

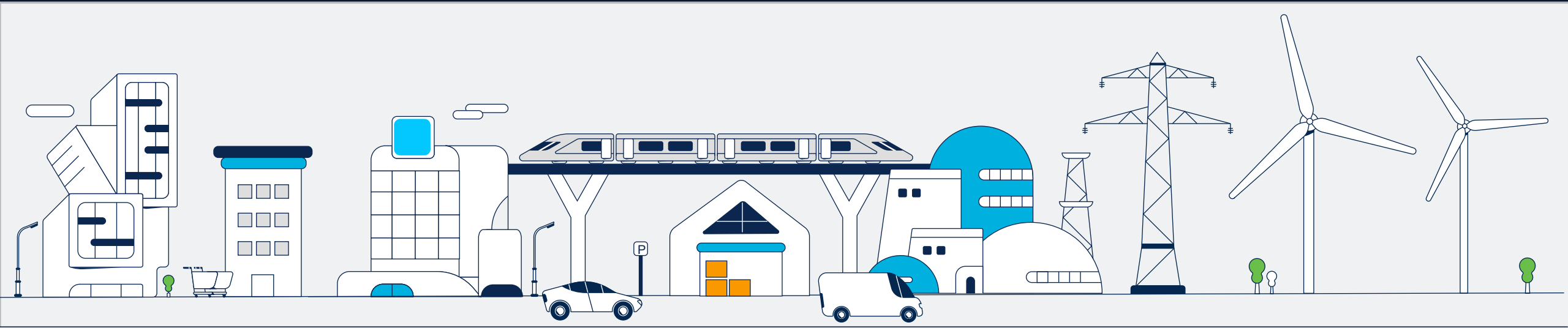
Bez viditelnosti není bezpečnost: Jak chránit industriální sítě před moderními hrozbami

Cisco Cyber Vision

Stanislav Kraus, Cisco SE
stakraus@cisco.com



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



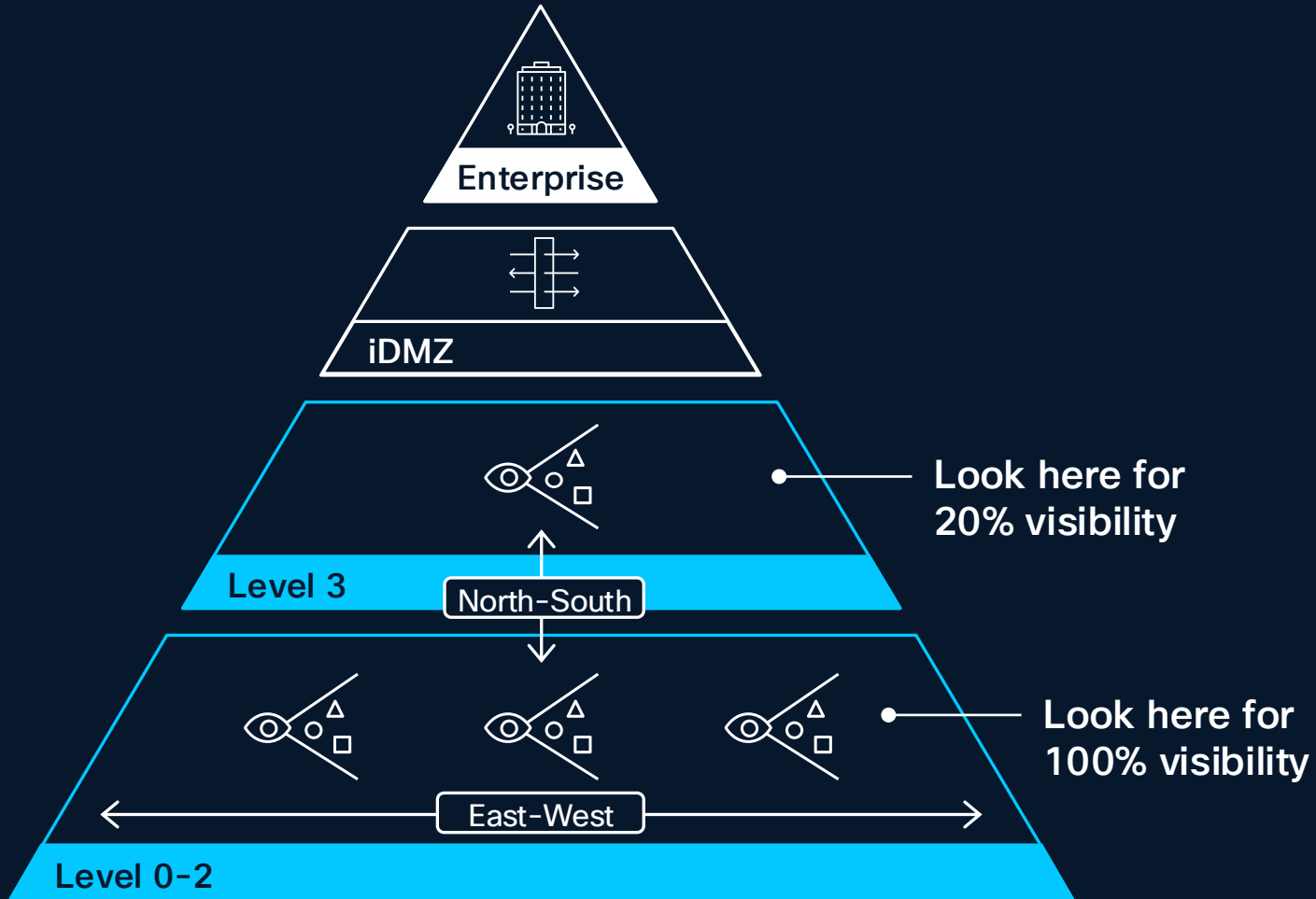
Detect bypass or
leaks in the IDMZ



Drive compliance
and governance

OT context and insights are foundational to securing industrial networks

Security starts with visibility, but where you look matters

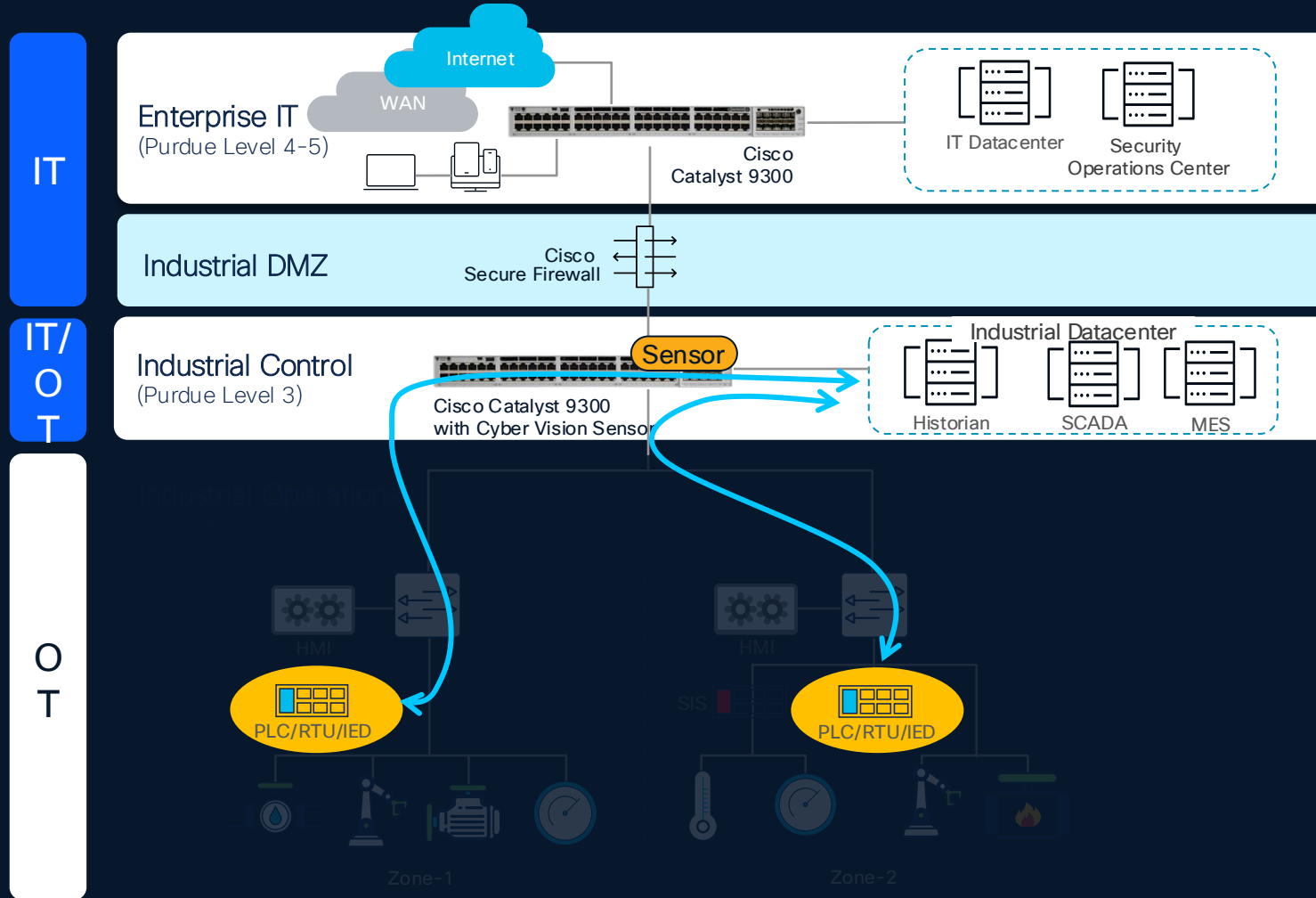


Purdue Model

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

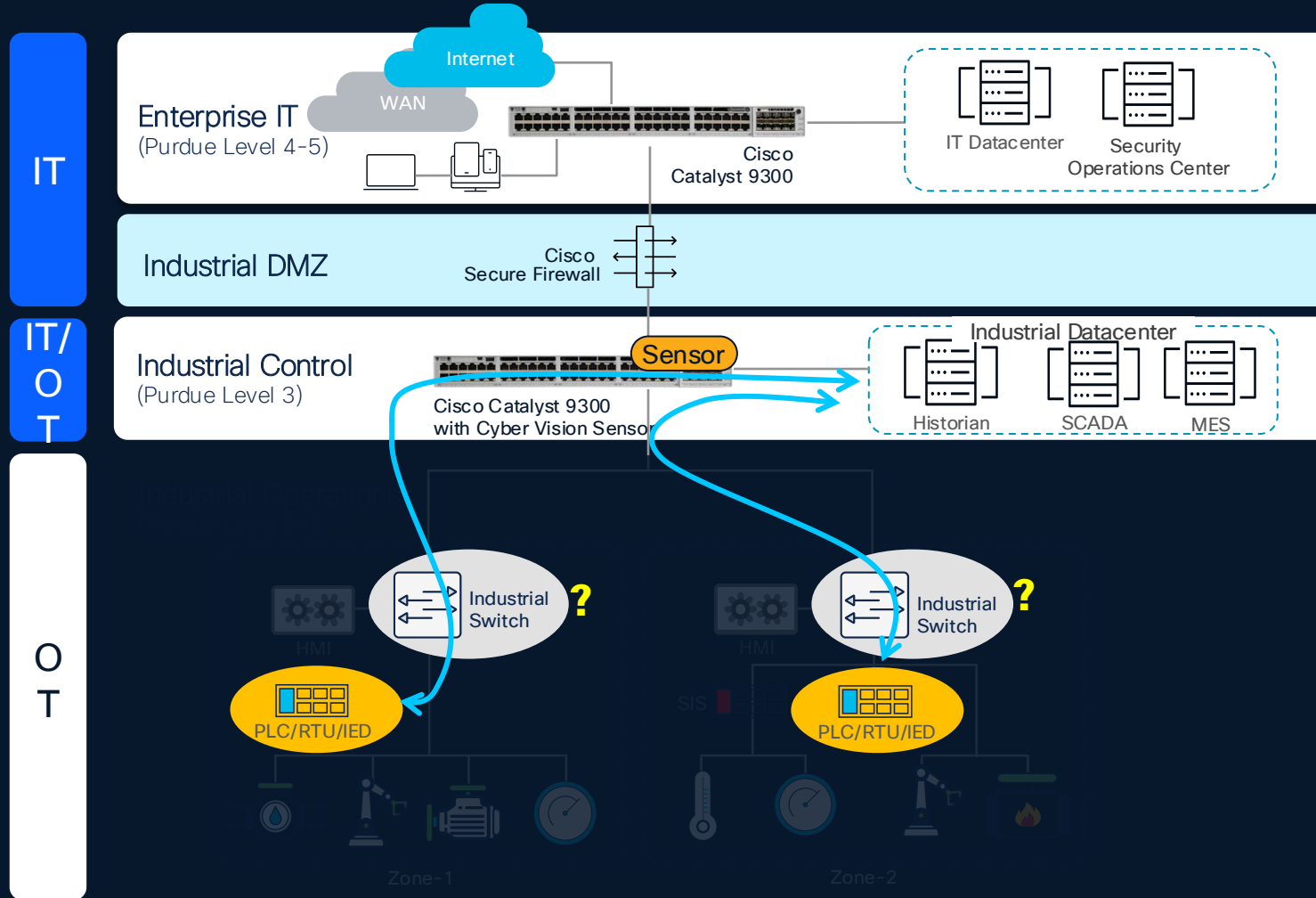
Gaining visibility at the aggregation layer sees very little as most OT traffic is local to the production cell

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



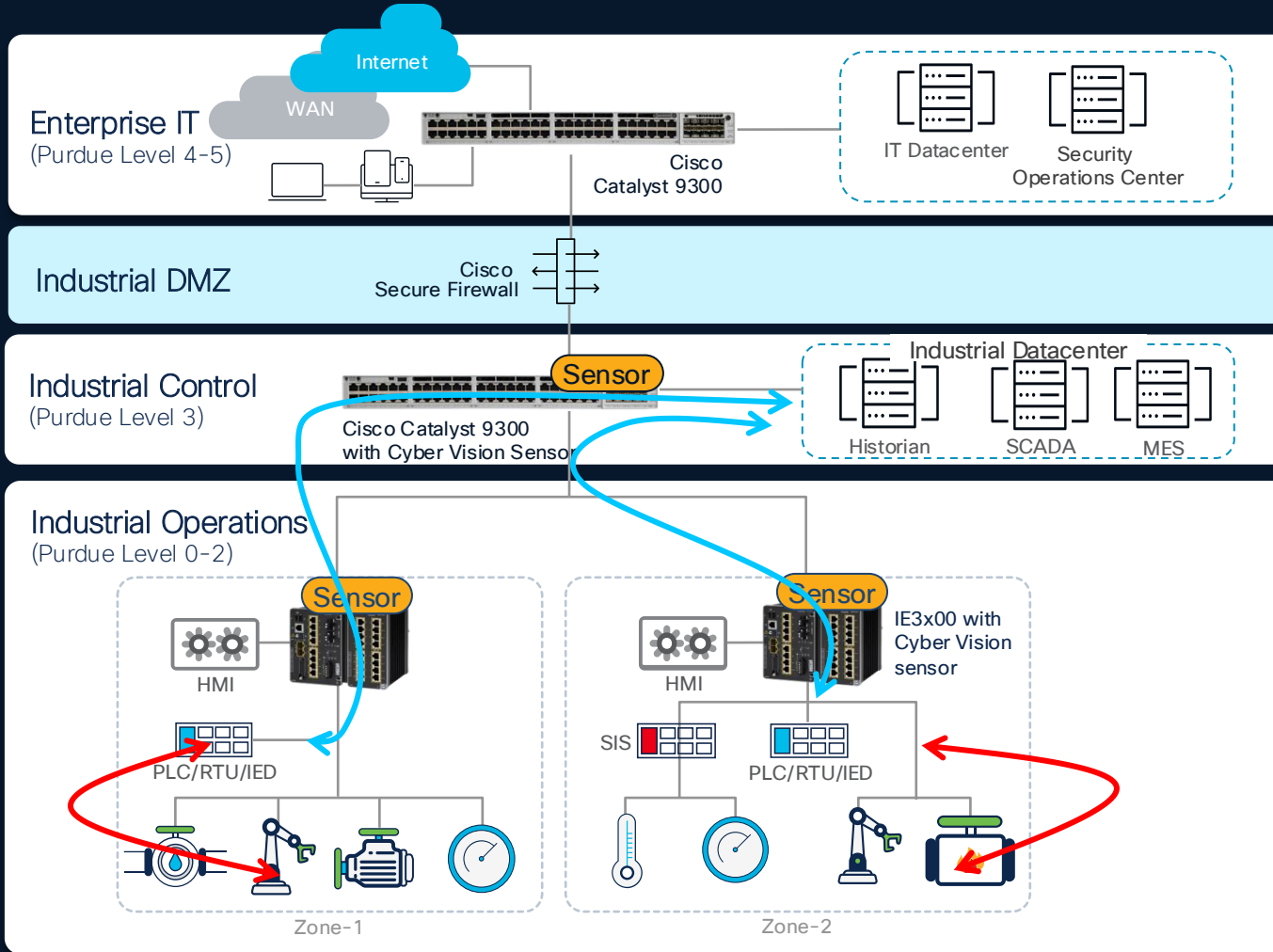
Step-2: Work with OT to identify the critical industrial switches that connect these key assets

