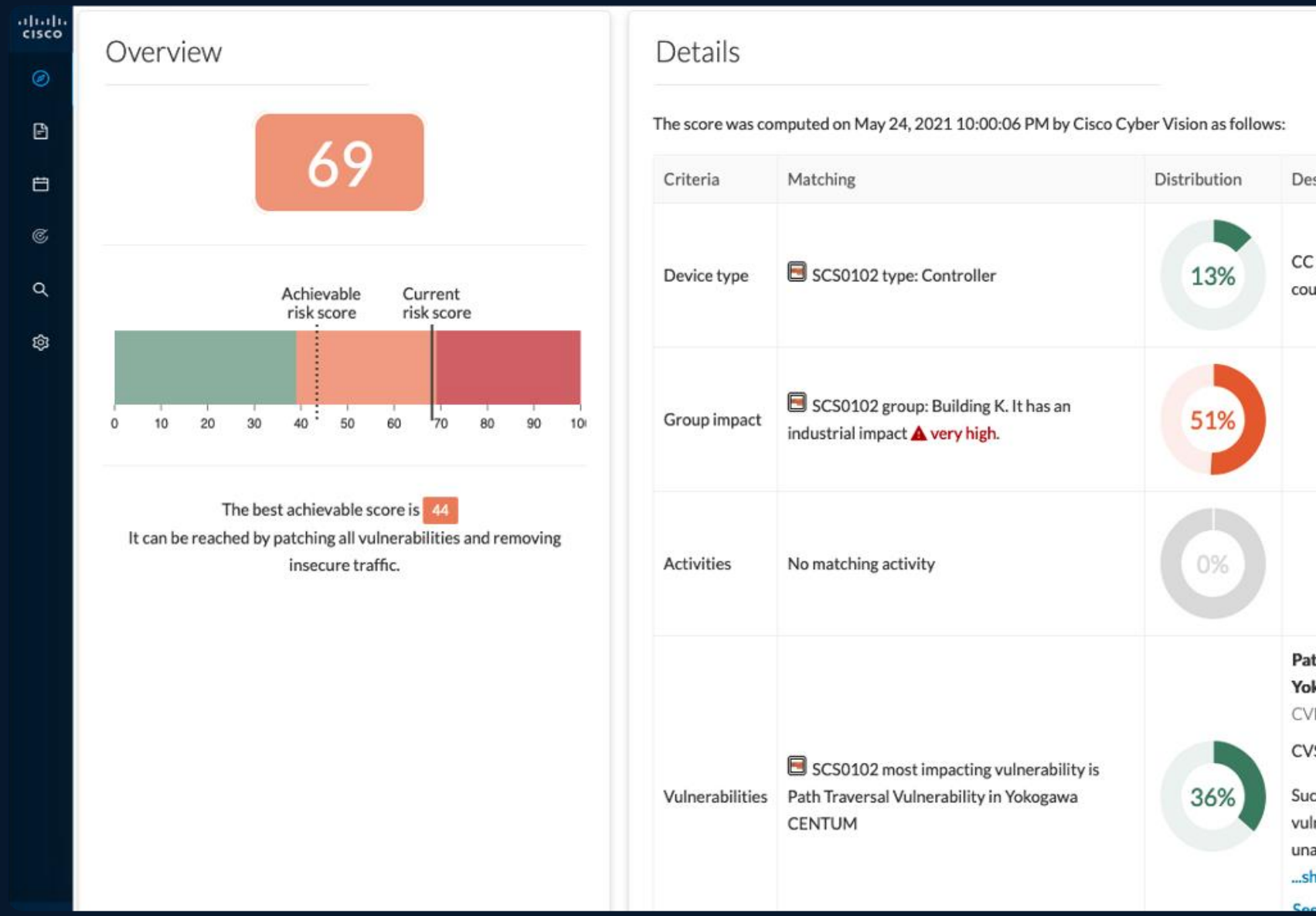
Detect malicious intrusions with Snort IDS and Talos threat intelligence



Cyber Vision

Track your Risk Exposure

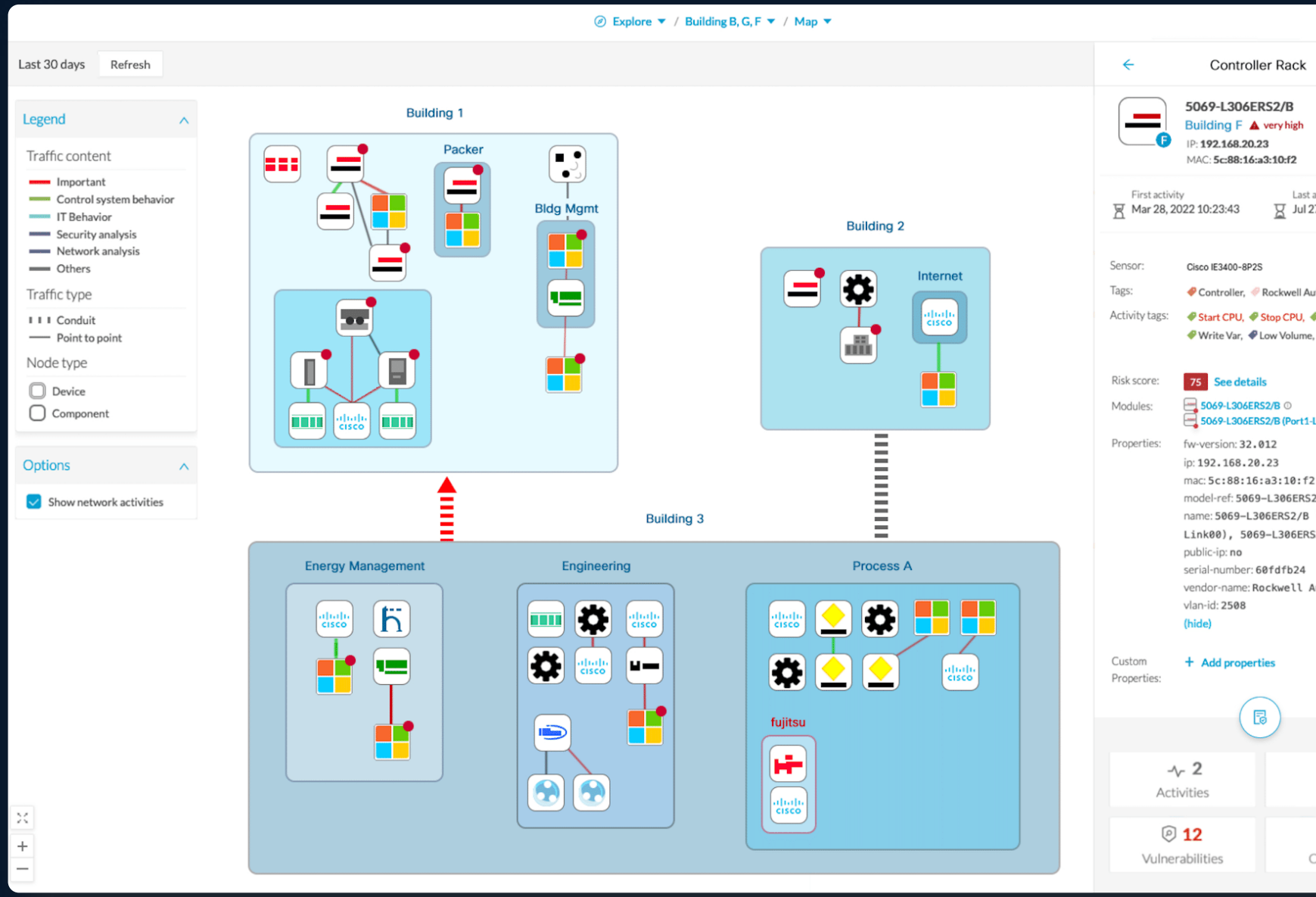
Asset risk scoring based on impact and likelihood to help you improve compliance



Cyber Vision

IEC-62443 segmentation made simple

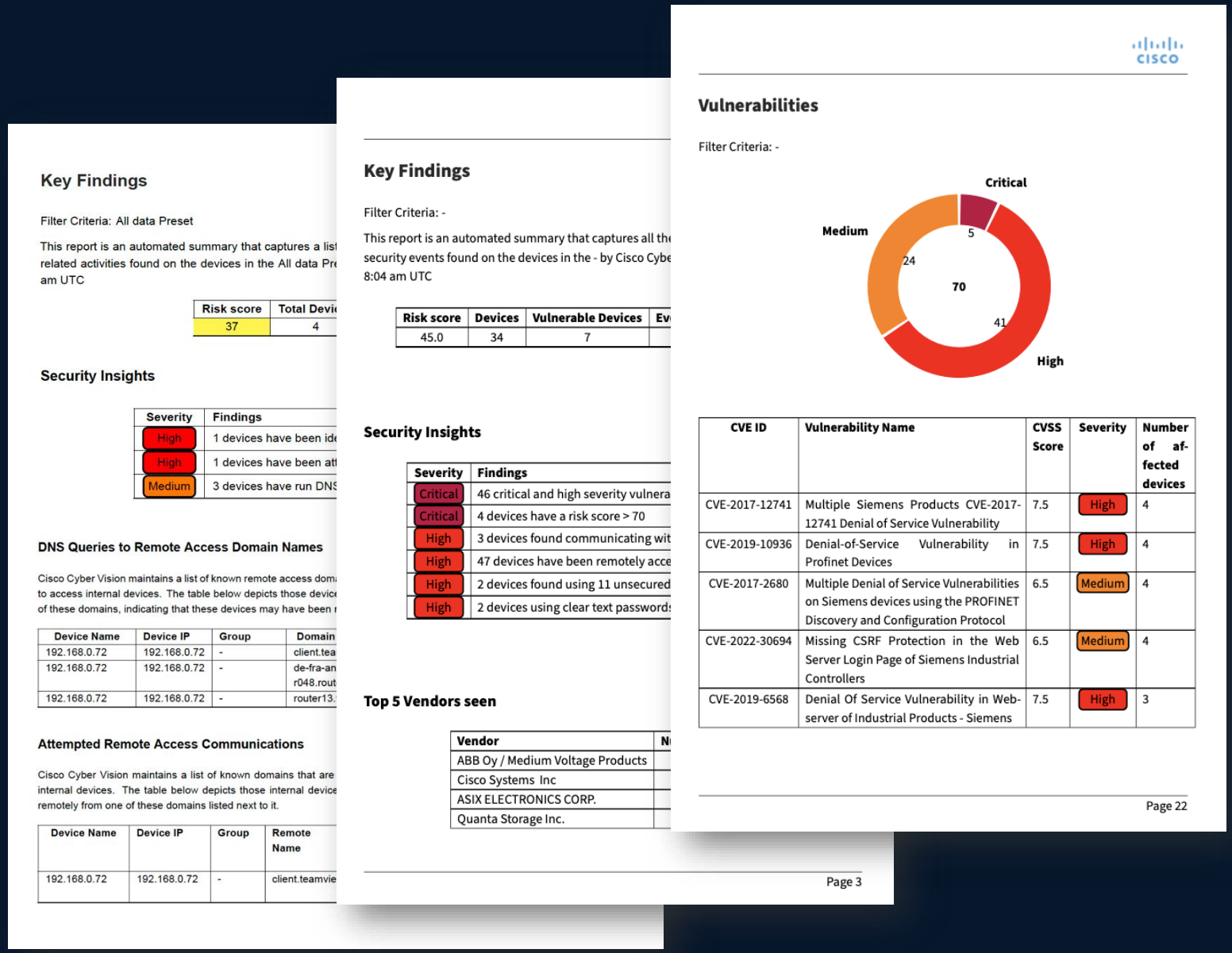
- Group OT assets into zones
- Visualize conduits
- Identify traffic violations
- Share context with other platforms to enforce segmentation
- Changes to groups automatically update access policies