Helps you get a footprint into OT

IT

IT/
OT

OT

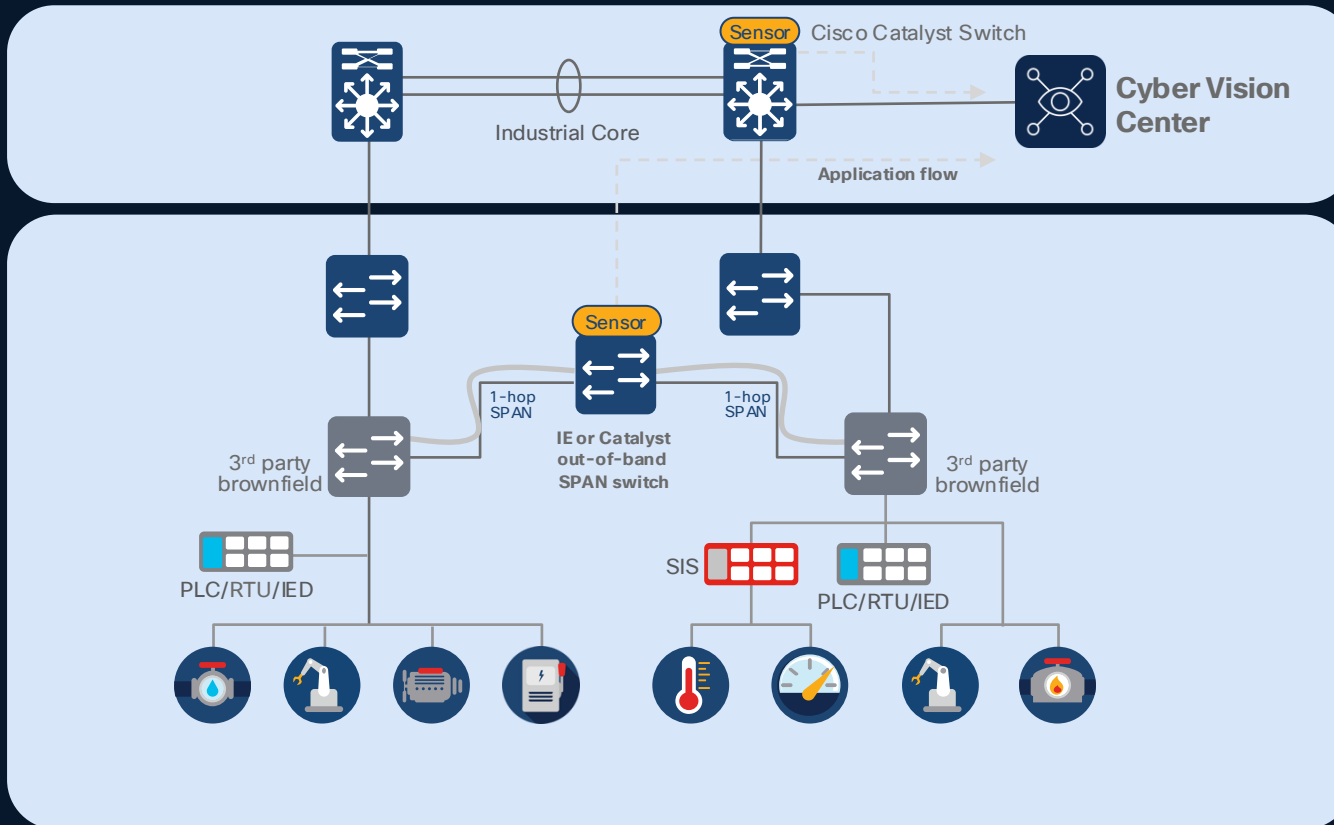


Cyber Vision
is licensed per endpoint,
not per sensor!

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

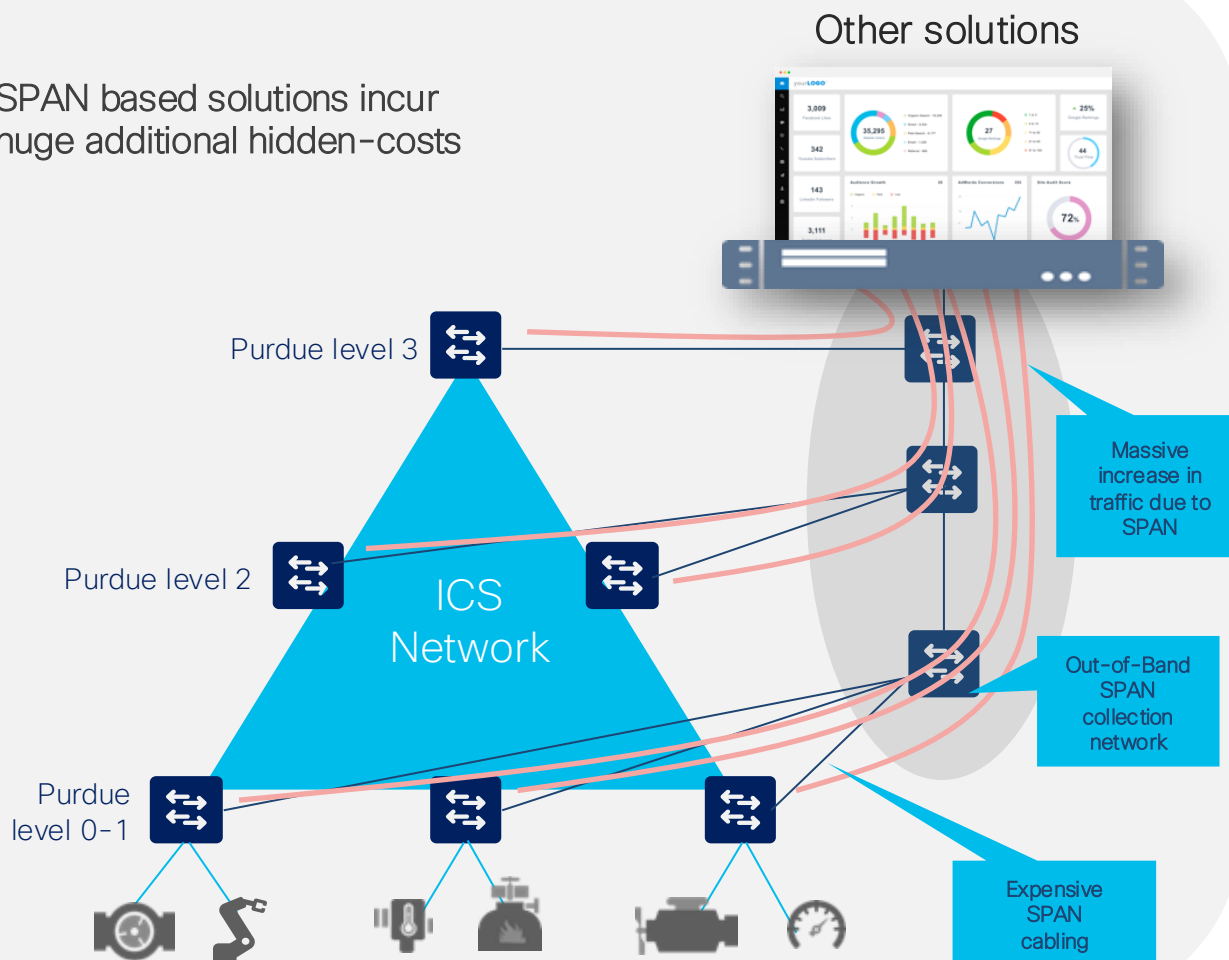
Out-of-Band Collection



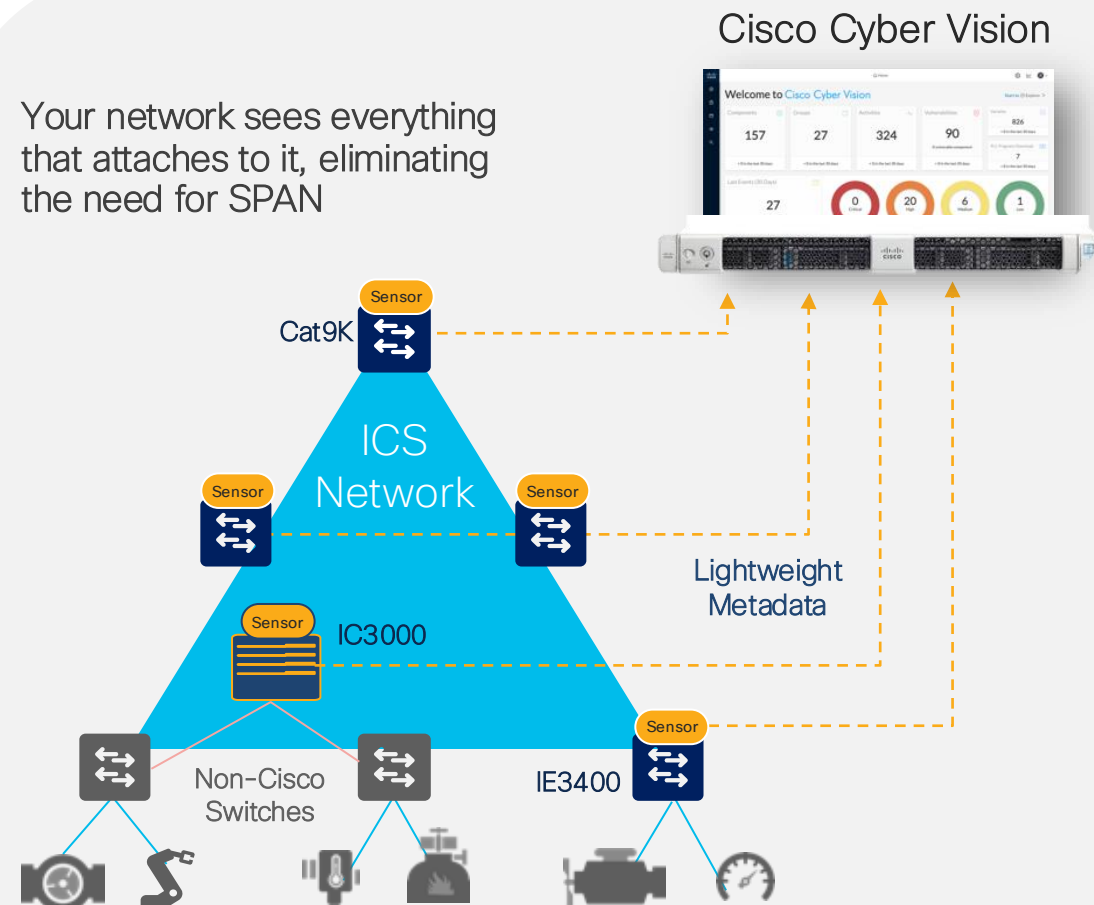
- Embedded Sensor on IE3400 and Catalyst 9300 can be leveraged as out of band sensor
- Enables aggregation of multiple SPAN sessions from across infrastructure
- Environment and scale are deciding factors for IE3400 or Catalyst 9300
- Unlike other solutions that require SPAN all the way to the monitoring 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

SPAN based solutions incur huge additional hidden-costs



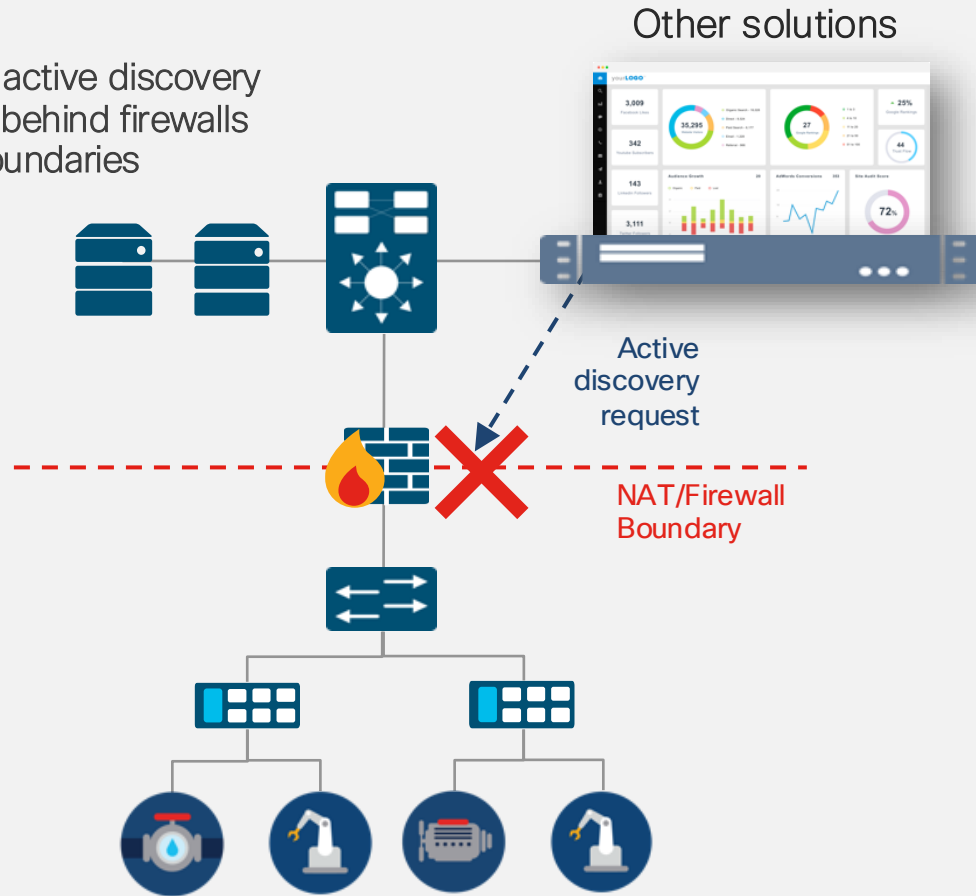
Your network sees everything that attaches to it, eliminating the need for SPAN



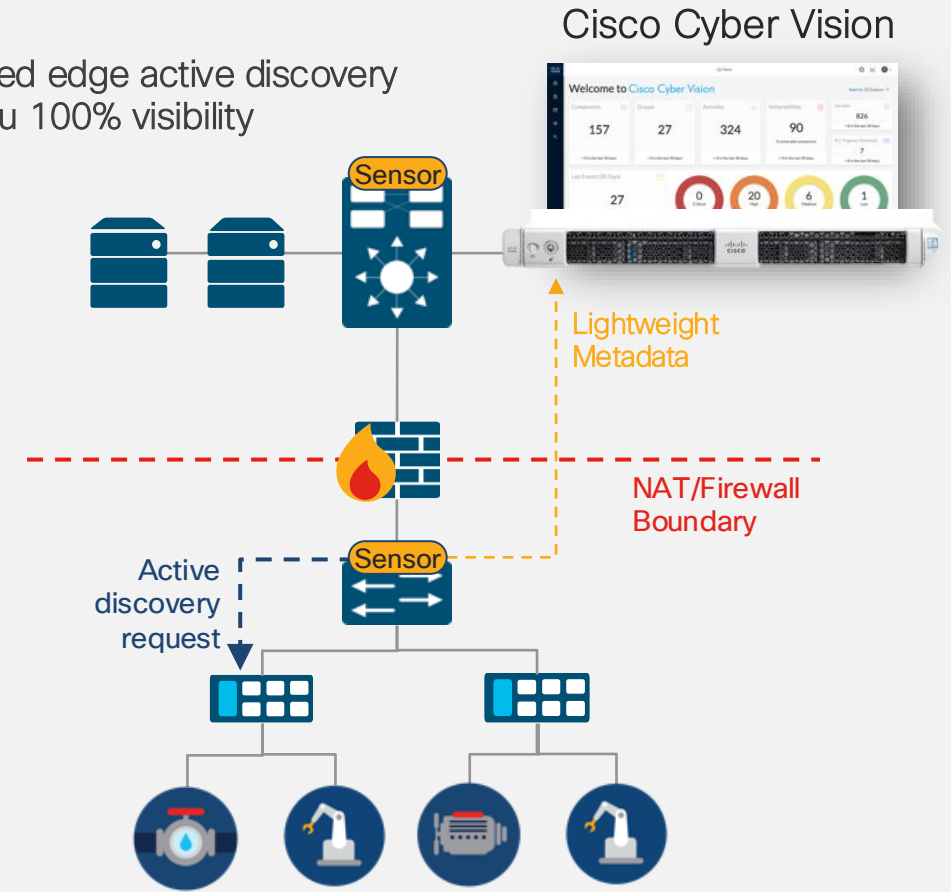
Distributed edge discovery sees more

Silent devices, FWs

Centralized active discovery cannot see behind firewalls and NAT boundaries

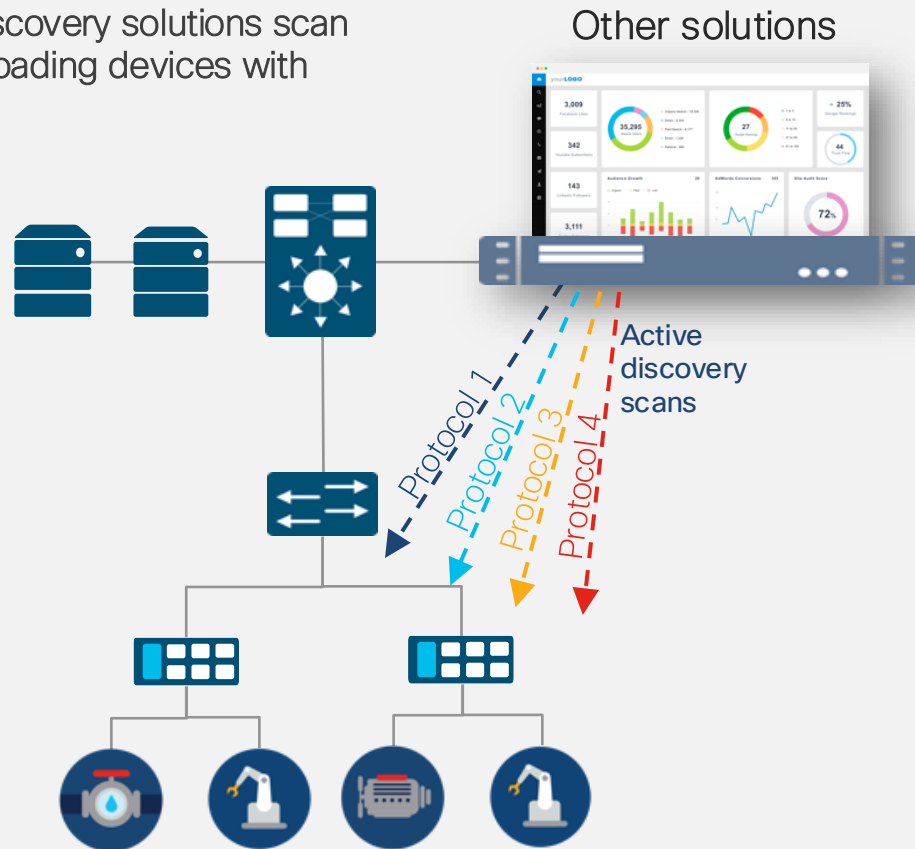


Distributed edge active discovery gives you 100% visibility

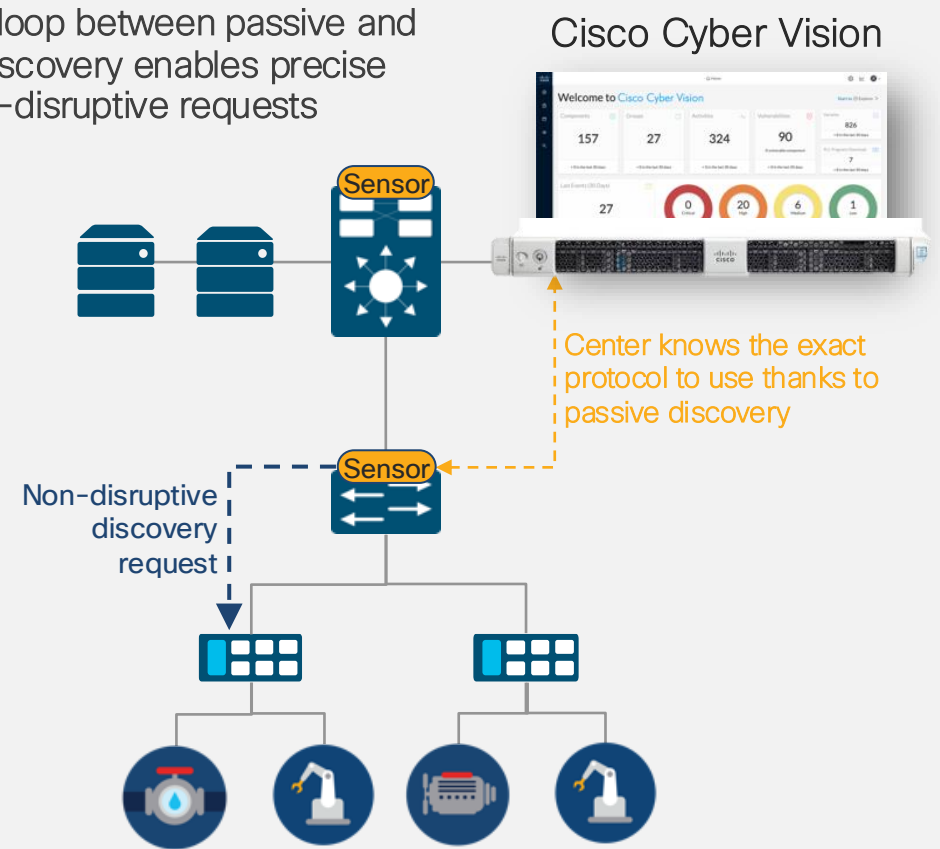


Closed-loop control makes active discovery safe

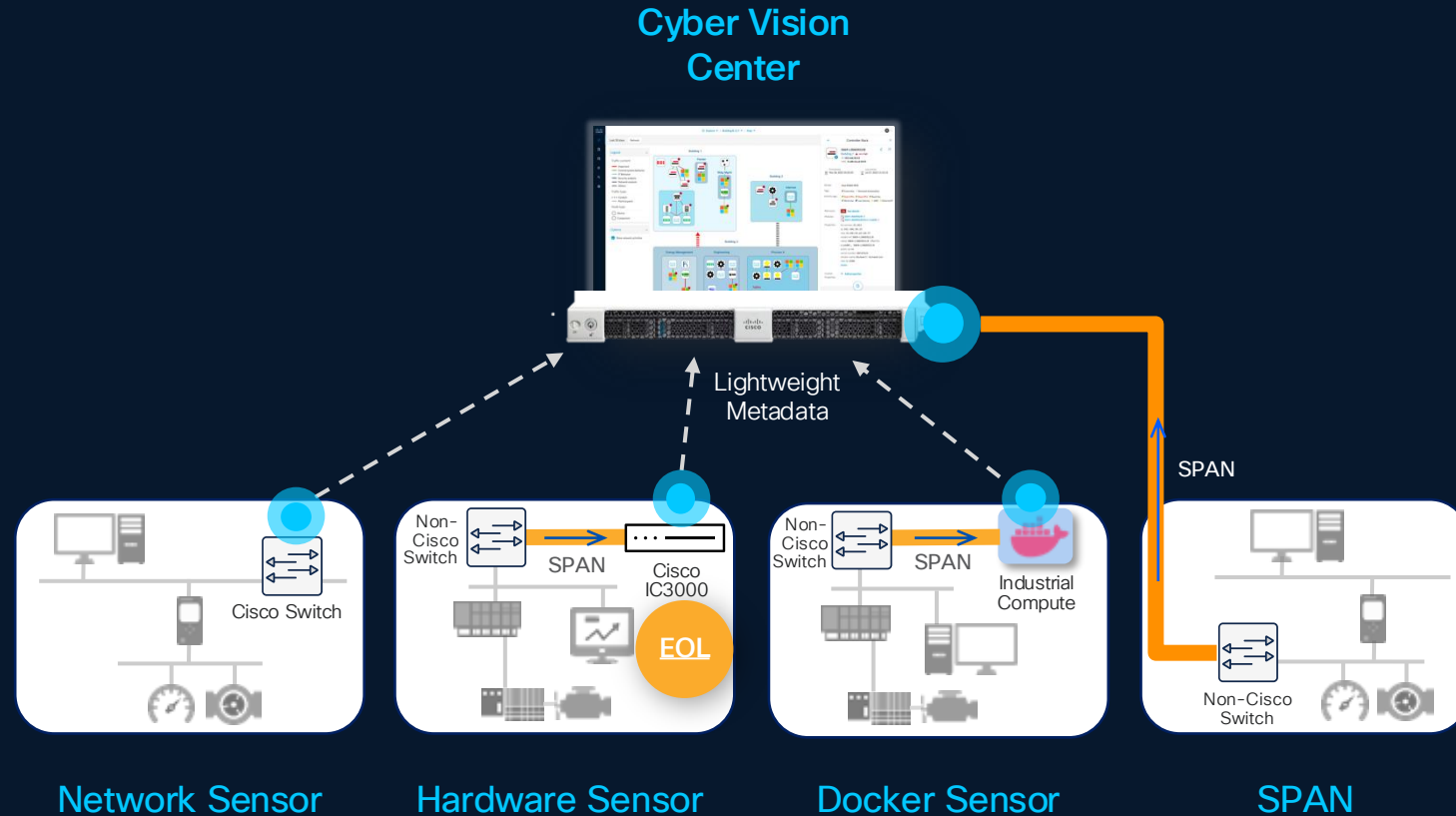
Basic active discovery solutions scan networks overloading devices with ARP requests



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



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



Amazon Web
Services



Microsoft
Azure



Google Cloud

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

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

Sensors



Sensor

IE3300, IE3400,
and IE3500
Switches



Sensor

IE3400HD and IE3500HD
IP67 Switch



Sensor

Catalyst IR1101
Cellular Router



Sensor

Catalyst IR1800
Cellular Router



Sensor

IDS

Catalyst IR8300
Multiservice Router



Sensor

Catalyst IE9300
Rugged Switches



Sensor

IDS

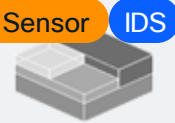
Catalyst 9300/9350/9400
Aggregation Switches



Sensor

IDS

x86 or ARM64 Compute
running Docker



Sensor

IDS

x86 Compute
running VMWare



Sensor

IDS

EOL

Cisco IC3000
Industrial Compute

Network Sensors

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

Compute Sensors

DPI and active discovery via SPAN to support brownfield

Cyber Vision VM Sensor – Technical Summary

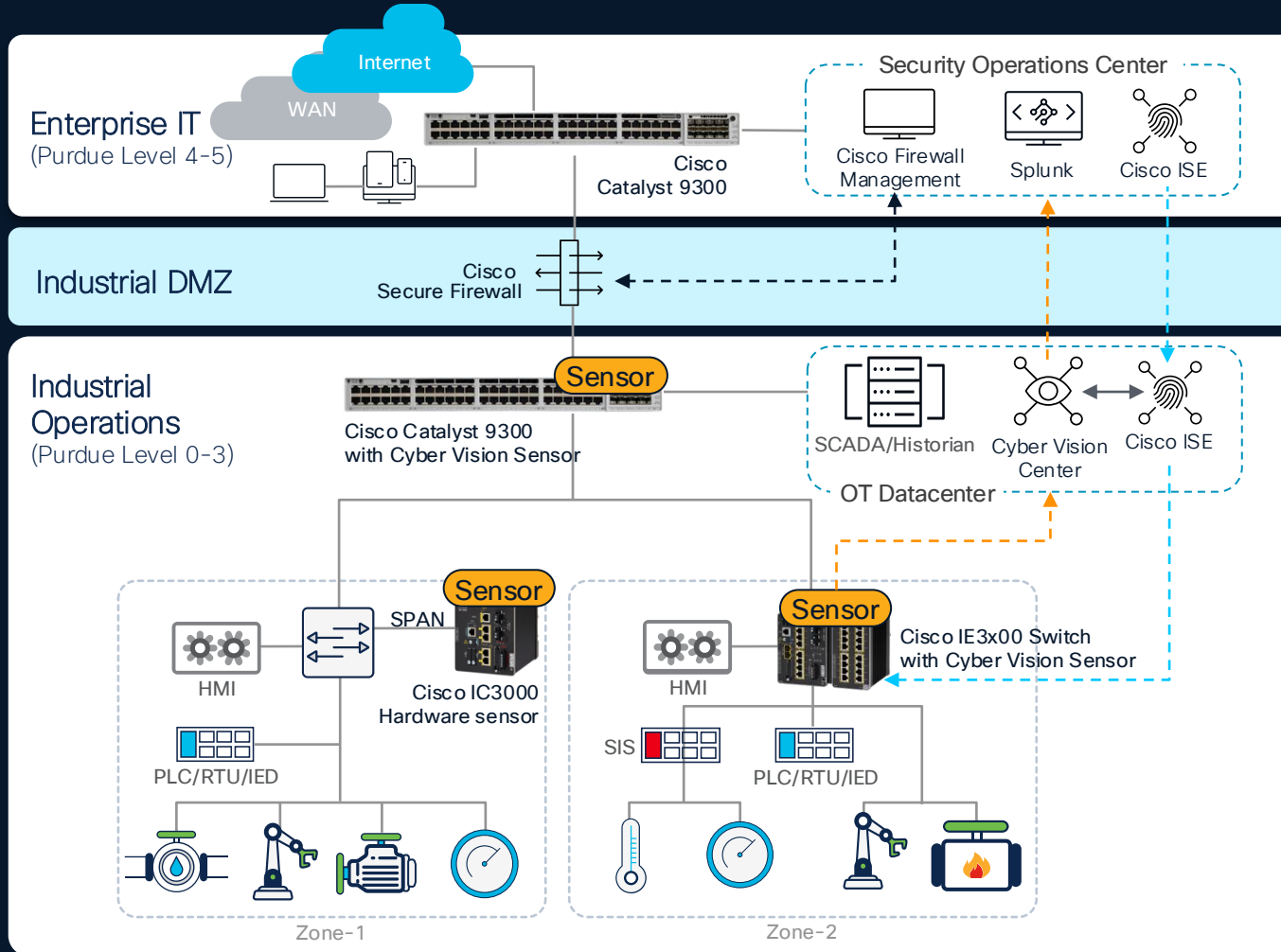
- Compatible with x86-64 devices
 - VMWare v6.x required
 - Minimum of 4GB dedicated memory required (8GB recommended)
 - Minimum of 2 dedicated CPU cores required
- Required network communication
 - Host to CV Center ports: 443/80
 - VM instance to Center ports: 5671, 10514
- Storage allocation of instance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