Cyber Vision

Measure progress with reports

Track risk management improvements and show progress to management with historical reports



Key Findings

Filter Criteria: All data Preset

This report is an automated summary that captures a list related activities found on the devices in the All data Pr am UTC

Risk score	Total Devi
37	4

Security Insights

Severity	Findings
High	1 devices have been id
High	1 devices have been at
Medium	3 devices have run DNS

DNS Queries to Remote Access Domain Names

Cisco Cyber Vision maintains a list of known remote access dom to access internal devices. The table below depicts those devic of these domains, indicating that these devices may have been

Device Name	Device IP	Group	Domain
192.168.0.72	192.168.0.72	-	client.tea
192.168.0.72	192.168.0.72	-	de-fra-an r048.rout
192.168.0.72	192.168.0.72	-	router13.

Attempted Remote Access Communications

Cisco Cyber Vision maintains a list of known domains that are internal devices. The table below depicts those internal devic remotely from one of these domains listed next to it.

Device Name	Device IP	Group	Remote Name
192.168.0.72	192.168.0.72	-	client.teamvie

Key Findings

Filter Criteria: -

This report is an automated summary that captures all th security events found on the devices in the - by Cisco Cybe 8:04 am UTC

Risk score	Devices	Vulnerable Devices	Ev
45.0	34	7	

Security Insights

Severity	Findings
Critical	46 critical and high severity vulnera
Critical	4 devices have a risk score > 70
High	3 devices found communicating wit
High	47 devices have been remotely acce
High	2 devices found using 11 unsecured
High	2 devices using clear text password

Top 5 Vendors seen

Vendor	N
ABB Oy / Medium Voltage Products	
Cisco Systems Inc	
ASIX ELECTRONICS CORP.	
Quanta Storage Inc.	

Page 3

Vulnerabilities

Filter Criteria: -

CVE ID	Vulnerability Name	CVSS Score	Severity	Number of affected devices
CVE-2017-12741	Multiple Siemens Products CVE-2017-12741 Denial of Service Vulnerability	7.5	High	4
CVE-2019-10936	Denial-of-Service Vulnerability in Profinet Devices	7.5	High	4
CVE-2017-2680	Multiple Denial of Service Vulnerabilities on Siemens devices using the PROFINET Discovery and Configuration Protocol	6.5	Medium	4
CVE-2022-30694	Missing CSRF Protection in the Web Server Login Page of Siemens Industrial Controllers	6.5	Medium	4
CVE-2019-6568	Denial Of Service Vulnerability in Web-server of Industrial Products - Siemens	7.5	High	3

Page 22

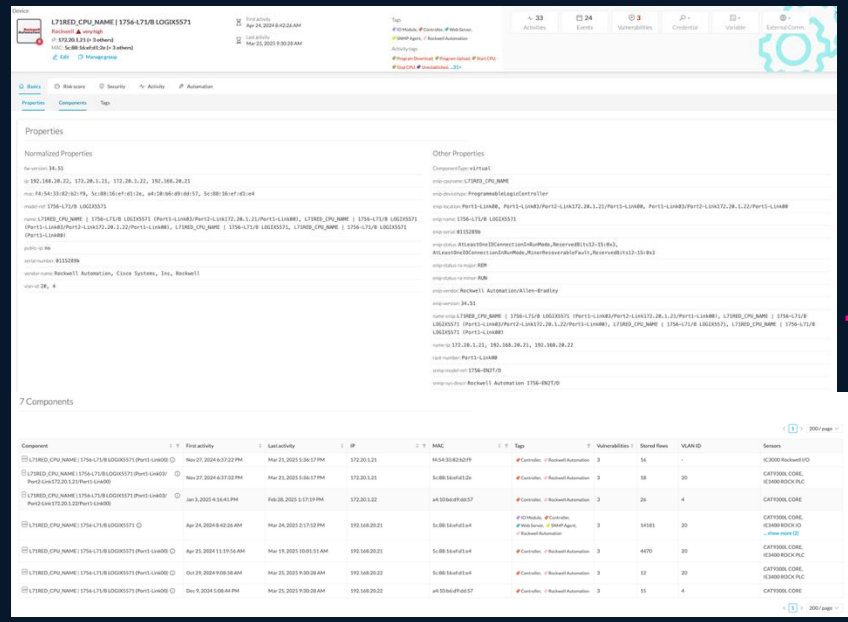
New Features

Cyber Vision New UI

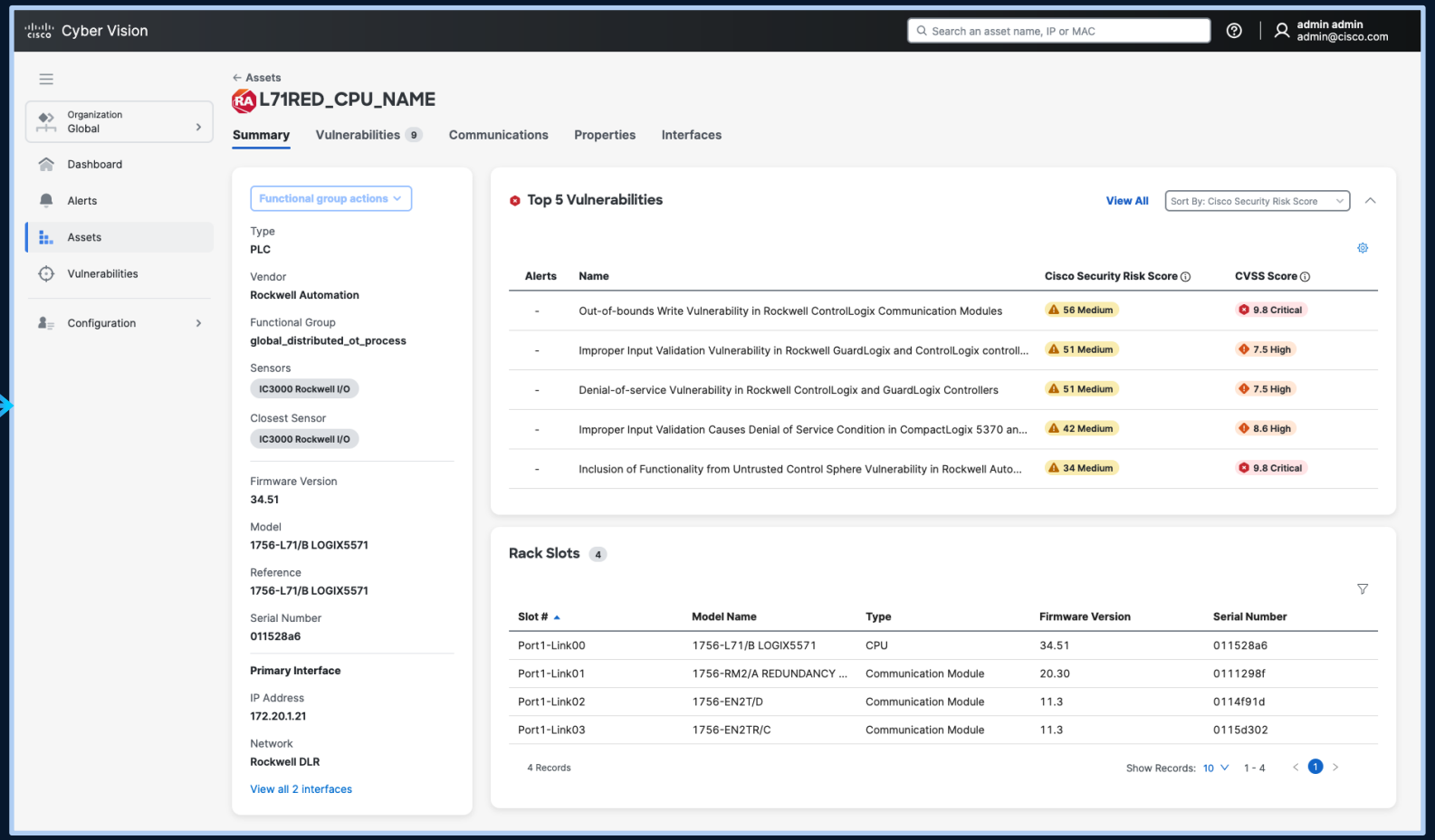
- **Why are we building a new UI?**
  - Focus on insights to reduce Time to Value
  - Asset centric approach to data
  - Simplified UI/UX to ease customer adoption
  - Align with other Cisco products (Magnetic UI)

- **How can I access this new UI?**
  - Mode switch button on the UI's top right
  - Available from release 5.3+ (before in Beta hidden parameter)

Asset details – Focus on what matters

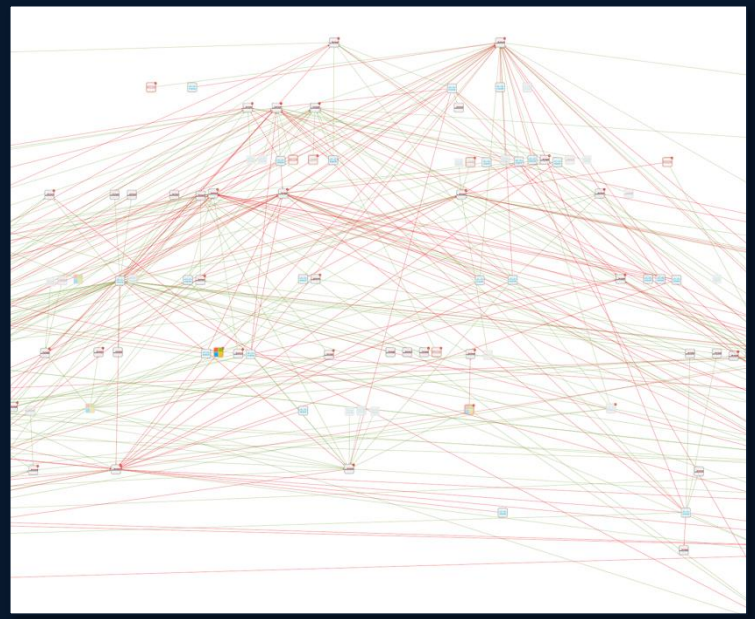


Devices can be made off multiple components and seen through different routers / firewalls which creates complexity