Security Architecture in Manufacturing

IT

IT/
OT

OT



1

Visibility built into your industrial network to identify OT assets, vulnerabilities, assess security posture and detect threats

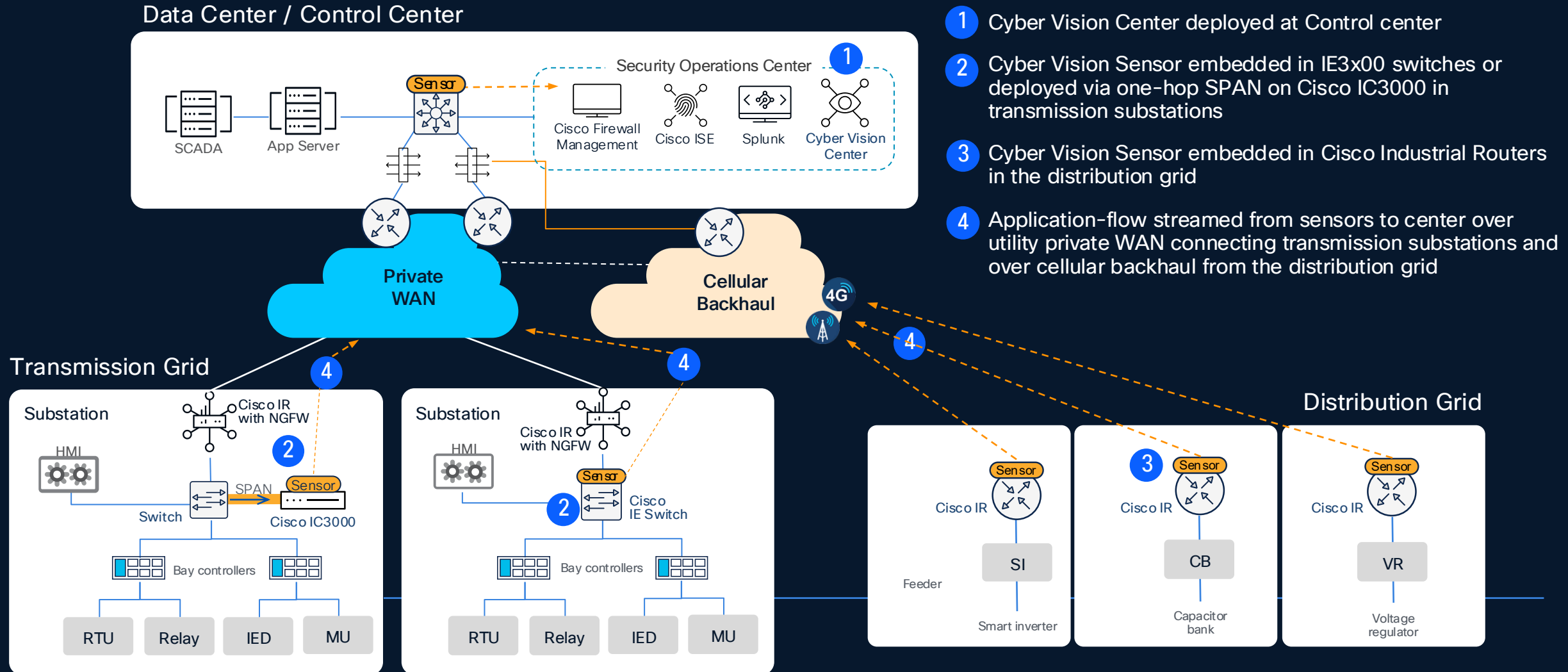
2

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



Key Features

Cyber Vision

Visibility into connected industrial assets

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

The screenshot displays the Cisco Cyber Vision interface, which provides visibility into connected industrial assets. The interface is divided into several sections:

- Component Details:** Shows information for a Rockwell Automation component (1769-L16ER/B LOGIX5 316ER). It includes the IP address (192.168.249.50), MAC address (f4:54:33:91:cb:ee), and activity logs (First activity: Apr 14, 2021 11:45:12 AM; Last activity: Apr 16, 2021 11:00:01 AM). It also lists tags such as Controller, Rockwell Automation, Stop CPU, Diagnostics, Read Var, Write Var, and Low Volume.
- Properties:** A detailed view of the component's properties, including vendor-name (Rockwell Automation), fw-version (31.011), model-ref (1769-L16ER/B LOGIX5316ER), serial-number (60771949), name (1769-L16ER/B LOGIX5316ER), ip (192.168.249.50), public-ip (no), and mac (f4:54:33:91:cb:ee).
- Network Diagram:** A visual representation of the network topology, titled "Drilling Machine". It shows a central Dell switch (Dell 192.168.105.241) connected to various industrial devices, including Siemens PLCs (Siemens 192.168.105.150, PLC_3, Siemens 192.168.105.105), a Supermicro server (Super 192.168.105.1), and an S7-400 station. Red arrows indicate network connections between these devices.

Identify & Track Vulnerabilities

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

Explore / 192.168.1 subnet / Vulnerabilities
Jan 1, 2020 12:00:00 AM - Nov 19, 2020 3:27:00 PM (10 mths 19 days 11 hrs 27 mins) • LIVE

192.168.1 subnet

My preset

Active baseline: No active baseline

Active Discovery: Disabled

This preset is filtered with keywords «192.168.1»

Criteria Select all | Reject all | Default

Search criteria

NETWORKS ▾

COMPONENT TAGS ▴

- ☐ Components without tags
- ☐ Device - Level 0-1
- ☐ Device - Level 2
- ☐ Device - Level 3-4
- ☐ Network analysis
- ☐ Software
- ☐ System

ACTIVITY TAGS ▾

GROUPS ▾

SENSORS ▾

73 Vulnerabilities

10 most matched vulnerabilities

■ CVE-2015-5627 • Yokogawa Multiple Products Buffer Overflow Vulnerabilities - CVE-2015-5627 2 affected components ■ CVE-2020-5609 • Path Traversal Vulnerability in Yokogawa CENTUM 2 affected components ■ CVE-2019-10936 • Denial-of-Service Vulnerability in Profinet Devices 3 affected components ■ CVE-2017-12741 • Multiple Siemens Products CVE-2017-12741 Denial of Service Vulnerability 3 affected components ■ CVE-2018-16196 • Yokogawa Vnet/IP Open Communication Driver Vulnerabilities 2 affected components	■ CVE-2014-0781 • Yokogawa CENTUM 'BKCLogSvr.exe' Heap Based Buffer Overflow... 2 affected components ■ CVE-2014-3888 • Yokogawa CENTUM BKFSim_vhfd.exe Buffer Overflow - Packet Storm 2 affected components ■ CVE-2019-13940 • Uncontrolled Resource Consumption Vulnerability in Siemens SIMATIC S7 2 affected components ■ CVE-2017-2680 • Multiple Denial of Service Vulnerabilities on Siemens devices using the... 3 affected components ■ CVE-2019-5909 • Yokogawa License Manager Service Vulnerabilities 2 affected components
---	---

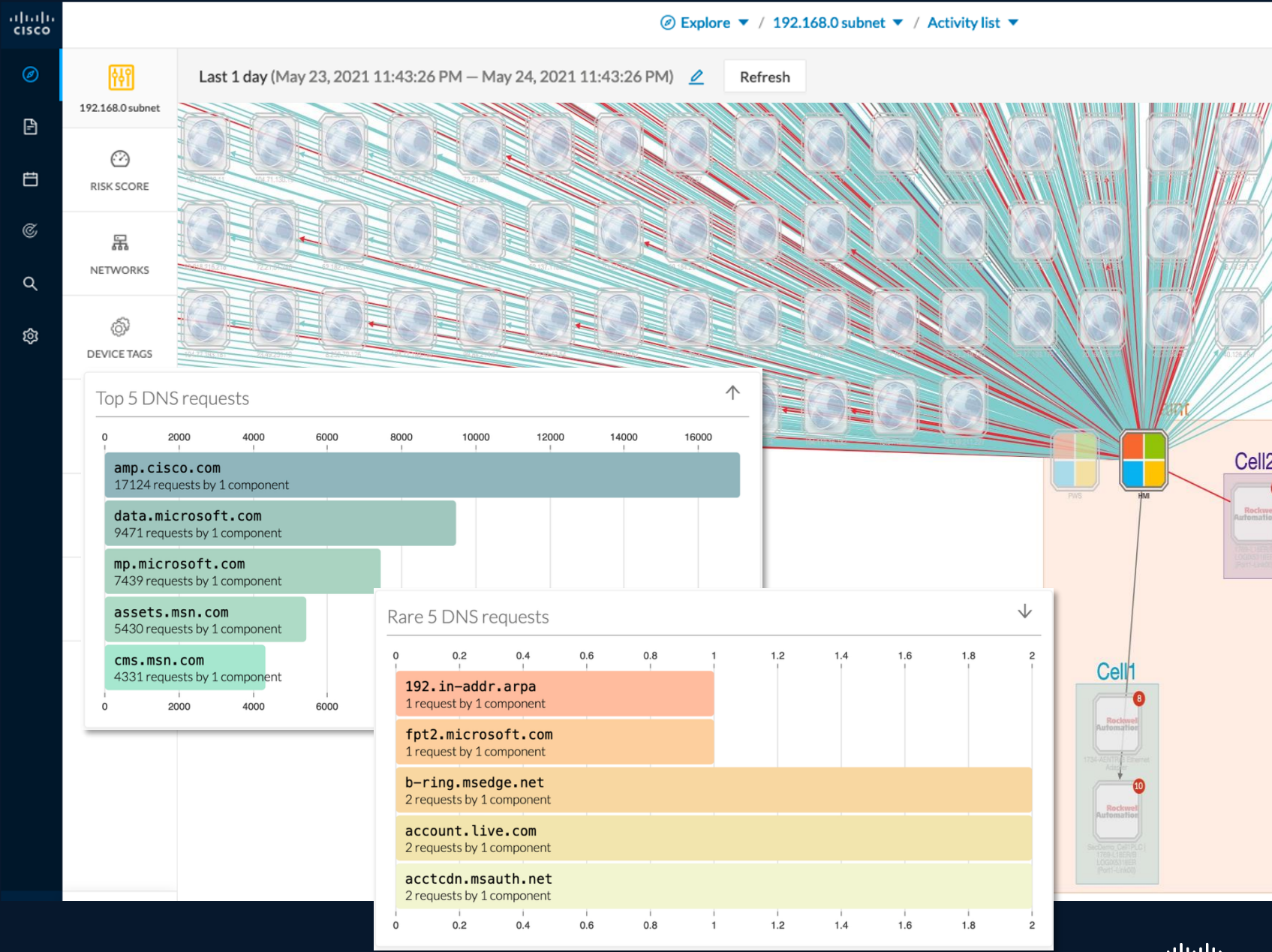
Vulnerability severity legend:
■ NONE
 ■ LOW
 ■ MEDIUM
 ■ HIGH
 ■ CRITICAL

Vulnerability title	CVE	CVSS score	Affected components
Multiple Denial of Service Vulnerabilities on Siemens devices using the PROFINET Discovery and Configuration Protocol	CVE-2017-2680	6.5 (v3)	3
Multiple Siemens Products CVE-2017-12741 Denial of Service Vulnerability	CVE-2017-12741	7.5 (v3)	3
Denial-of-Service Vulnerability in Profinet Devices	CVE-2019-10936	7.5 (v3)	3
Yokogawa CENTUM 'BKHOdeq.exe' Stack Based Buffer Overflow Vulnerability	CVE-2014-0783	9.0 (v2)	2
Yokogawa CENTUM BKFSim_vhfd.exe Buffer Overflow - Packet Storm	CVE-2014-3888	8.3 (v2)	2
Schneider Electric Modicon Modbus Protocol Multiple Authentication Bypass Vulnerabilities	CVE-2017-6032	5.3 (v3)	2
Yokogawa CENTUM 'BKESimmgr.exe' Stack Based Buffer Overflow Vulnerability	CVE-2014-0782	0.0 (v2)	2

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









Today

Auto-follow ☐

17 499 579 637

category Signature based Detection X severity veryhigh X

Search an event

Day Week

16:12:09.236 Signature based Detection Snort allow on TCP id 27679 with signature A Network Trojan was detected

Snort Event

- Occurred at: 10/04-14:44:21.061415
- Sensor: SENSORVM-INT17233
- Action: allow
- Gid: 1
- Signature ID: 27679
- Priority: 1
- Rule: 1:27679:4 (Revision4)
- Classification: A Network Trojan was detected

- In network interface: /data/tmp/BIN_KuluoZ-Asprox_9F842AD20C50AD1AAB41F20B321E
- Message: MALWARE-CNC Win.Trojan.KuluoZ variant outbound connection
- From 192.168.248.165:2538 To 85.214.114.16:8080 (00:0C:29:D9:6F:DB -> 00:50:00:00:00:00)
- Protocol: TCP
- Direction: C2S
- Ethernet type: 0x800
- Service: unknown
- VLAN: 0

Related data: [DOWNLOAD DATA](#)

16:12:18.255 Signature based Detection Snort allow on TCP id 42339 with signature Attempted Information Leak

Snort Event

- Occurred at: 04/17-16:17:01.746538
- Sensor: SENSORVM-INT17233
- Action: allow
- Gid: 1
- Signature ID: 42339
- Priority: 2
- Rule: 1:42339:3 (Revision3)
- Classification: Attempted Information Leak

- In network interface: /data/tmp/eternalromance-success-2008r2.pcap
- Message: OS-WINDOWS Microsoft Windows SMB possible leak of kernel heap memory
- From 172.23.33.10:445 To 10.99.99.8:51661 (00:0C:29:9E:89:5F -> 00:2A:E3:CC:A2)
- Protocol: TCP
- Direction: S2C
- Ethernet type: 0x800
- Service: netbios-ssn
- VLAN: 0

Related data: [DOWNLOAD DATA](#)

16:12:18.258 Signature based Detection Snort allow on TCP id 50626 with signature Attempted Administrator Privilege Gain

Snort Event

- Occurred at: 04/17-16:17:01.754745
- Sensor: SENSORVM-INT17233
- Action: allow
- Gid: 1
- Signature ID: 50626
- Priority: 1
- Rule: 1:50626:1 (Revision1)
- Classification: Attempted Administrator Privilege Gain

- In network interface: /data/tmp/eternalromance-success-2008r2.pcap
- Message: OS-WINDOWS Microsoft Windows raw WriteAndX InData pointer attempt
- From 10.99.99.8:51661 To 172.23.33.10:445 (00:2A:E3:CC:A2:2E -> 00:00:00:00:00:00)
- Protocol: TCP
- Direction: C2S
- Ethernet type: 0x800
- Service: netbios-ssn
- VLAN: 0

Related data: [DOWNLOAD DATA](#)

© 2026 Cisco and/or its affiliates. All rights reserved.



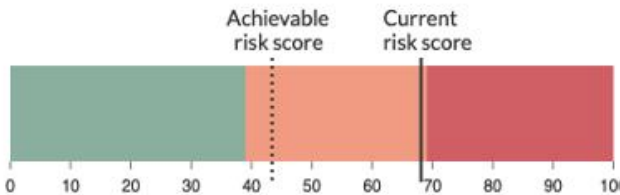
Cyber Vision

Track your Risk Exposure

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



Overview



The best achievable score is 44
It can be reached by patching all vulnerabilities and removing insecure traffic.

Details

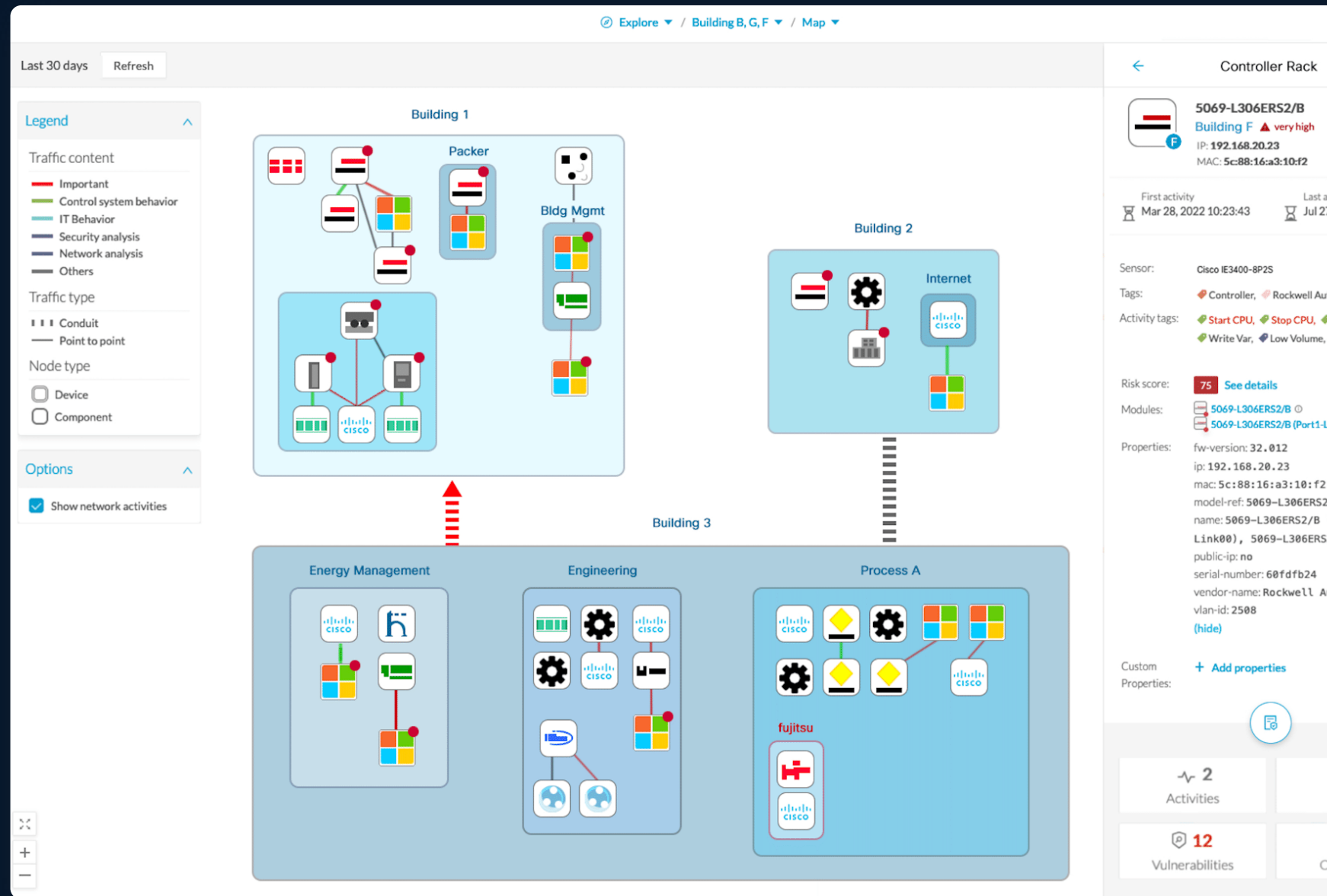
The score was computed on May 24, 2021 10:00:06 PM by Cisco Cyber Vision as follows:

Criteria	Matching	Distribution	Des
Device type	SCS0102 type: Controller	13%	CC cou
Group impact	SCS0102 group: Building K. It has an industrial impact ▲ very high.	51%	
Activities	No matching activity	0%	
Vulnerabilities	SCS0102 most impacting vulnerability is Path Traversal Vulnerability in Yokogawa CENTUM	36%	Pat Yok CVI CV: Suc vuln una ...sh See

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

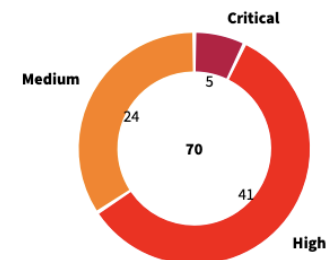


Measure progress with reports

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

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

Page 3

Key Findings

Filter Criteria: All data Preset

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

Risk score	Total Deviation
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 domains to access internal devices. The table below depicts those devices 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 devices 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 the security events found on the devices in the - by Cisco Cyber

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 with
High	47 devices have been remotely acc
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.	

New Features

Cyber Vision New UI

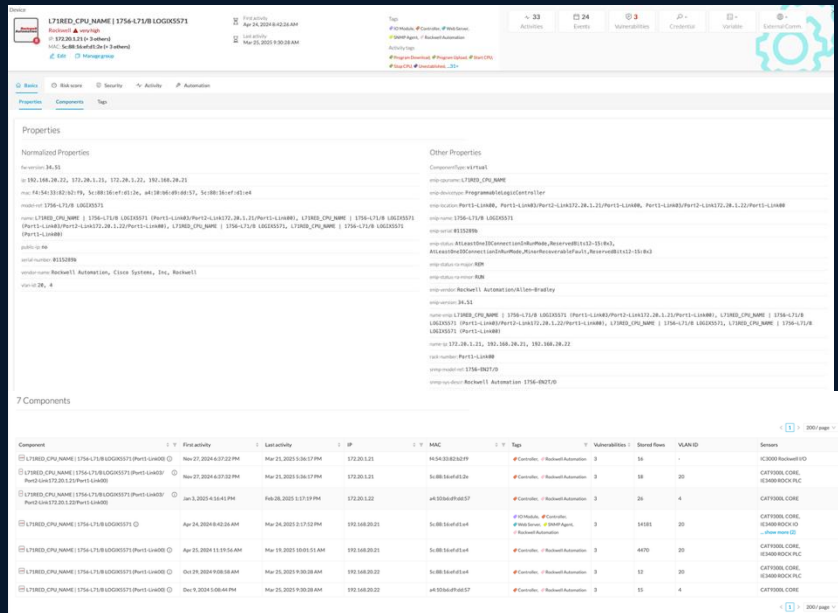
- **Why are we building a new UI?**

- 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)

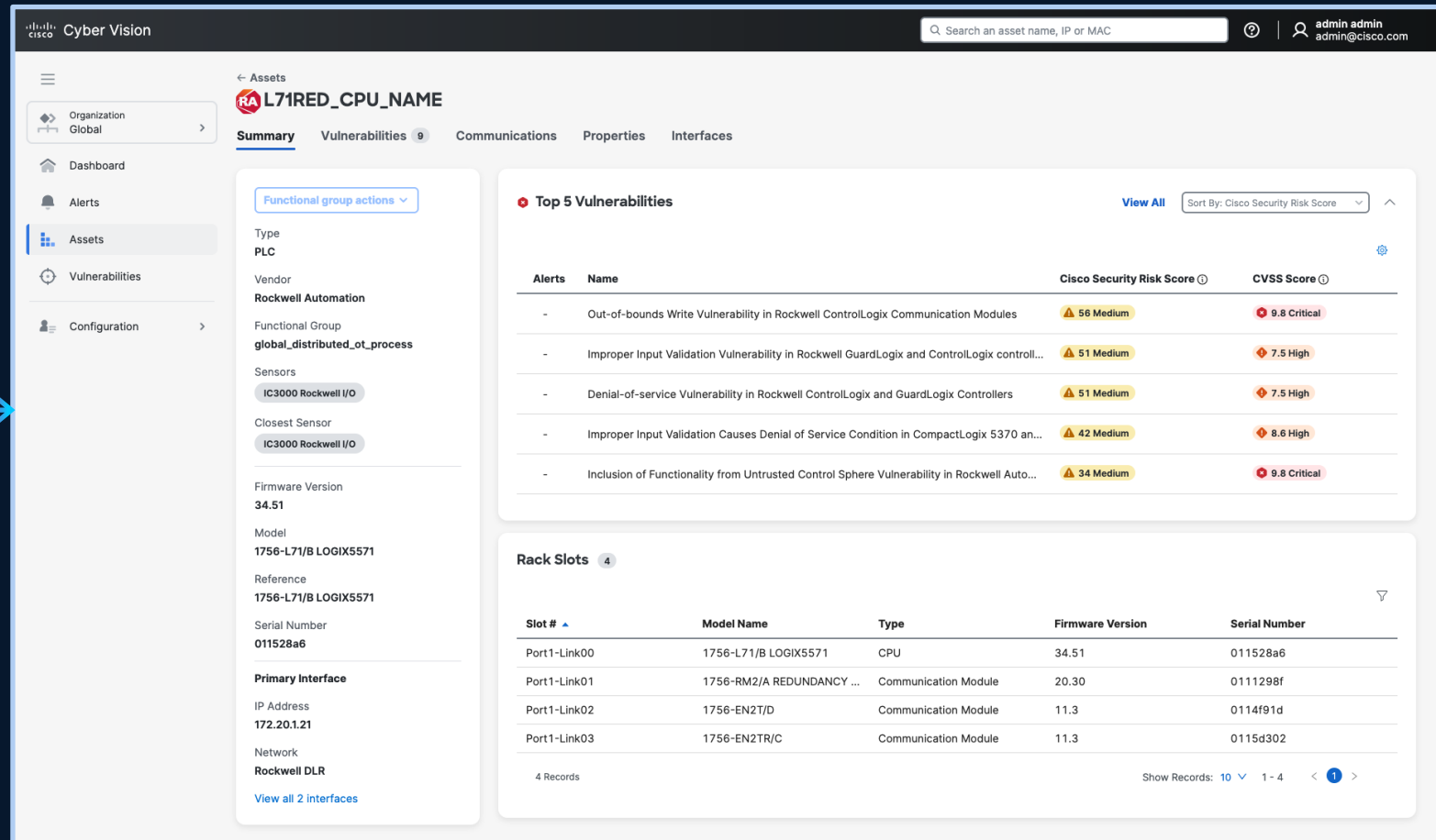
- **How can I access this new UI?**

- 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**



Assets

L71RED_CPU_NAME

Summary Vulnerabilities 9 Communications Properties Interfaces

Organization: Global

Dashboard Alerts Assets Vulnerabilities Configuration

Functional group actions

Type: PLC

Vendor: Rockwell Automation

Functional Group: global_distributed_ot_process

Sensors: IC3000 Rockwell I/O

Closest Sensor: IC3000 Rockwell I/O

Firmware Version: 34.51

Model: 1756-L71/B LOGIX5571

Reference: 1756-L71/B LOGIX5571

Serial Number: 011528a6

Primary Interface: Rockwell DLR

View all 2 interfaces

Top 5 Vulnerabilities

Alerts	Name	Cisco Security Risk Score	CVSS Score
-	Out-of-bounds Write Vulnerability in Rockwell ControlLogix Communication Modules	56 Medium	9.8 Critical
-	Improper Input Validation Vulnerability in Rockwell GuardLogix and ControlLogix controll...	51 Medium	7.5 High
-	Denial-of-service Vulnerability in Rockwell ControlLogix and GuardLogix Controllers	51 Medium	7.5 High
-	Improper Input Validation Causes Denial of Service Condition in CompactLogix 5370 an...	42 Medium	8.6 High
-	Inclusion of Functionality from Untrusted Control Sphere Vulnerability in Rockwell Auto...	34 Medium	9.8 Critical

Rack Slots

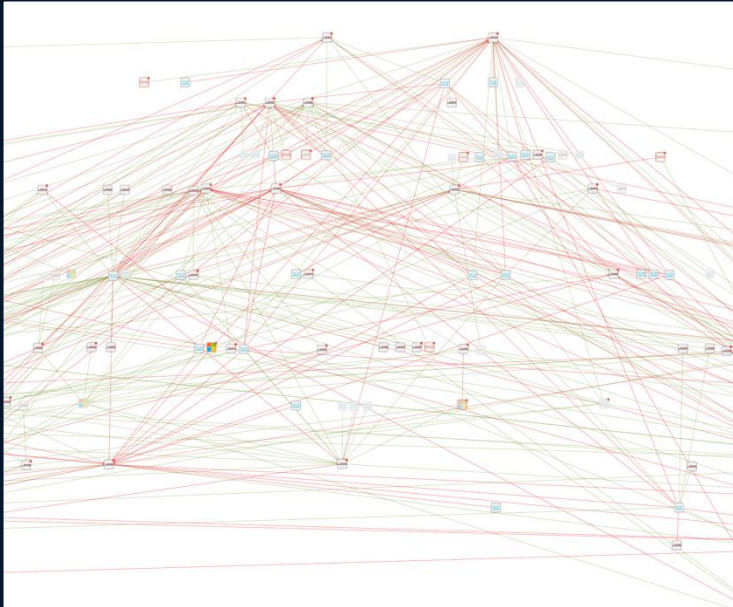
Slot #	Model Name	Type	Firmware Version	Serial Number
Port1-Link00	1756-L71/B LOGIX5571	CPU	34.51	011528a6
Port1-Link01	1756-RM2/A REDUNDANCY ...	Communication Module	20.30	0111298f
Port1-Link02	1756-EN2T/D	Communication Module	11.3	0114f91d
Port1-Link03	1756-EN2TR/C	Communication Module	11.3	0115d302