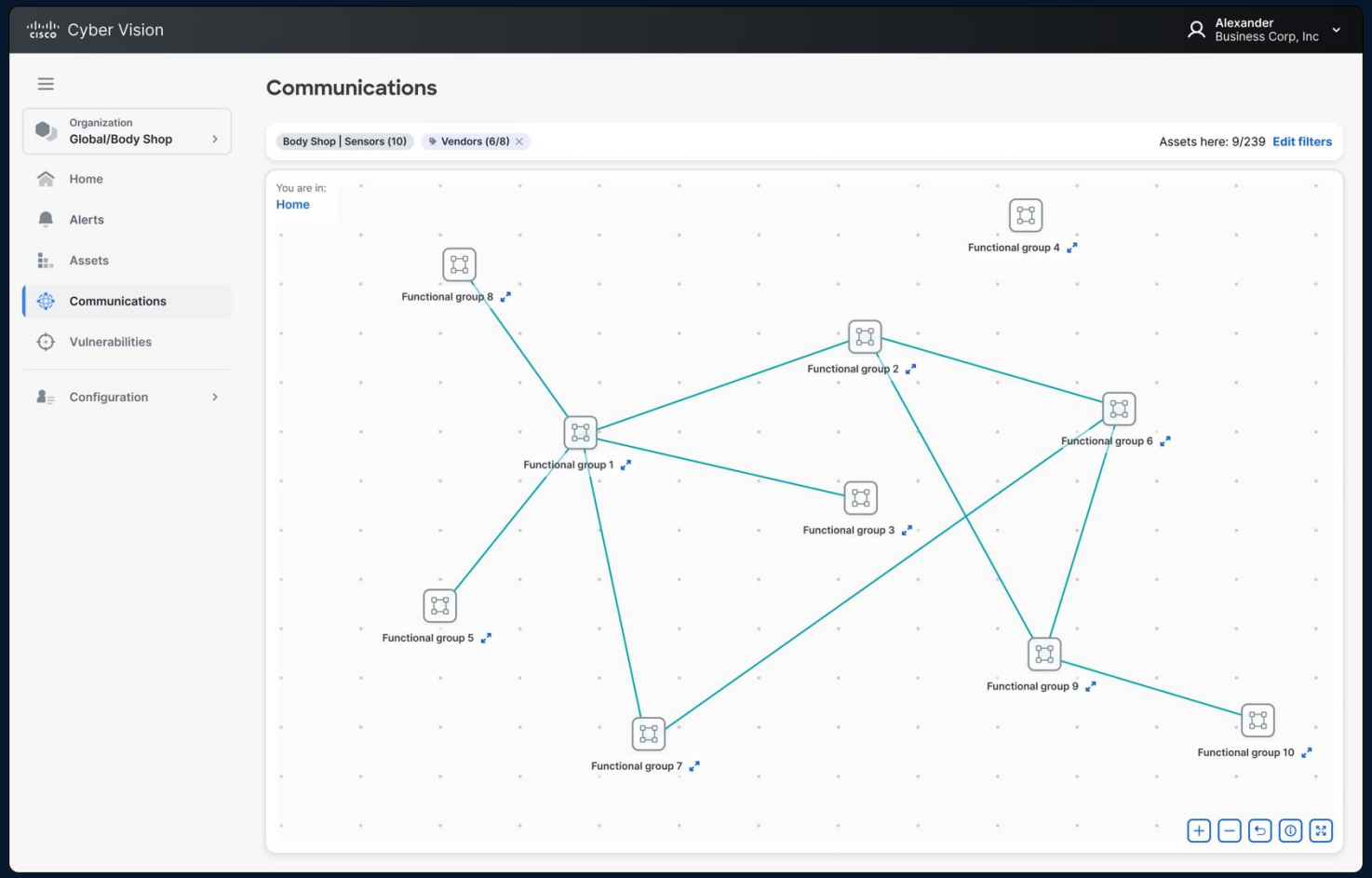


New UI only surface meaningful information

Introducing AI-driven asset auto-grouping



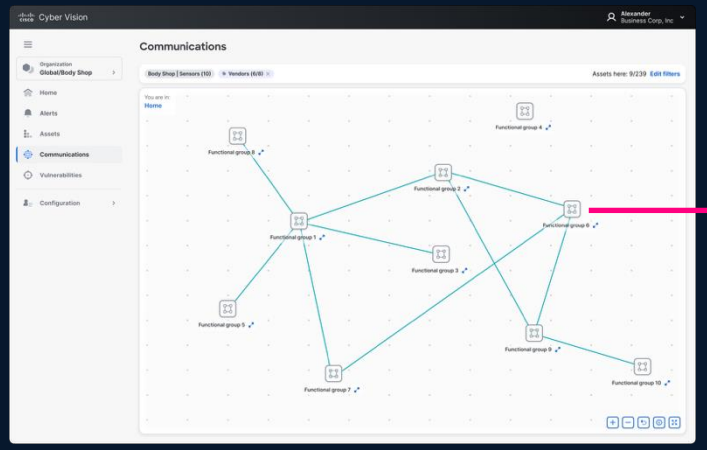
OT asset inventory projects highlight flat, unsegmented networks



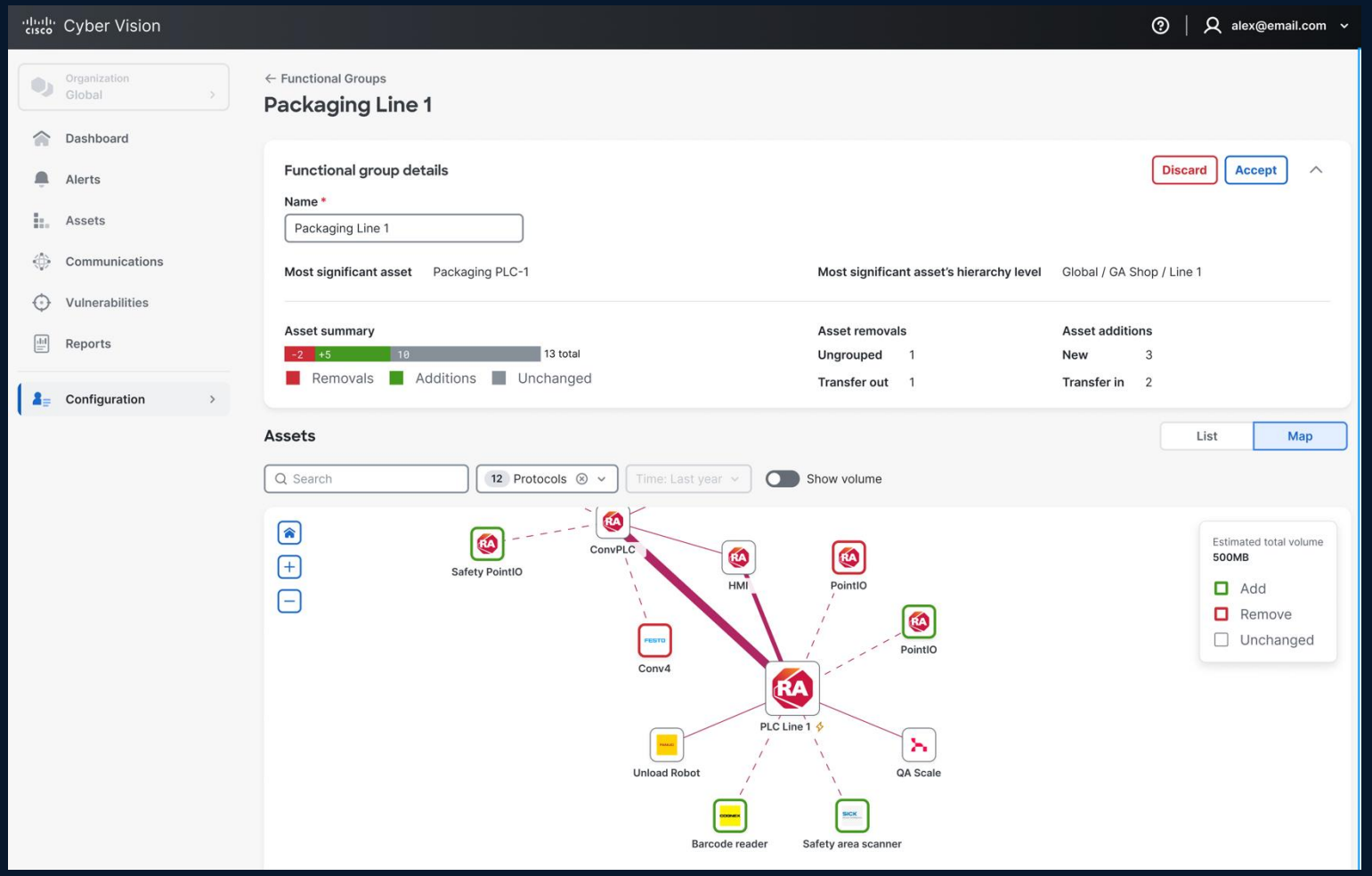
Cisco Cyber Vision ML-driven auto-grouping automatically creates security zones to drive network segmentation using Firewalls or NAC

Introducing AI-driven asset auto-grouping

Group-to-group overview



Detailed view of assets within a group



Role based access control on presets

Goals:

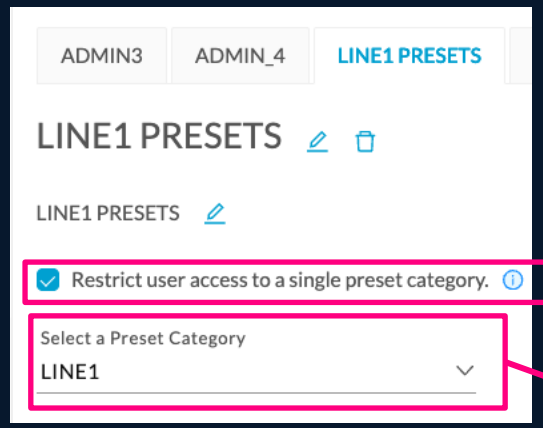
- Limit users access to a list of presets

Description:

- Allow Cyber Vision administrator to give read only

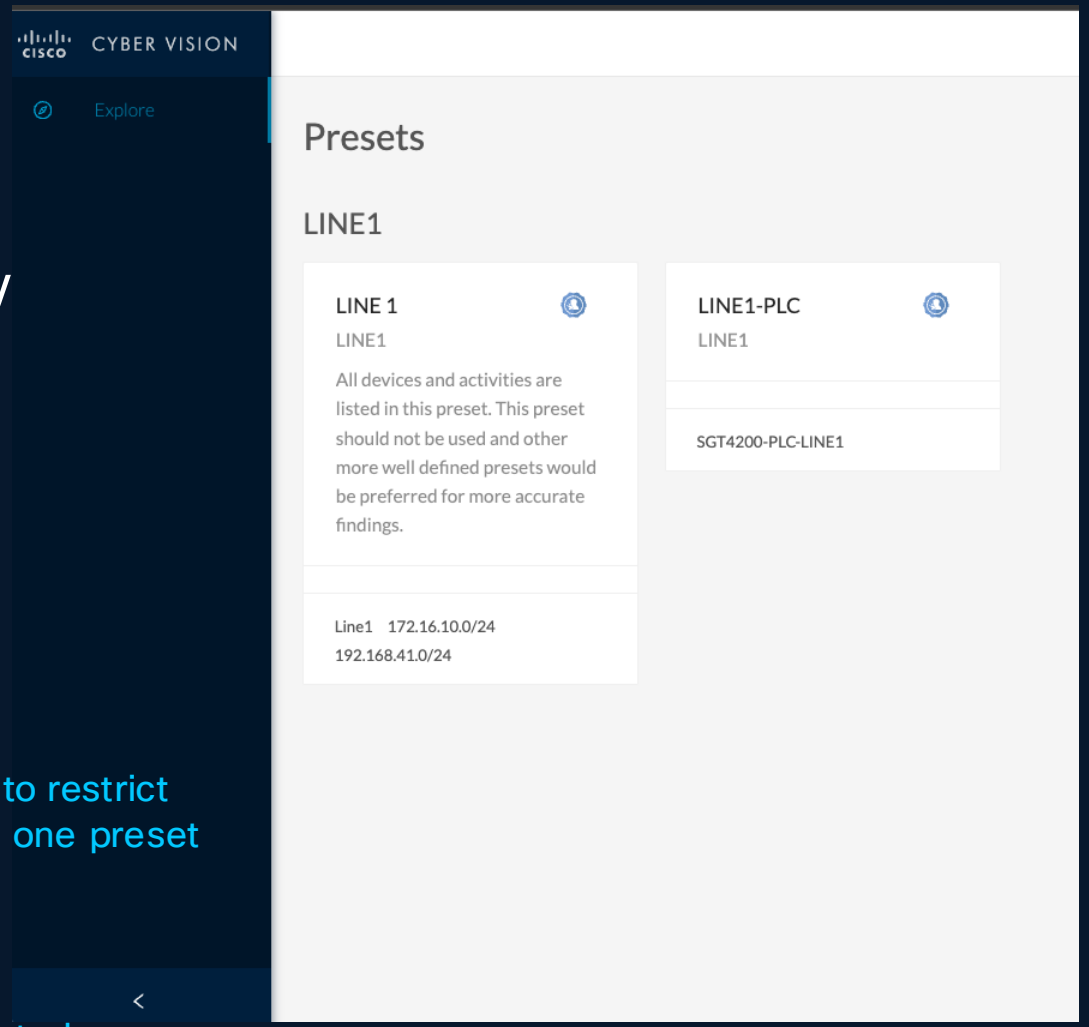
Limitation:

- Limited to Explore Mode
- You can still jump from one device to another



New feature to restrict navigation to one preset category

Category selected



Sensor GPS coordinates

Goals:

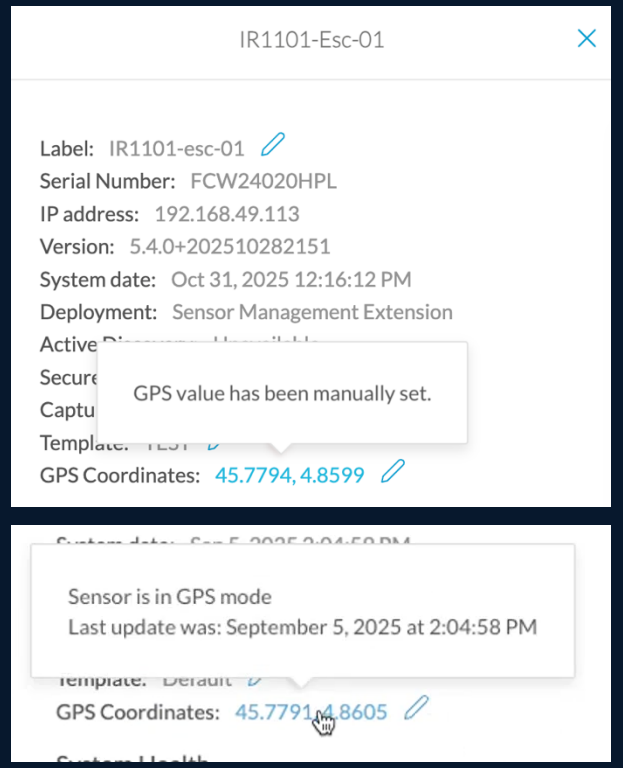
- Add GPS coordinates to sensor/platform

Description:

- Cyber Vision can now store and display GPS coordinates for sensors
  - GPS coordinates can be manually set
  - Or for routers with GPS module, they can be received from platforms
- Available through REST API

Limitation:

- GPS mode, limited to router with GPS module (IR1101, IR1800)



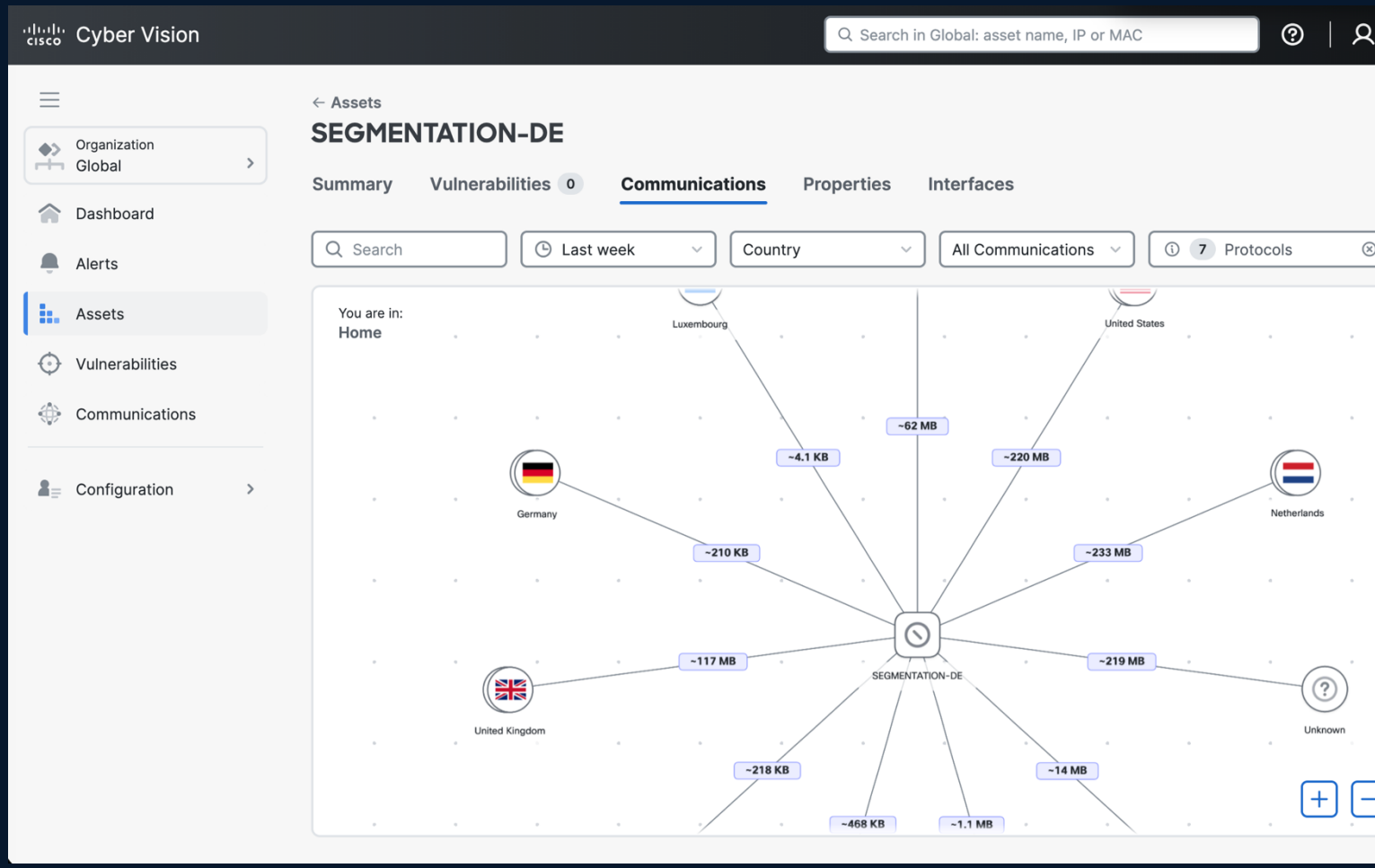
External communication tracking enhancements

New IP-to-Country Geolocation Mapping

Quickly map all communication flows
Map external connections to specific countries for threat context

Gain control over all communication
Tracks and visualizes communication between OT/IT assets and external public IP addresses

Geolocationwith new Intelligence Feed
Visualize IP-to-Country and Autonomous System Number (ASN) - Requires CVSM