4 Records

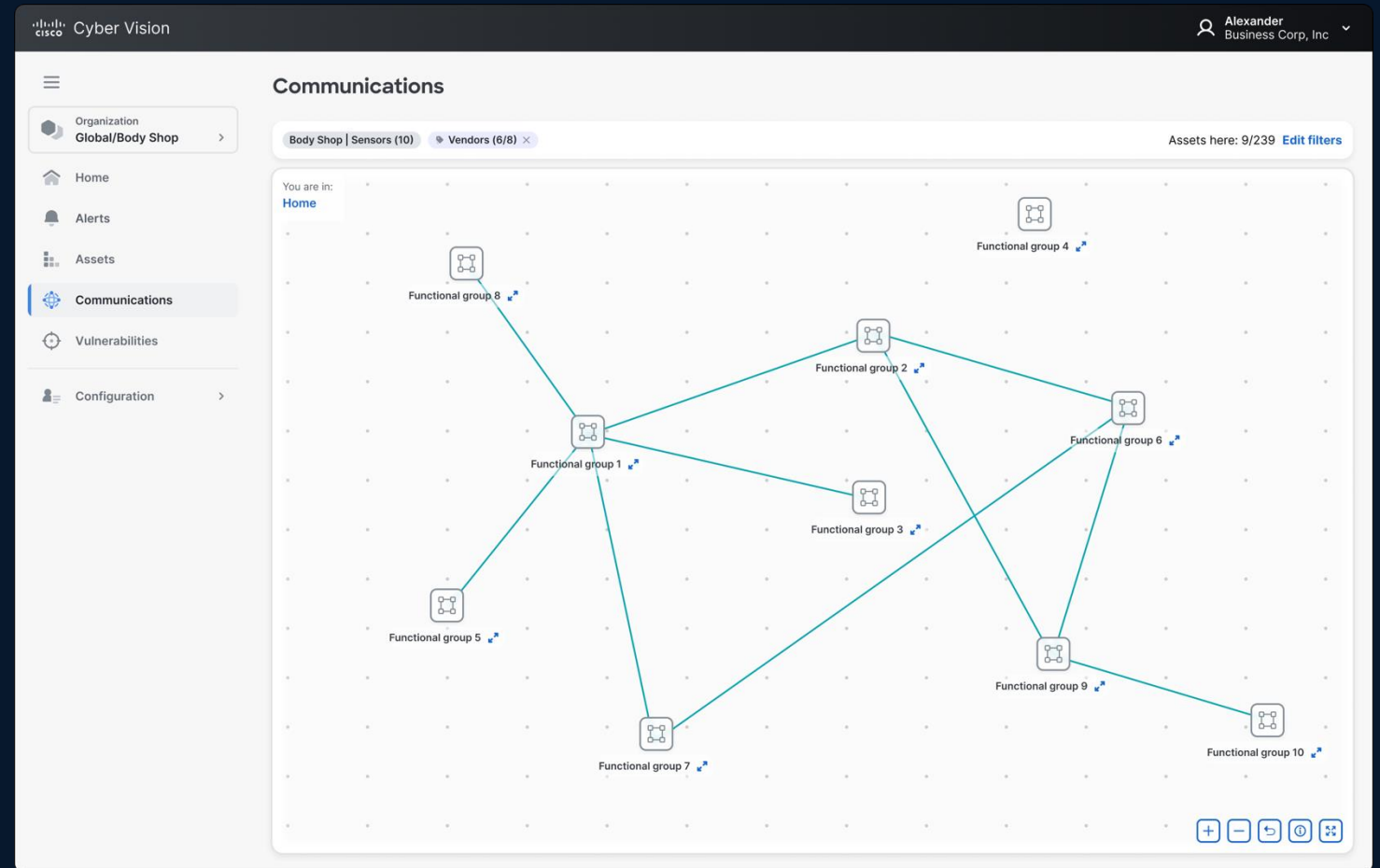
Show Records: 10 1 - 4

New UI only surface **meaningful information**

Introducing AI-driven asset auto-grouping



OT asset inventory projects highlight flat, unsegmented networks

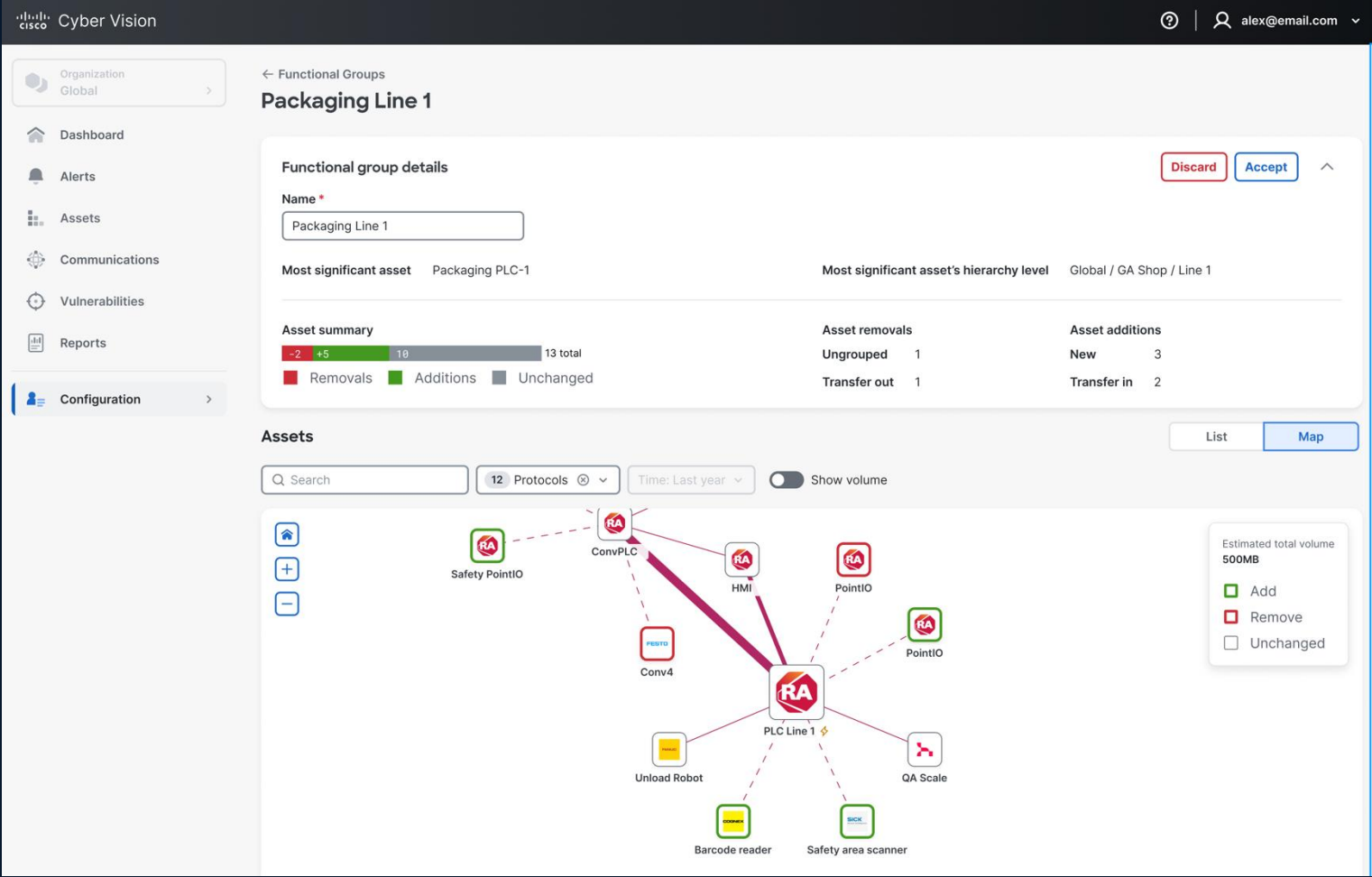
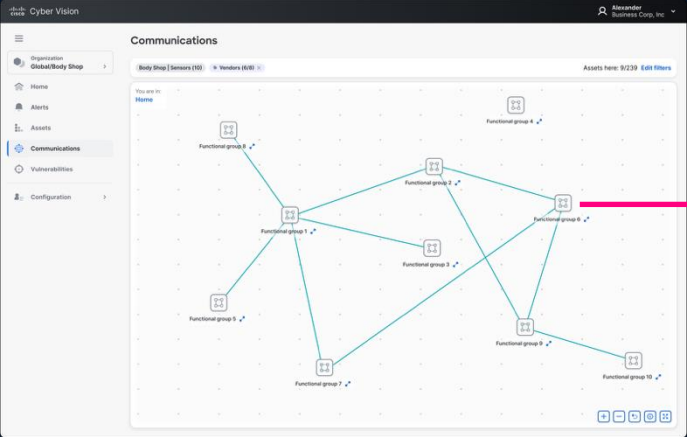


Cisco Cyber Vision ML-driven auto-grouping automatically creates security zones to drive network segmentation using Firewalls or NAC

Introducing AI-driven asset auto-grouping

Detailed view of assets within a group

Group-to-group overview



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

ADMIN3 ADMIN_4 **LINE1 PRESETS**

LINE1 PRESETS

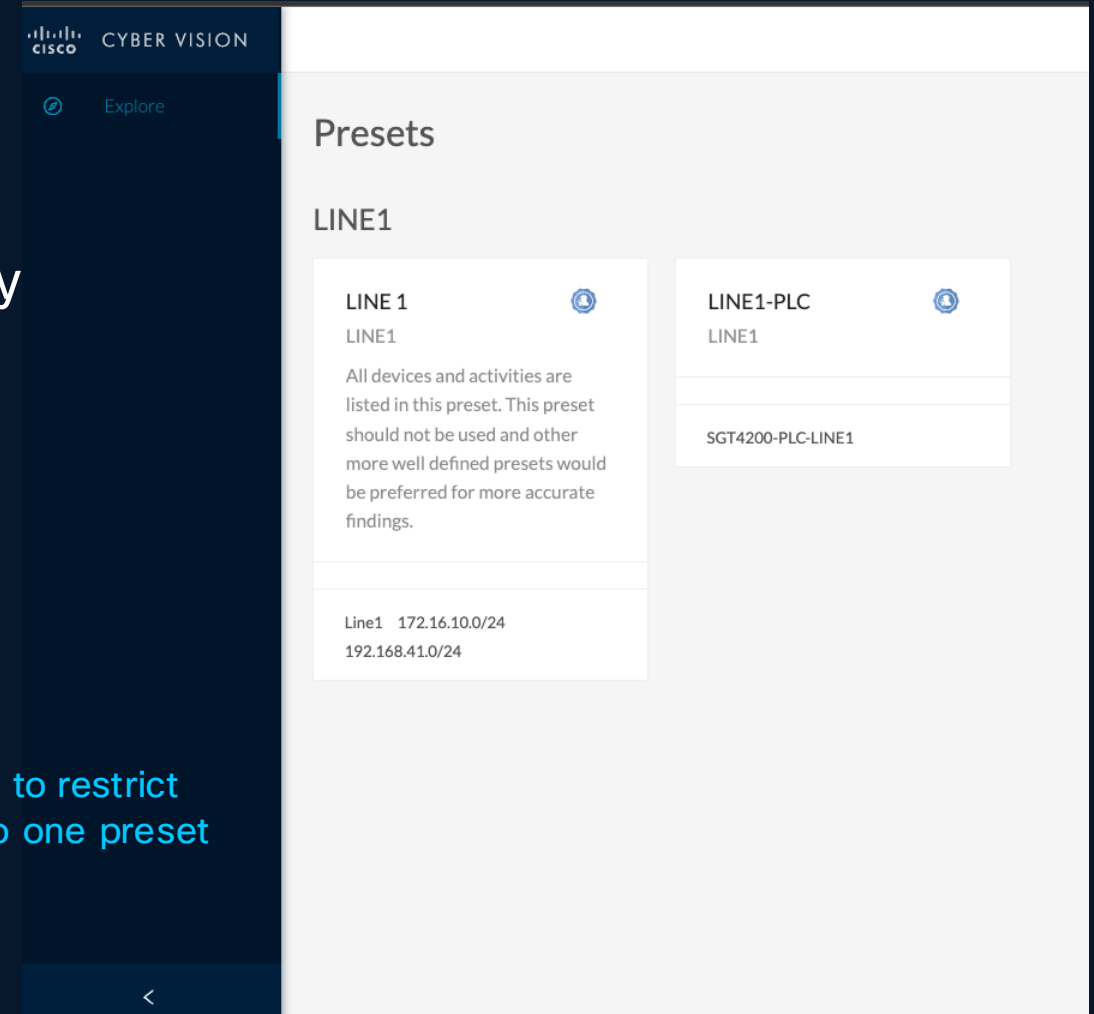
☒ Restrict user access to a single preset category.

Select a Preset Category

LINE1

New feature to restrict navigation to one preset category

Category selected



Sensor GPS coordinates

Goals:

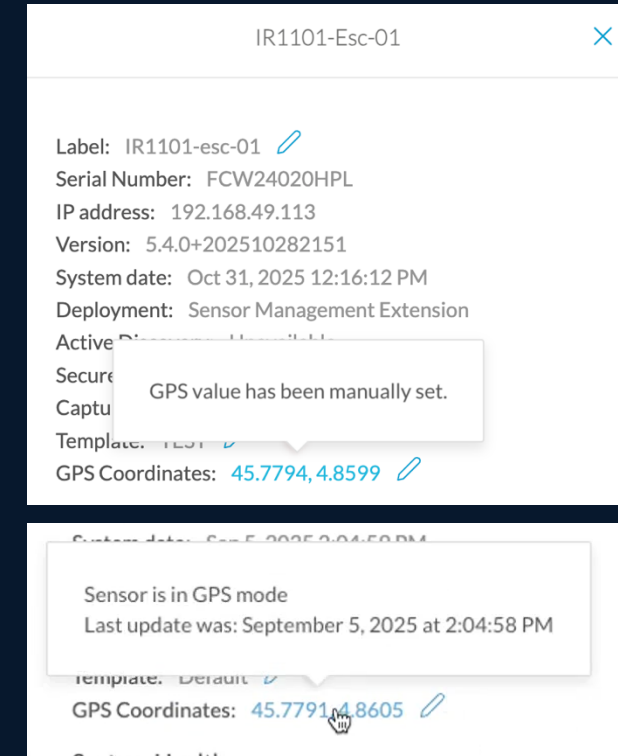
- Add GPS coordinates to sensor/platform

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



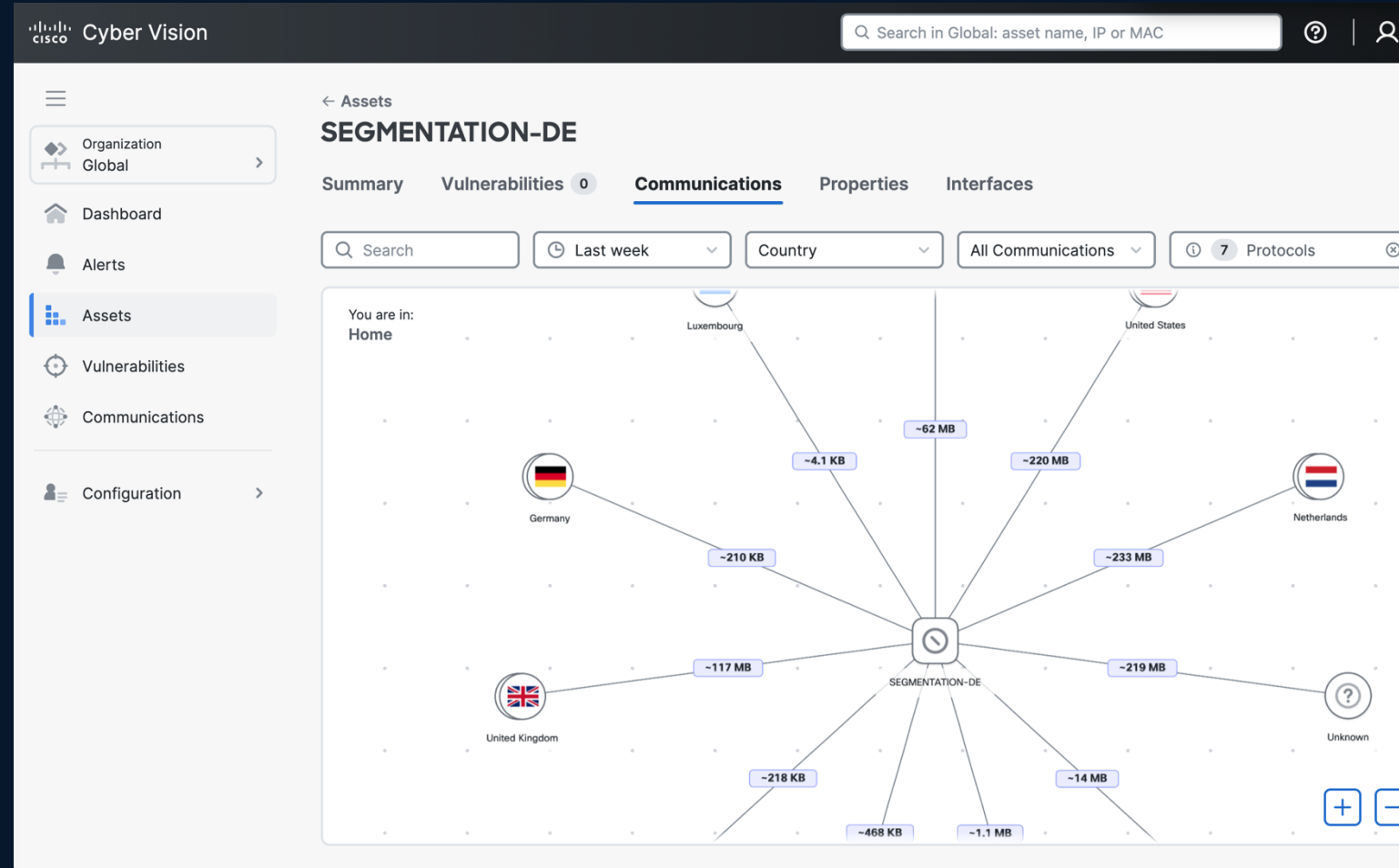
Quickly map all communication flows
Map external connections to specific countries for threat context