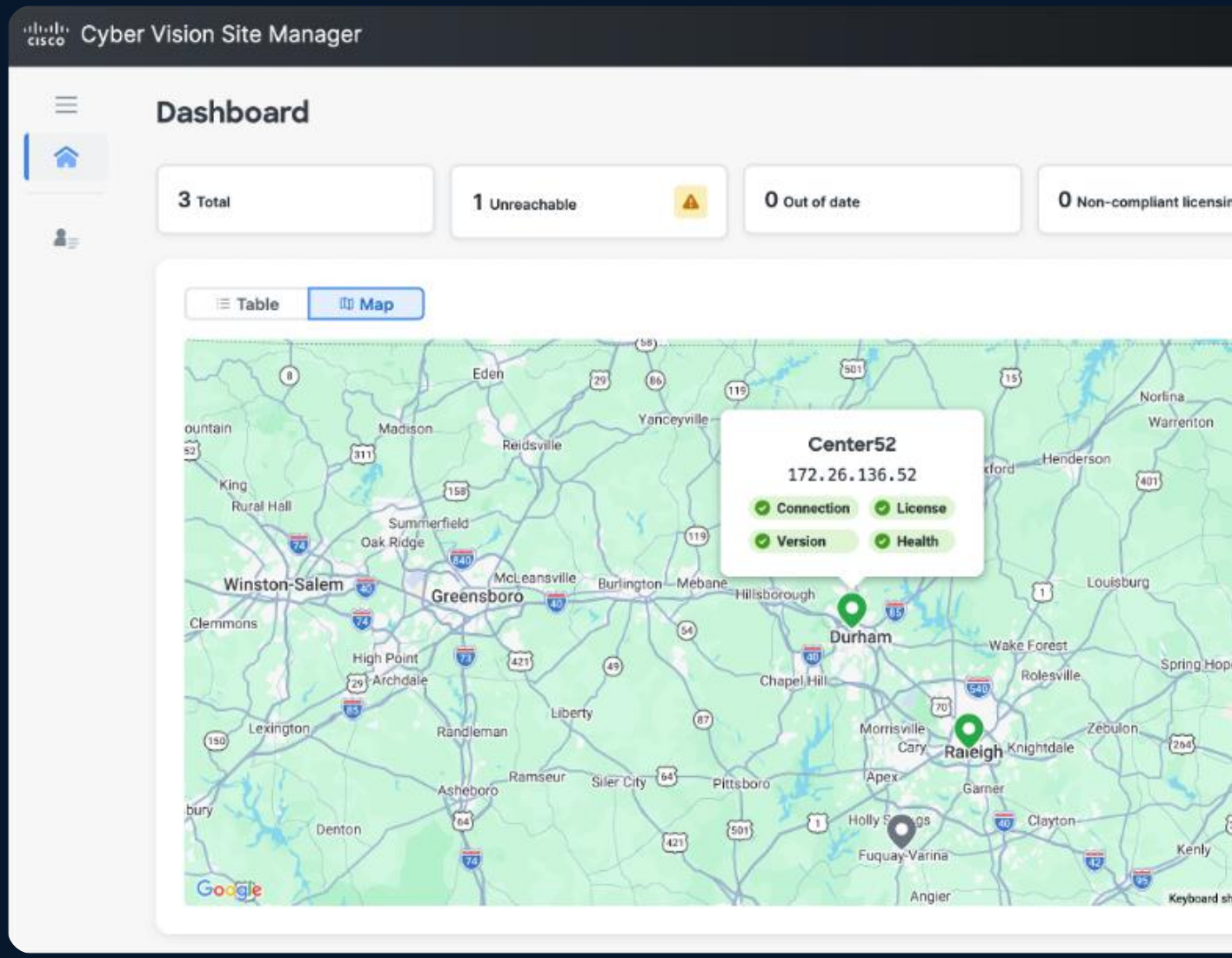


New
Cisco Cyber Vision Site Manager

Multi-Site Security Management

- 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

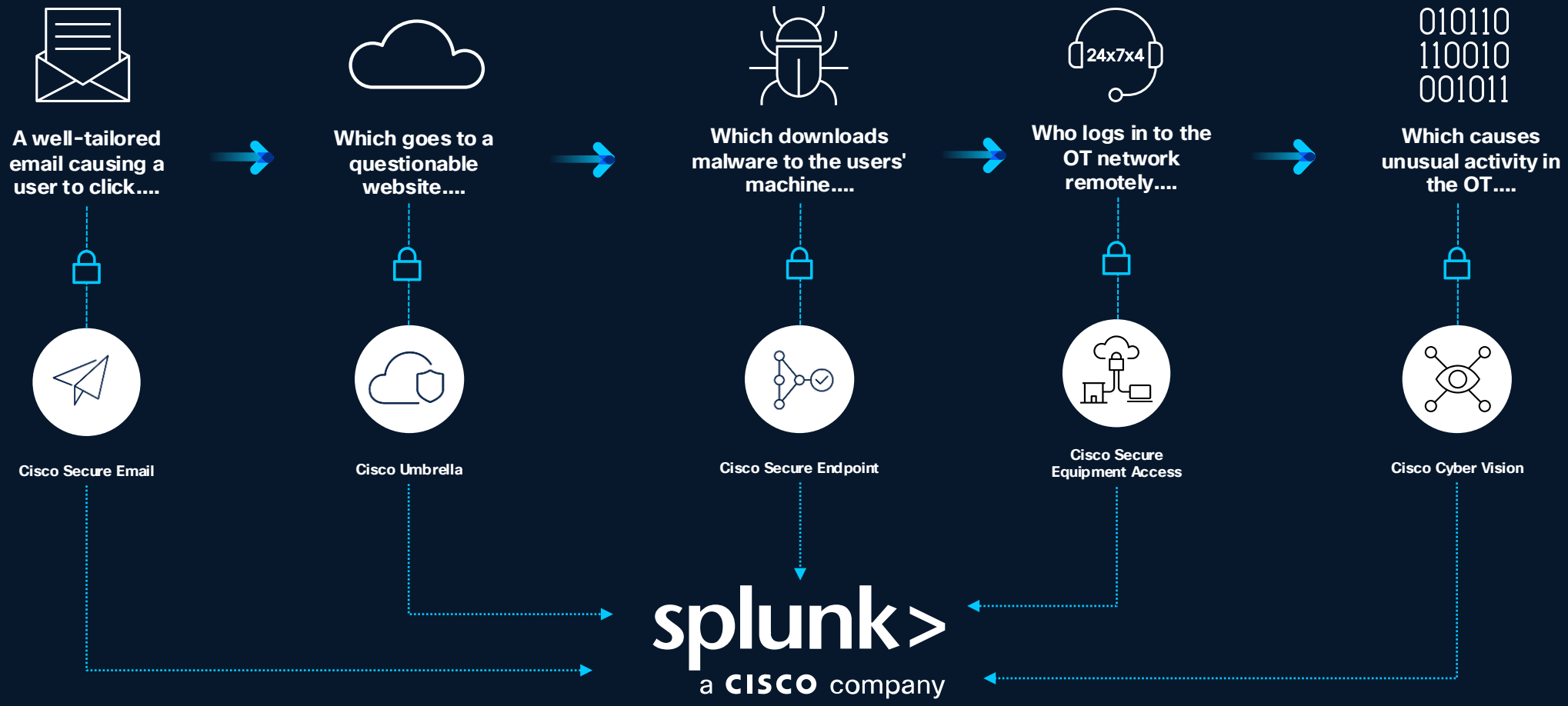
Give security teams time back to effectively manage cyber risk



Splunk & OT

A siloed approach is not enough to secure OT

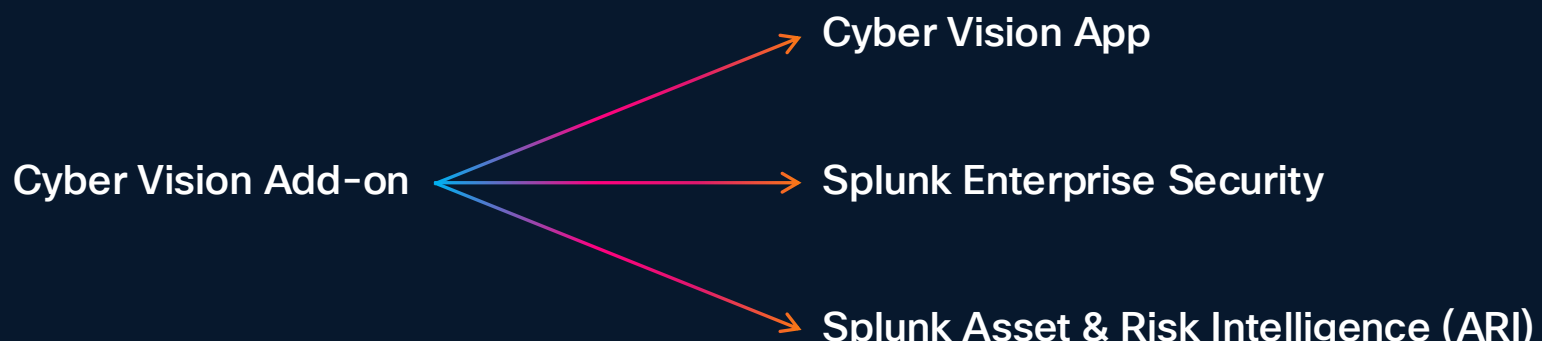
Detecting threats requires cross-domain visibility



Add-ons are for the system, Apps are for Humans

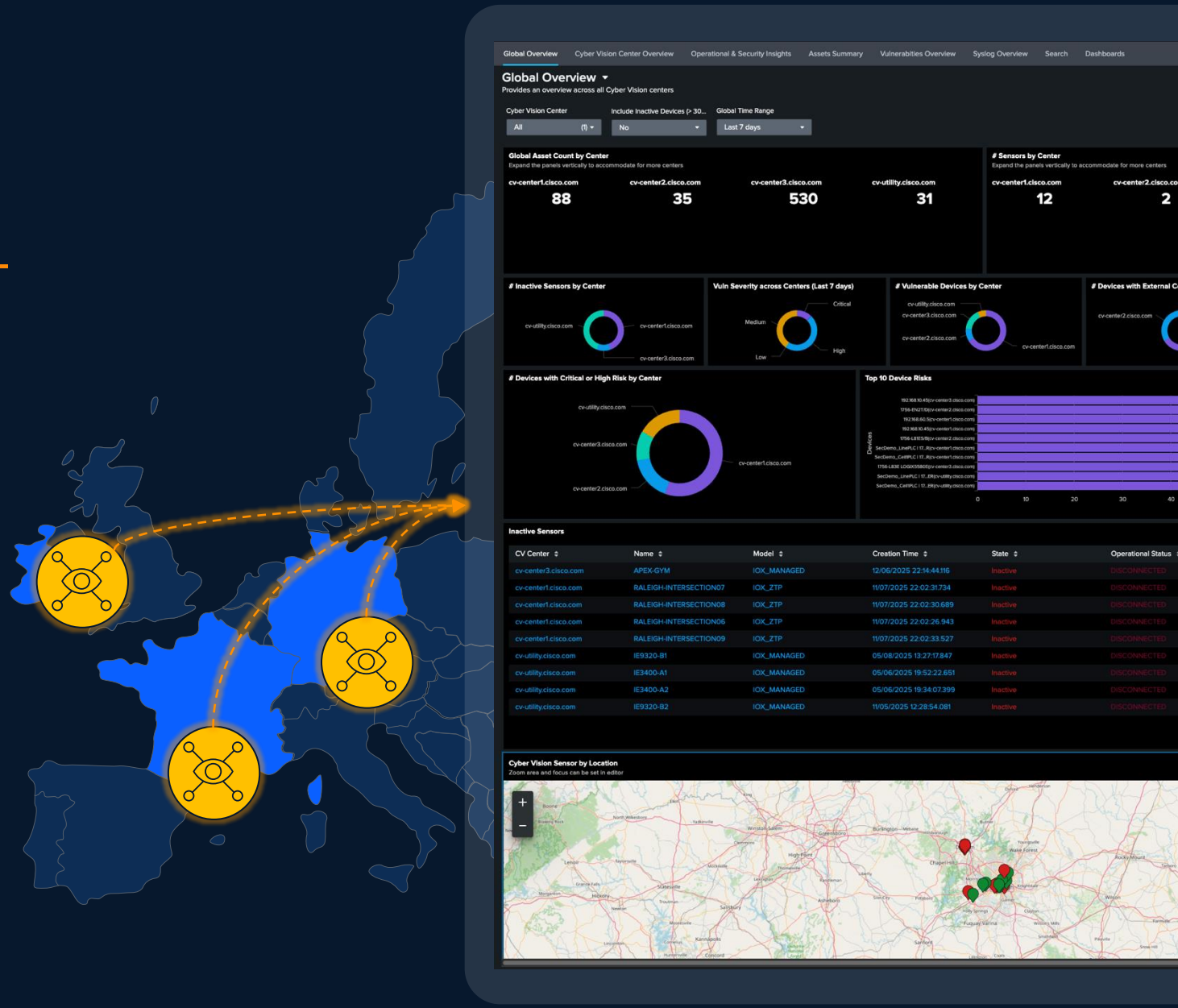
Cyber Vision Add-on is a background process that contains data parsing rules, field extractions, and configurations to ingest data from Cyber Vision correctly

Cyber Vision App contains dashboards, reports, saved searches and custom navigation menus so humans can make use of the data ingested by the add-on



Introducing the New Cyber Vision App

- Aggregate all Cyber Vision deployments
- Focused view per local center
- Operational & Security Overview
- Vulnerabilities Overview
- Real Time Syslog Collection
- Schedule reports over email



Cisco Secure Equipment Access

OT self service remote access with ZTNA control

Zero-Trust Security Controls

MFA, posture check, just-in-time access
Deny by default, least-privilege access

Threat Detection and Monitoring

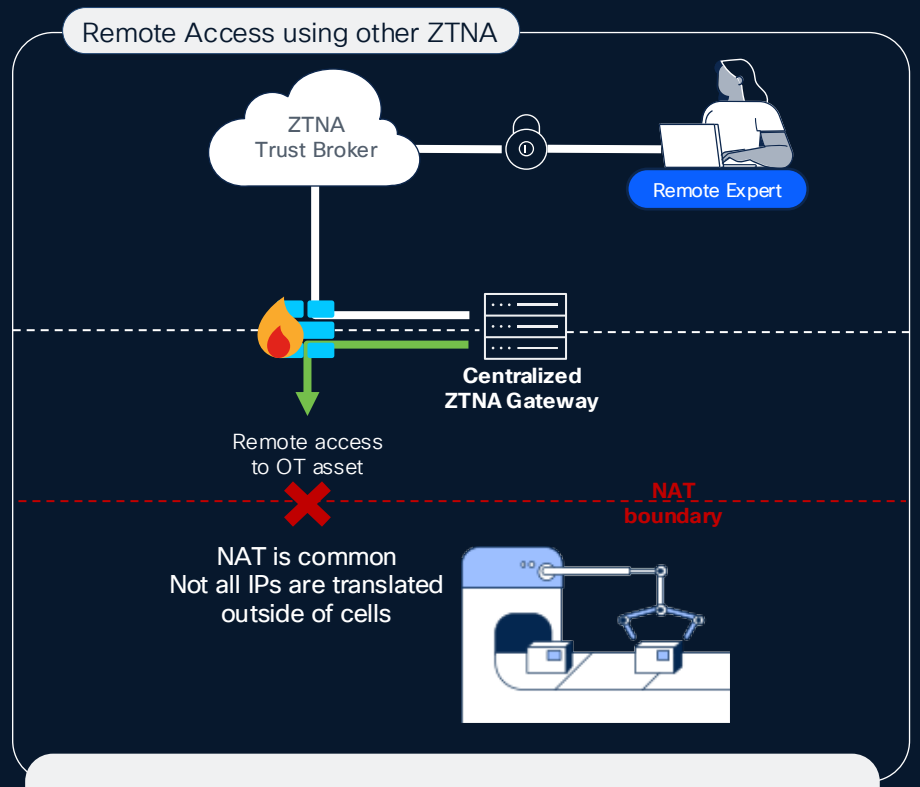
Identity anomaly detection
Session monitoring and recording

Easy to Deploy and Manage at Scale

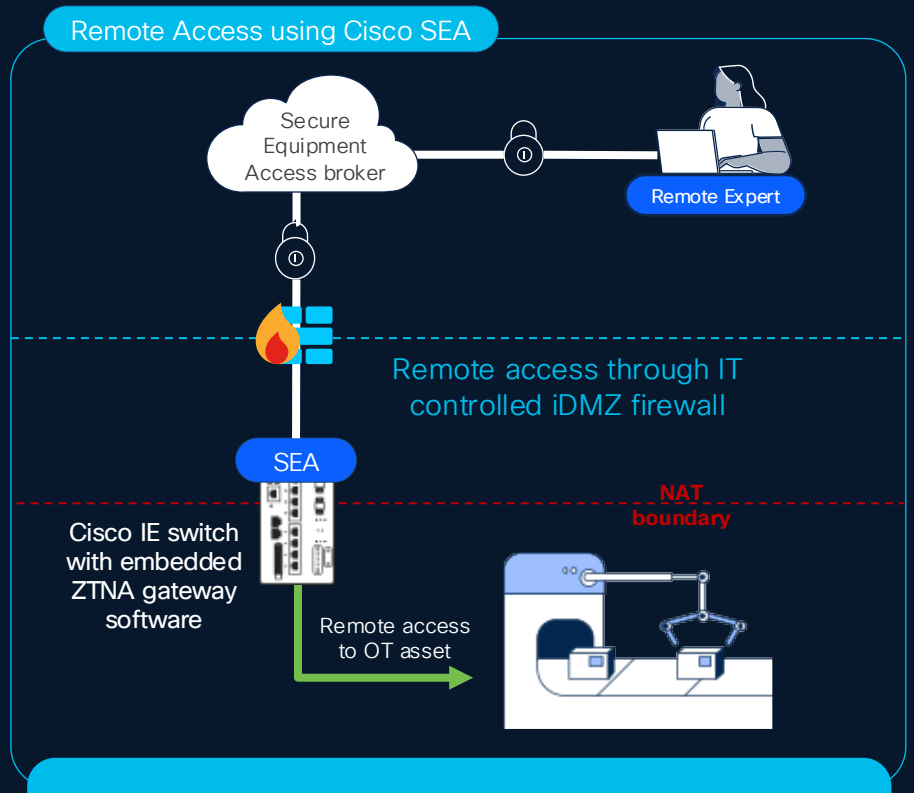
Centralized policy definition and enforcement
Network-embedded gateway

Not all ZTNA solutions are suited for use in OT environment

Cisco SEA simplifies remote access to NATed industrial devices



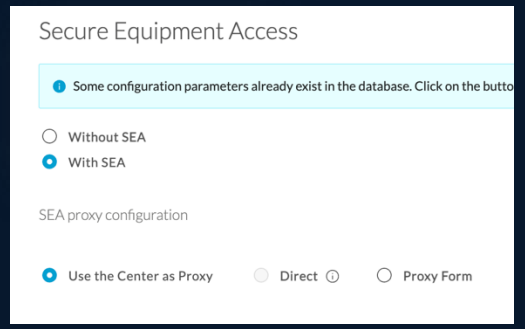
Centralized ZTNA gateway is too far from OT assets, forcing users to expose private IPs outside Level-2, negating resource isolation and increasing attack surface

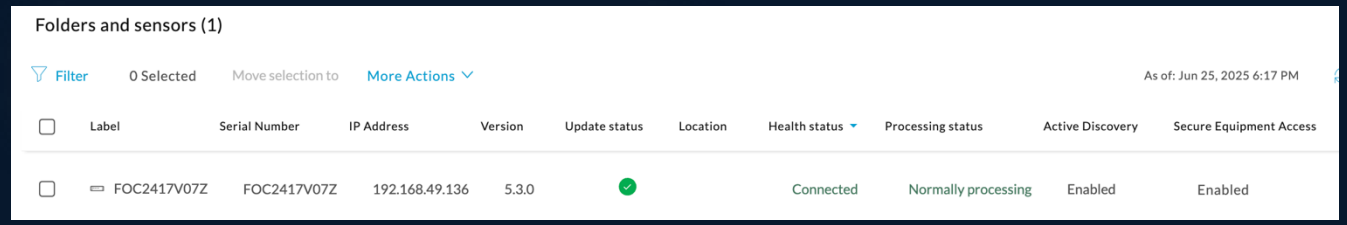


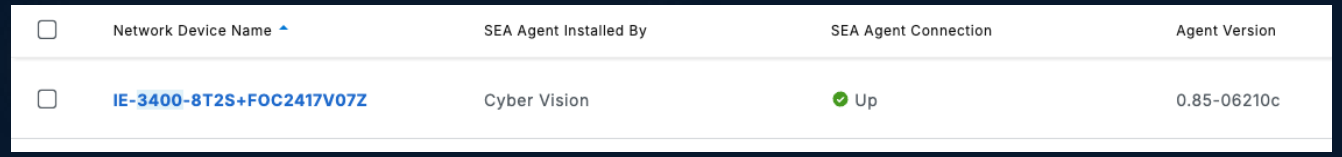
The switch or router connecting the NATed device is the ZTNA gateway, eliminating the need for complex network configuration for exposing private IP addresses

Single integrated IOx App for Cyber Vision and SEA

- As of Cyber Vision 5.3, the SEA Agent can be integrated in the Cyber Vision Sensor
- The integrated application is deployed on the network from Cyber Vision Center
- Cyber Vision Center integrates with SEA cloud for token exchange to authenticate the SEA Agent
- Users log into SEA and the Cyber Vision Center independently with Single Sign-On
- Docker deployments are not supported. See datasheet for the list of supported platforms