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



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

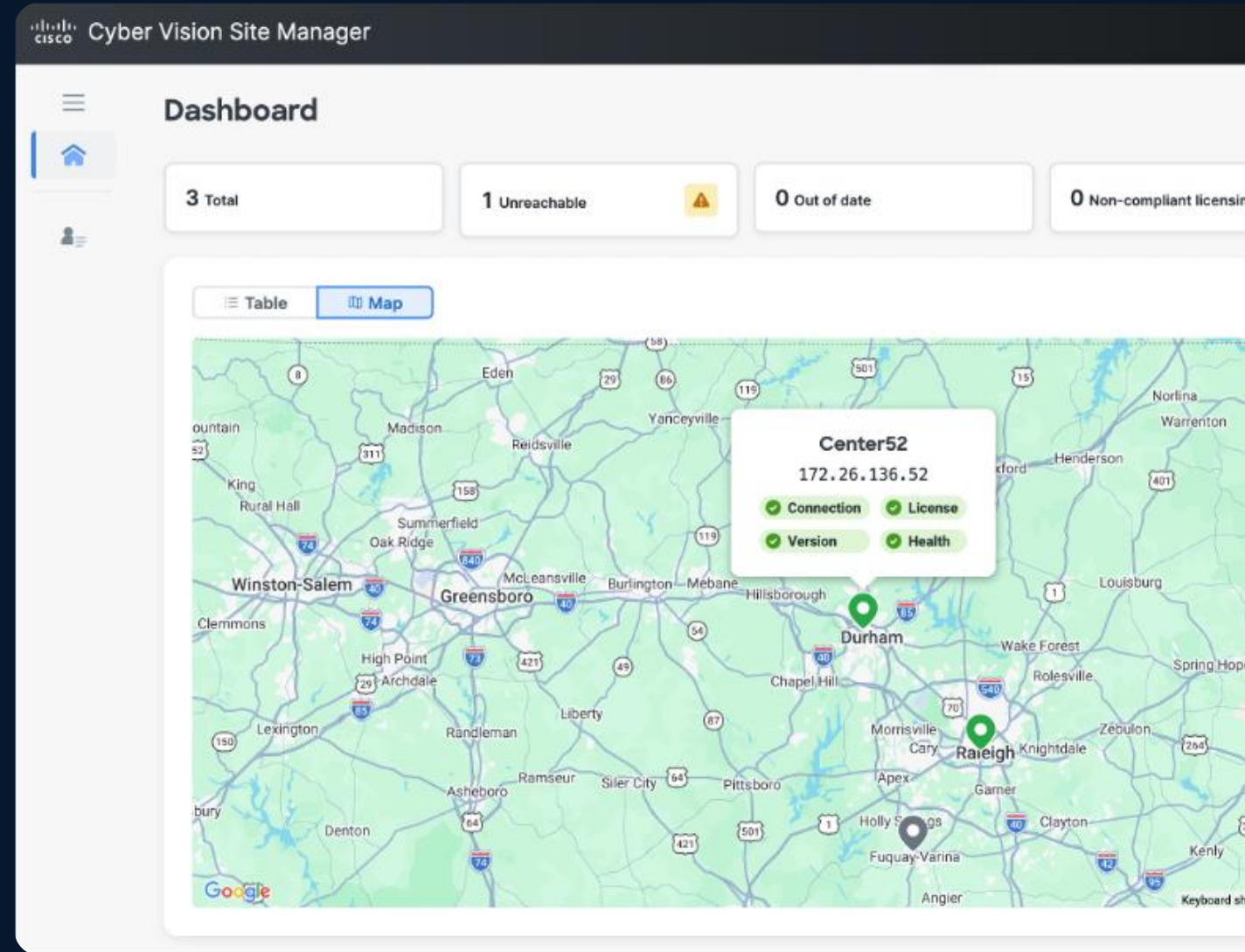


New Cisco Cyber Vision Site Manager

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

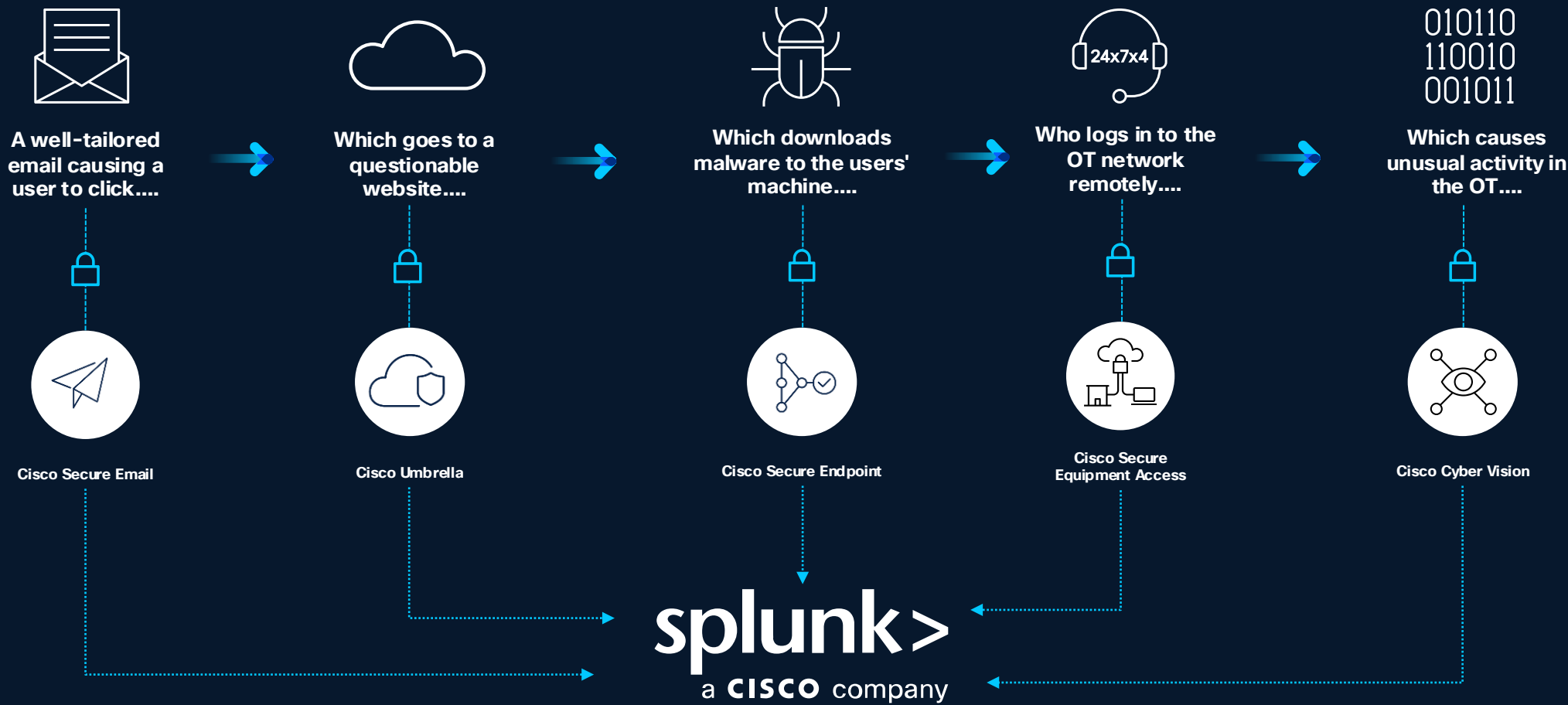
Give security teams time back
to effectively manage cyber risk



Splunk & OT

A siloed approach is not enough to secure OT

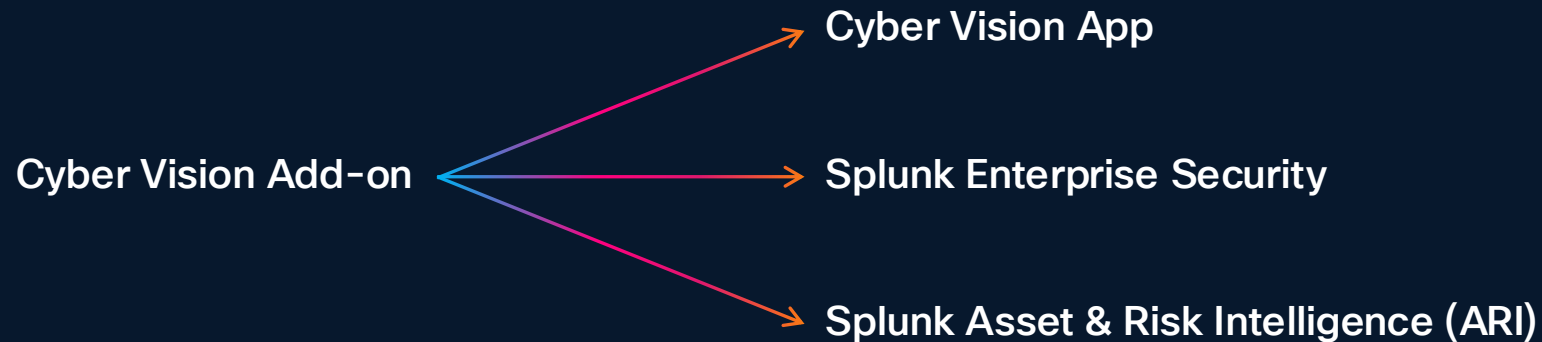
Detecting threats requires cross-domain visibility



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

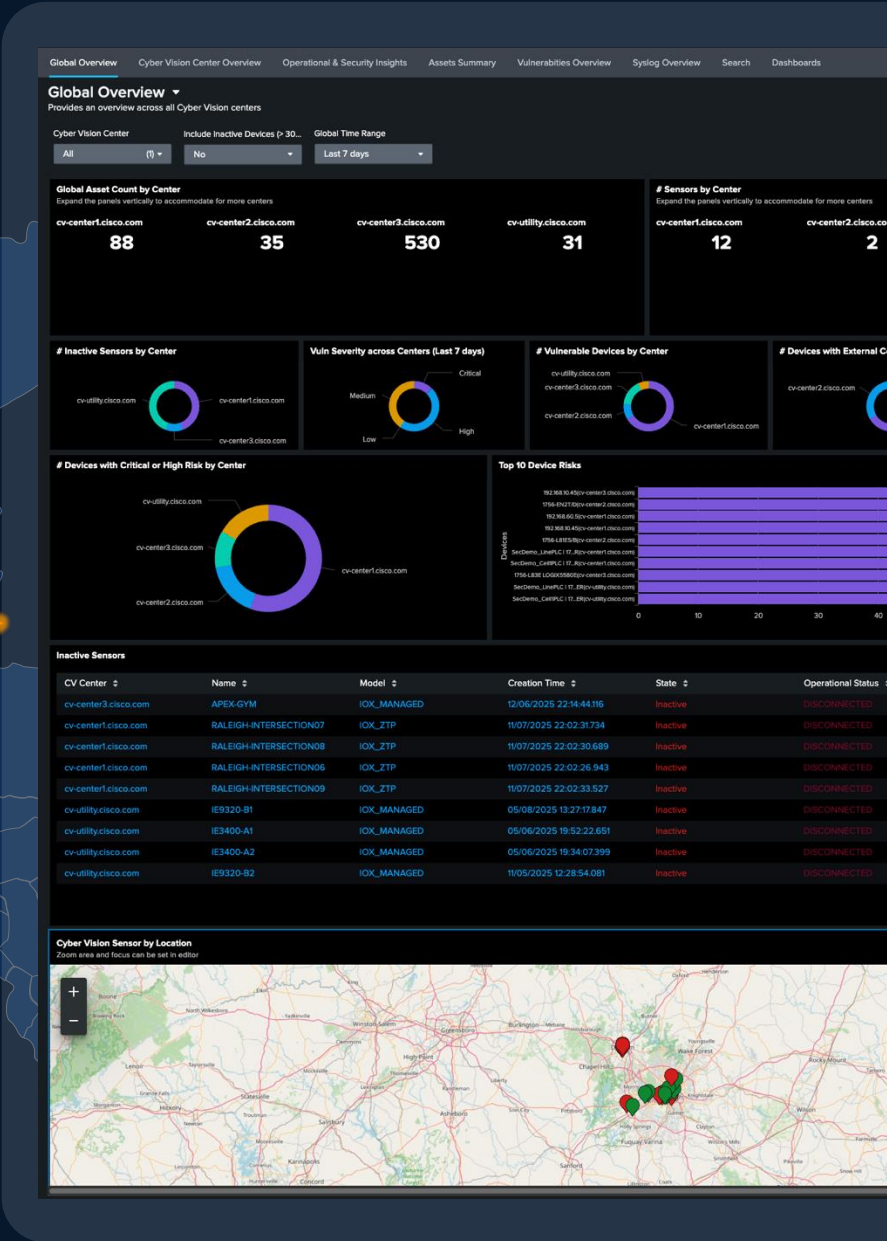
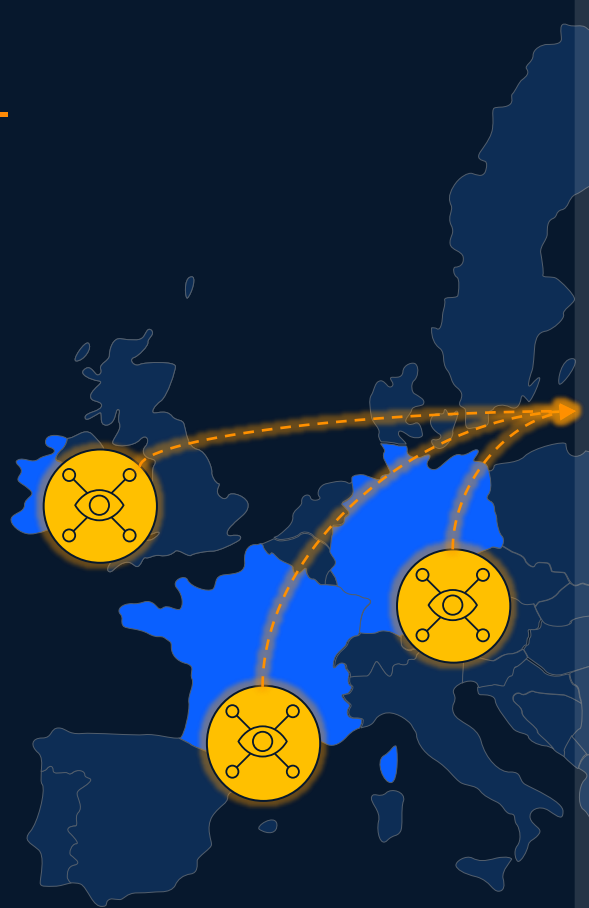
Cyber Vision Add-on is a background process that contains data parsing rules, field extractions, and configurations to ingest data from Cyber Vision correctly