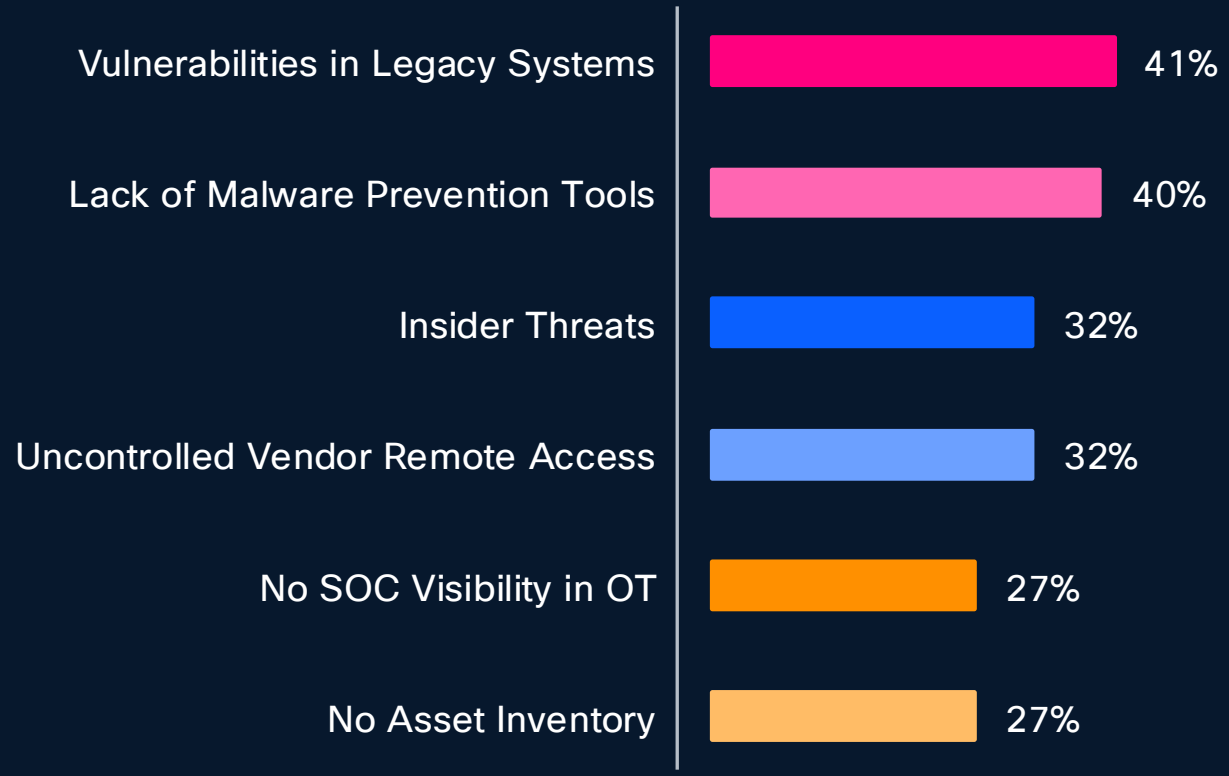
Segmentation

Many industrial networks have not moved from visibility to protection

Challenge Statistics

OT Security Challenges - What Operators Actually Face

Top Security Challenges in Industrial Networks



Source: Cisco 2024 State of Industrial Networking Report

Segmentation mitigates 5 of 6 challenges:

Contain threats from legacy Vulnerabilities ✓

Prevents Malware spread ✓

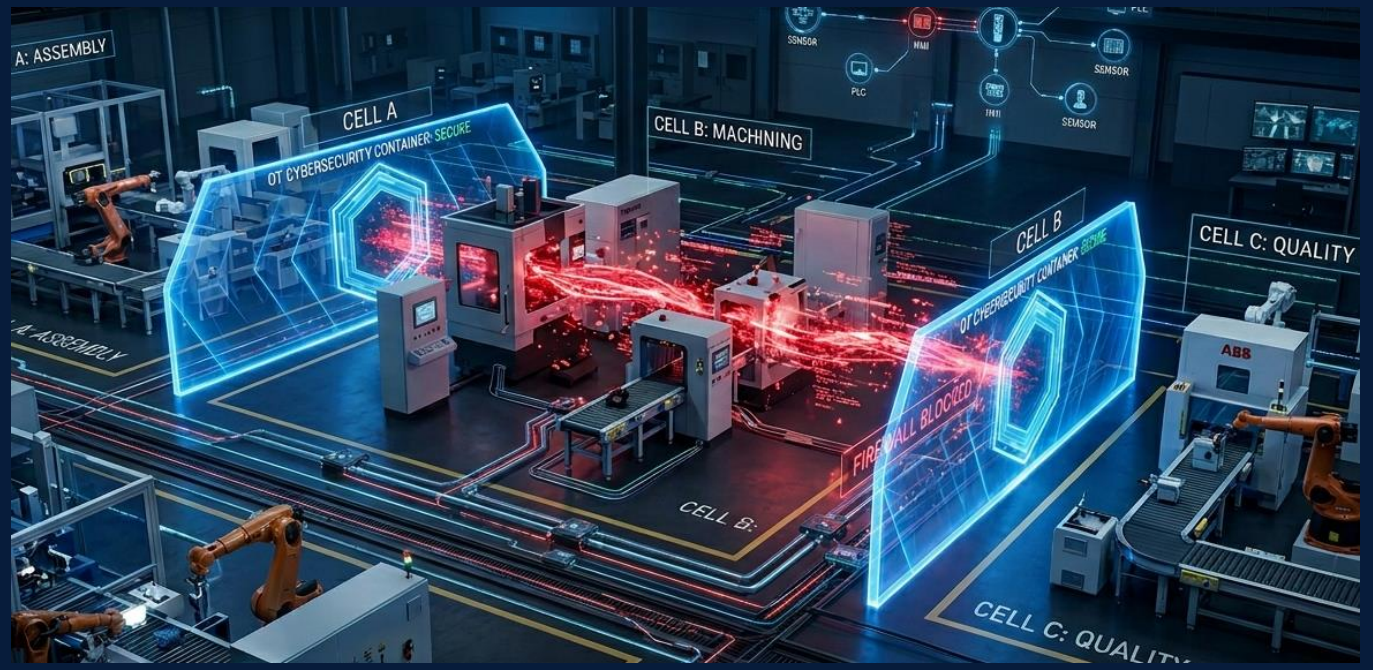
Limits insider threat movement ✓

Restricts vendor access scope ✓

Enables SOC Visibility through policy logs ✓

Mythos-class AI will significantly weaken the perimeter firewall

- Perimeter breaches will be followed by high-speed, autonomous lateral movement within the OT network
- Network segmentation between operational processes is critical to limiting the blast radius of attacks



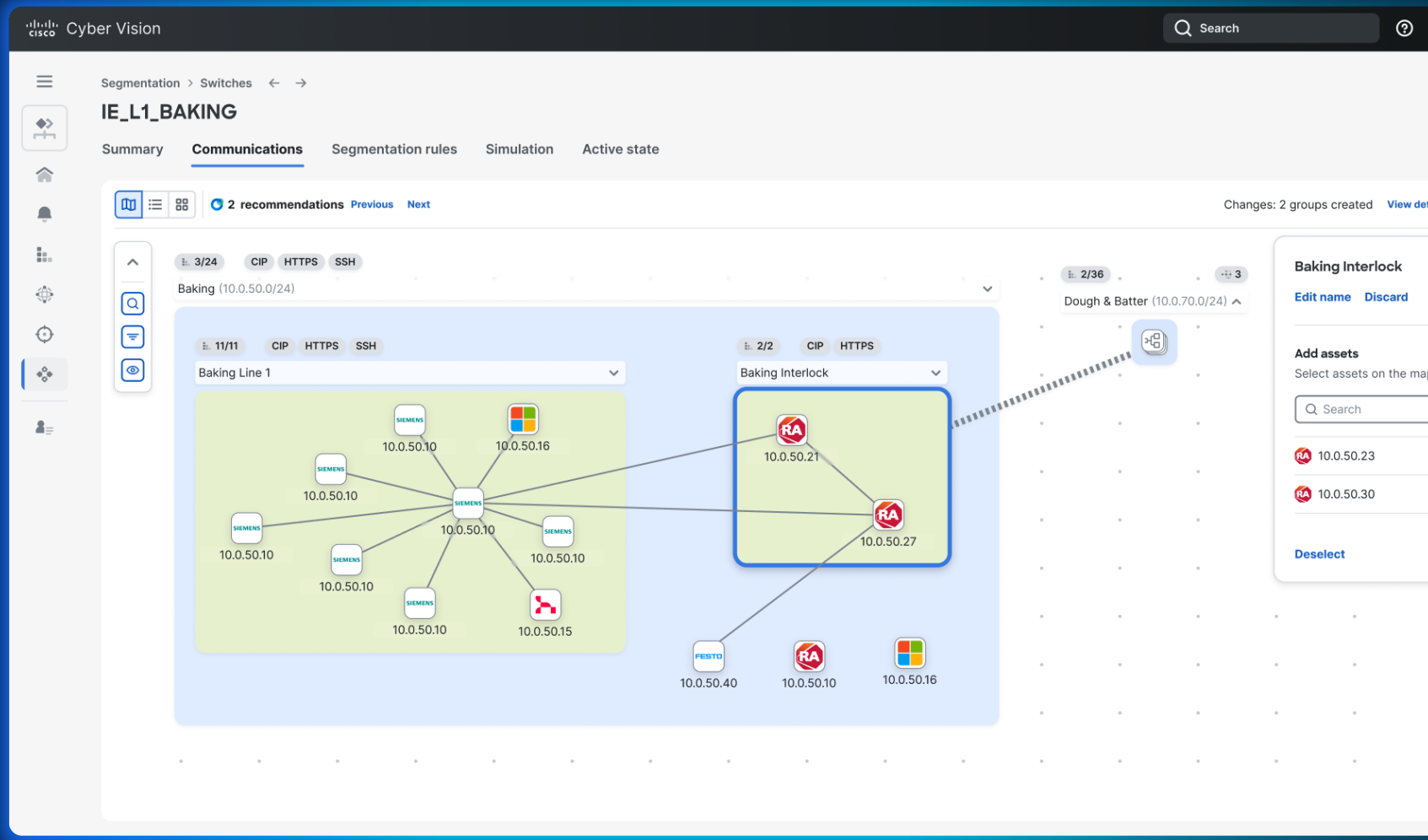
Zones & Conduits

Looks simple on paper, but hard to implement!

Cisco Cyber Vision

Asset auto-grouping

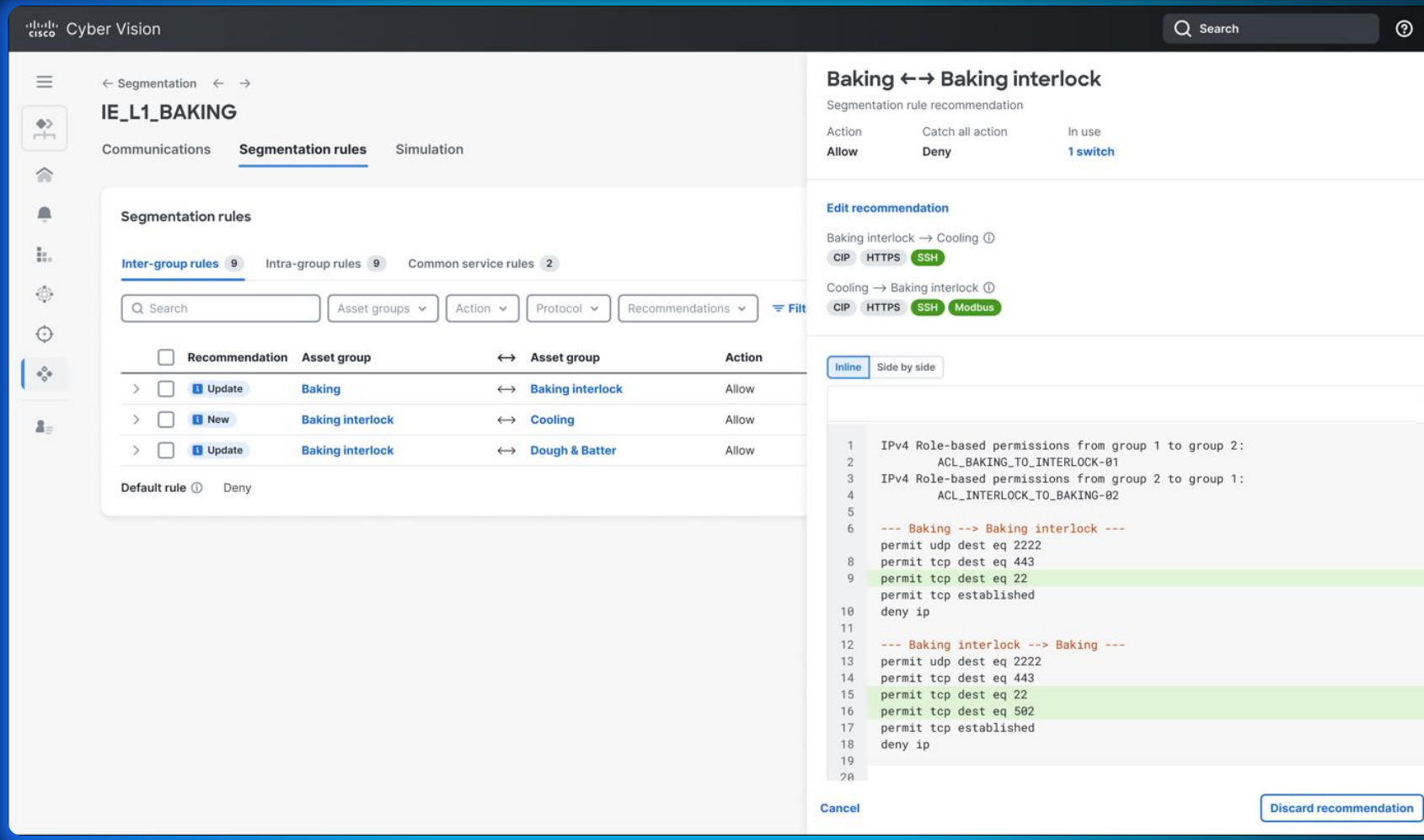
- Assets communicating through the switch are auto-grouped based on networks
- ML clustering recommends sub-groups within networks and groups for network-wide common services
- Users can modify system recommended groups



Cisco Cyber Vision

Automated Rule Creation

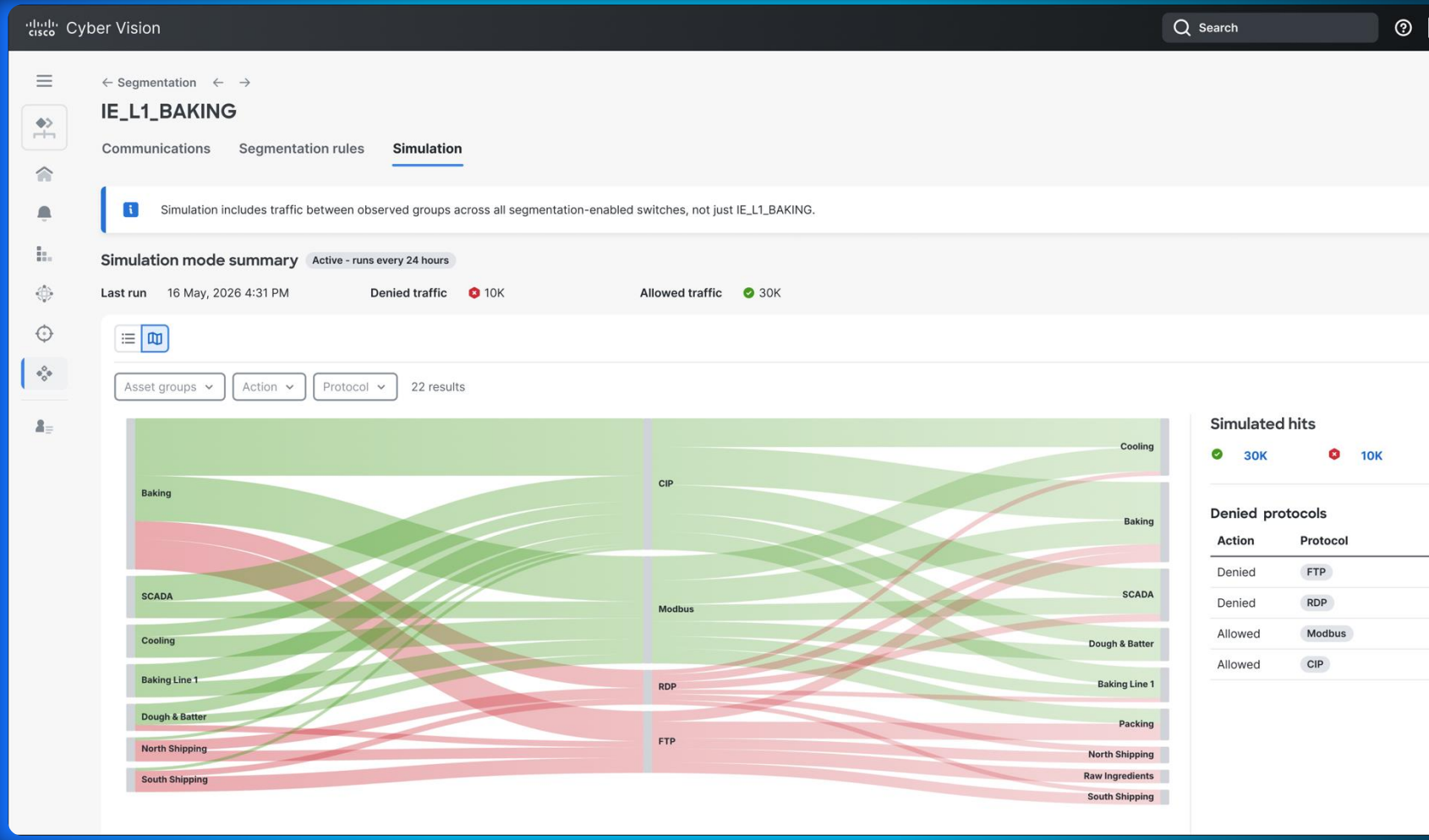
- System recommends rules based on communication between asset-groups
- Users can fine tune rules as needed



Cisco Cyber Vision

Segmentation Policy Simulations

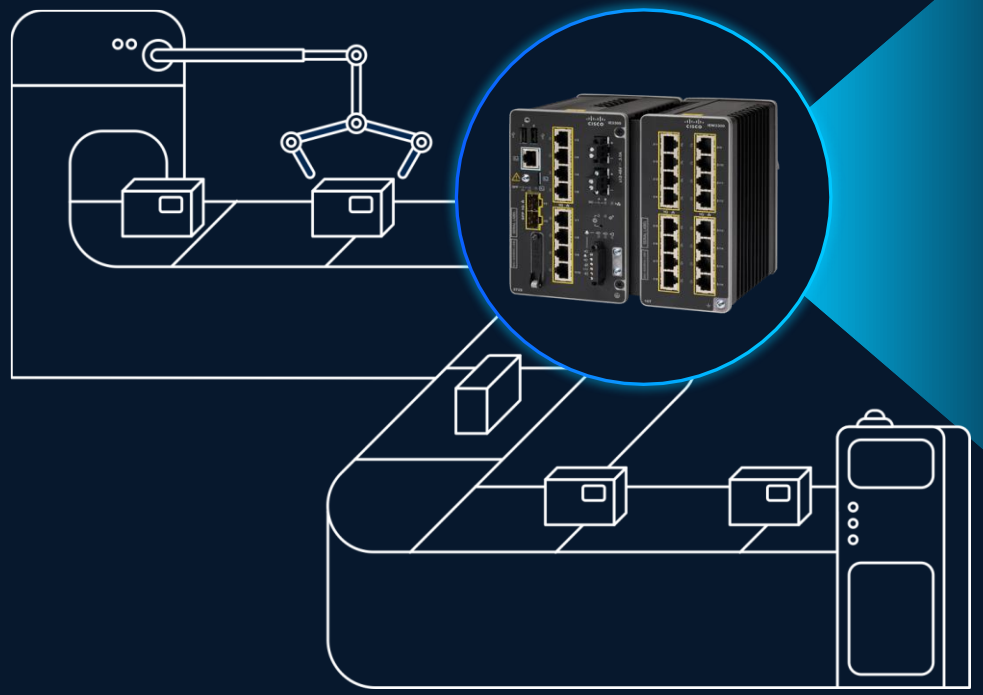
- Simulation shows the impact of rules against live traffic
- Helps identify legitimate traffic being blocked that was missed during rule creation
- Users can modify segmentation policy to fix issues identified



Summary

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

Děkujeme za Vaši pozornost

Následující Tech Club webinář:

23.6.2026 **Přehled novinek ze Cisco Live Las Vegas 2026**

Přednášející: Jiří Rott

Registrovat se můžete na oficiálním webu **Cisco Tech Club webináře**

Následující webinář

Tech Club portál


CISCO