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

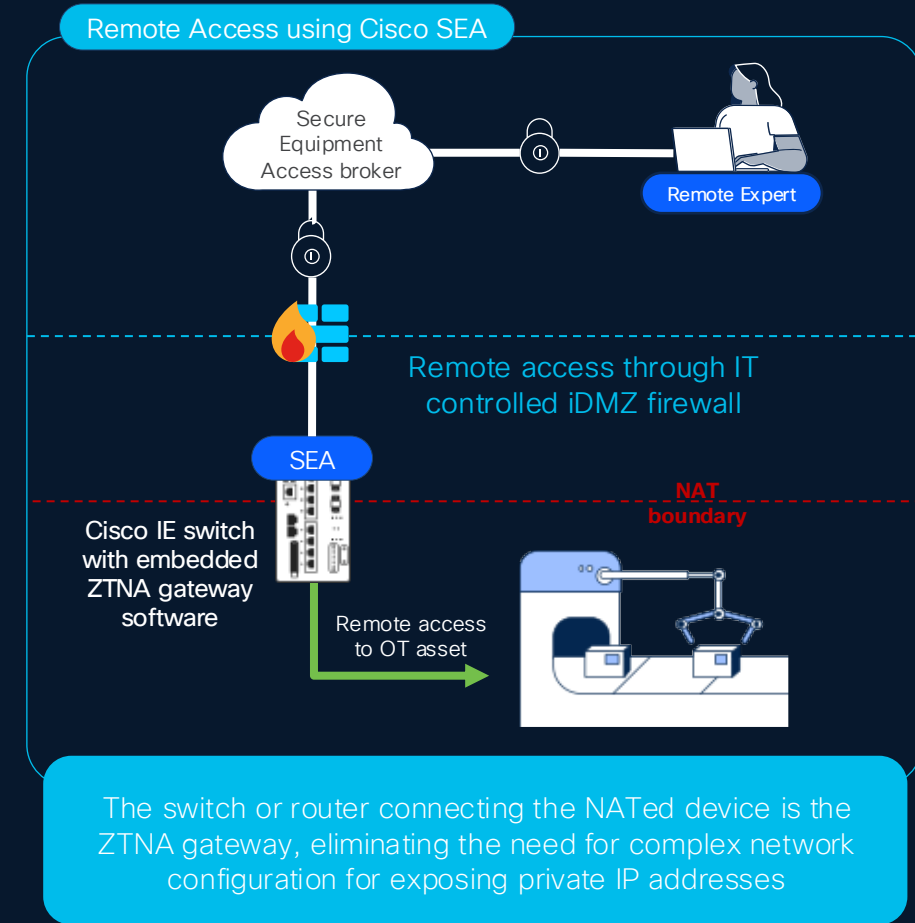
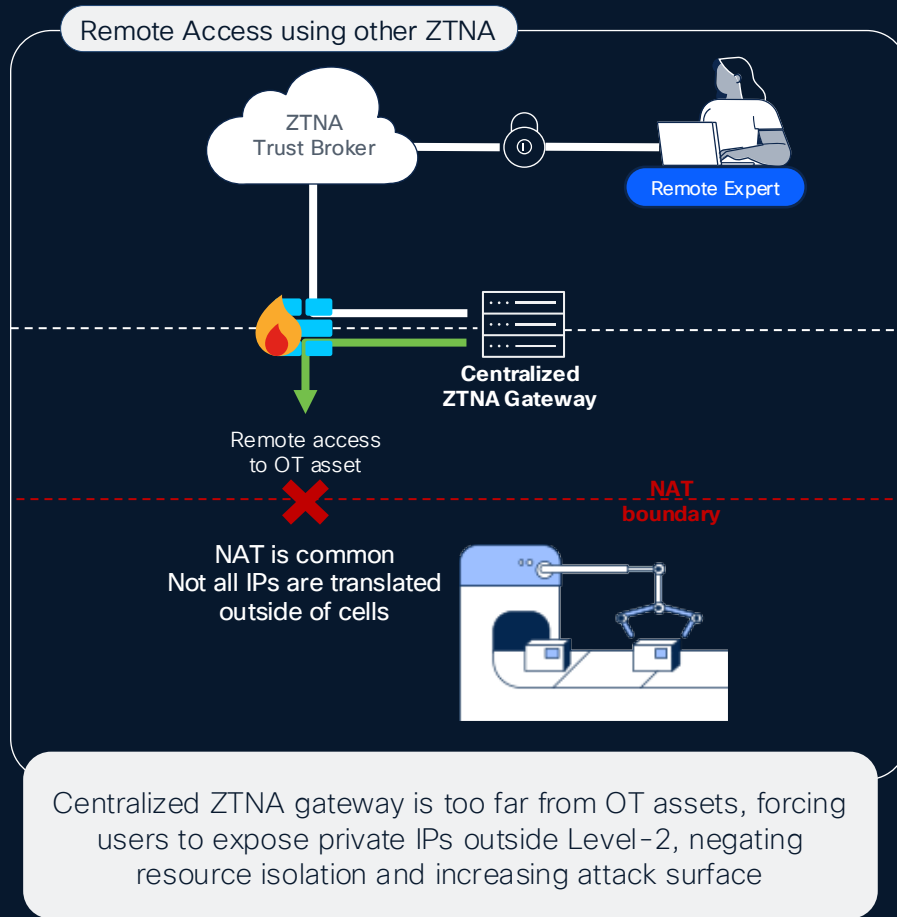


Easy to Deploy and Manage at Scale

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



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

Secure Equipment Access

Some configuration parameters already exist in the database. Click on the button

☐ Without SEA
☒ With SEA

SEA proxy configuration

☒ Use the Center as Proxy ☐ Direct ☐ Proxy Form

Configuration

* Region
Europe

Organization Name
ccv team

* Organization ID
f90be2a2

* API Key ID
ccv team

* API Key Secret

Reset

Folders and sensors (1)

Filter 0 Selected Move selection to More Actions As of: Jun 25, 2025 6:17 PM

☐	Label	Serial Number	IP Address	Version	Update status	Location	Health status	Processing status	Active Discovery	Secure Equipment Access
☐	FOC2417V07Z	FOC2417V07Z	192.168.49.136	5.3.0	✓		Connected	Normally processing	Enabled	Enabled

☐	Network Device Name	SEA Agent Installed By	SEA Agent Connection	Agent Version
☐	IE-3400-8T2S+FOC2417V07Z	Cyber Vision	✓ Up	0.85-06210c

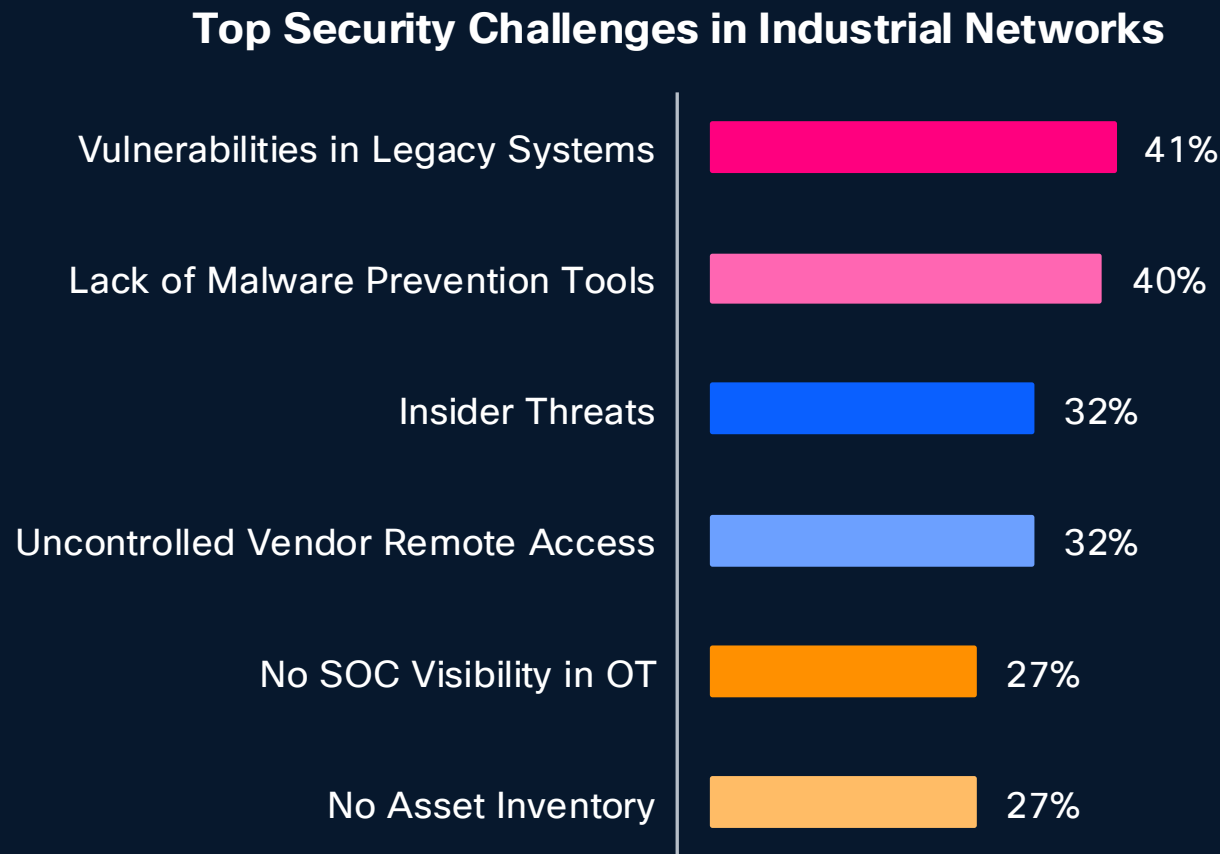
Segmentation



Many industrial networks have not moved from visibility to protection

Challenge Statistics

OT Security Challenges - What Operators Actually Face



Source: [Cisco 2024 State of Industrial Networking Report](#)

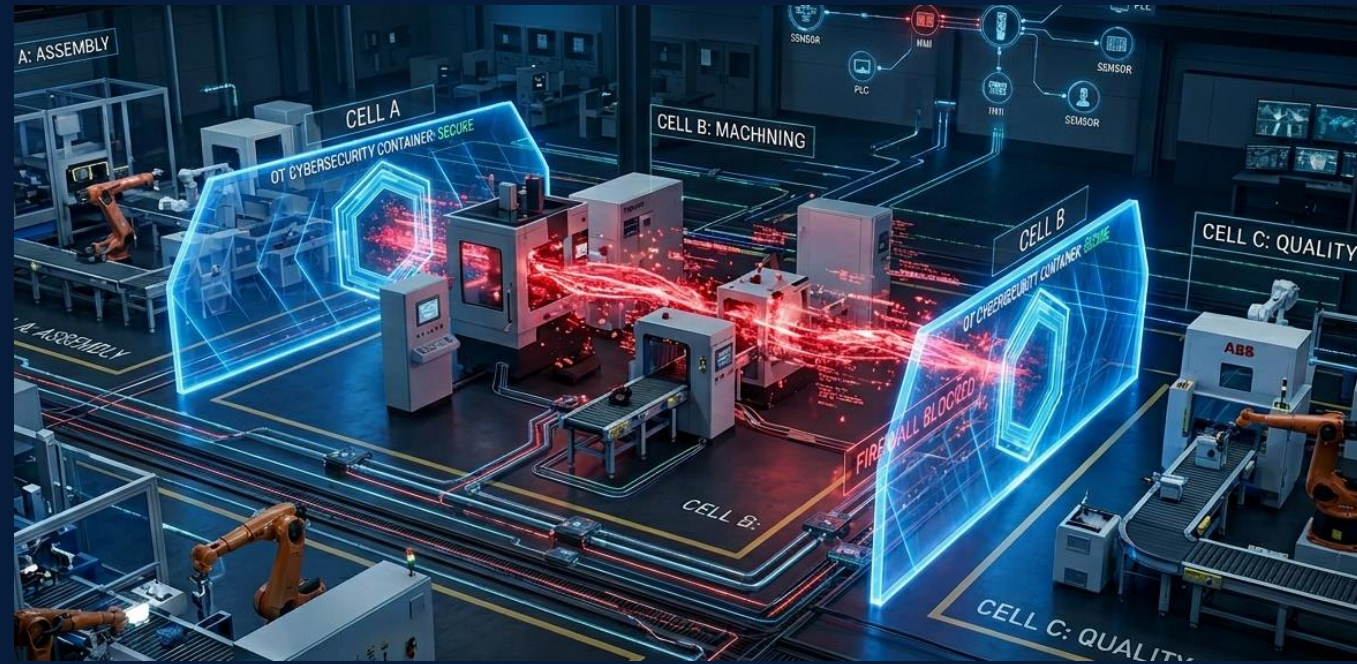


Segmentation mitigates 5 of 6 challenges:

- 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



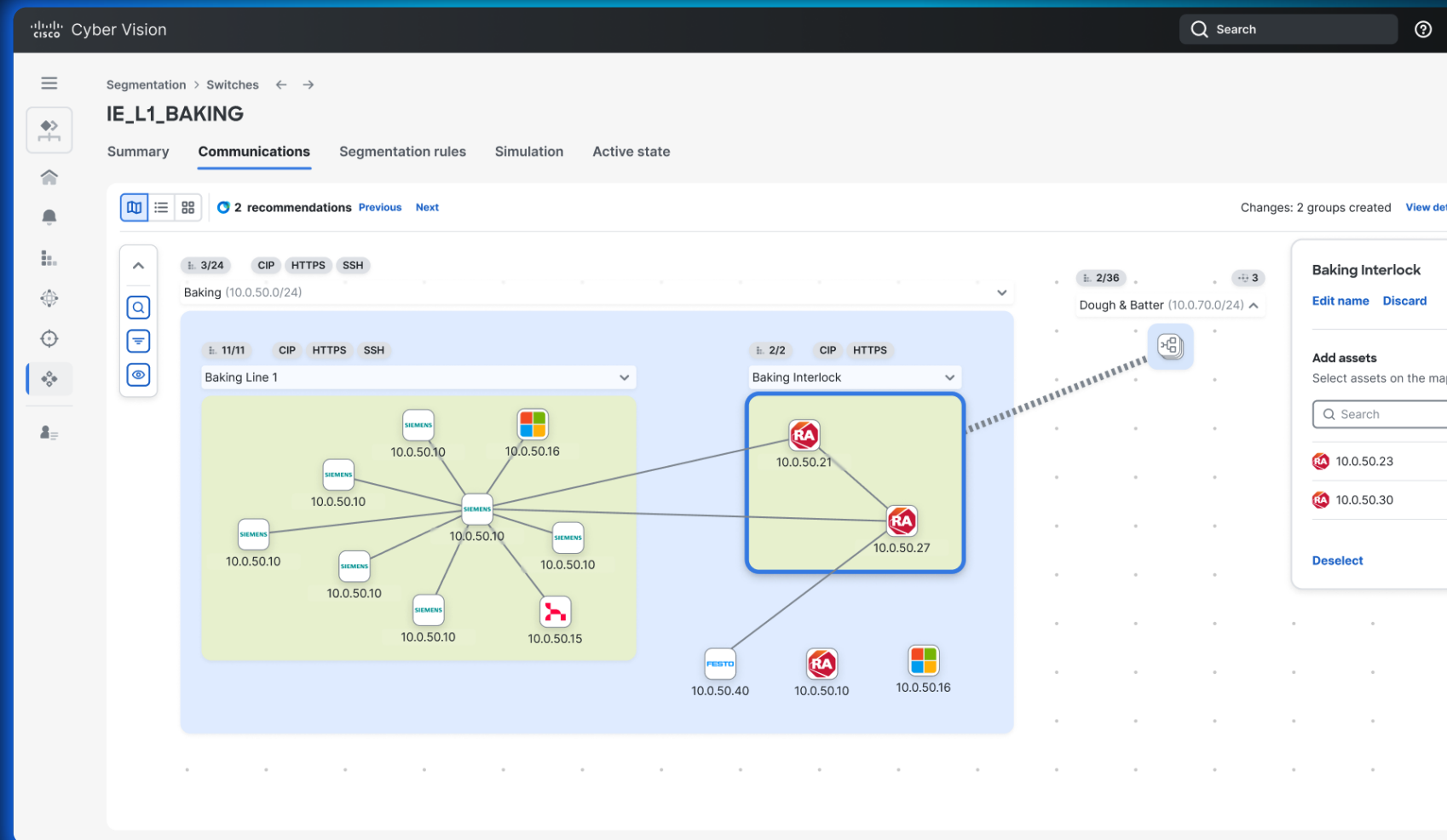
Zones & Conduits

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

The screenshot displays the Cisco Cyber Vision interface for managing segmentation rules. The main panel shows the 'IE_L1_BAKING' rule set under the 'Segmentation rules' tab. It lists three rules: 'Baking' (updated), 'Baking interlock' (new), and 'Baking interlock' (updated). The right panel shows the 'Baking ↔ Baking interlock' rule recommendation, which is currently set to 'Deny' and is in use by '1 switch'. The 'Edit recommendation' section shows the rule configuration for 'Baking interlock → Cooling' and 'Cooling → Baking interlock'. The 'Inline' tab is selected, showing the generated ACL rules for the recommendation.

Segmentation rules

Inter-group rules 9 Intra-group rules 9 Common service rules 2

Search Asset groups Action Protocol Recommendations Filter

Recommendation	Asset group	↔	Asset group	Action
☐ Update	Baking	↔	Baking interlock	Allow
☐ New	Baking interlock	↔	Cooling	Allow
☐ Update	Baking interlock	↔	Dough & Batter	Allow

Default rule ① Deny

Baking ↔ Baking interlock

Segmentation rule recommendation

Action Catch all action In use

Allow Deny 1 switch

Edit recommendation

Baking interlock → Cooling ①

CIP HTTPS SSH

Cooling → Baking interlock ①

CIP HTTPS SSH Modbus

Inline Side by side

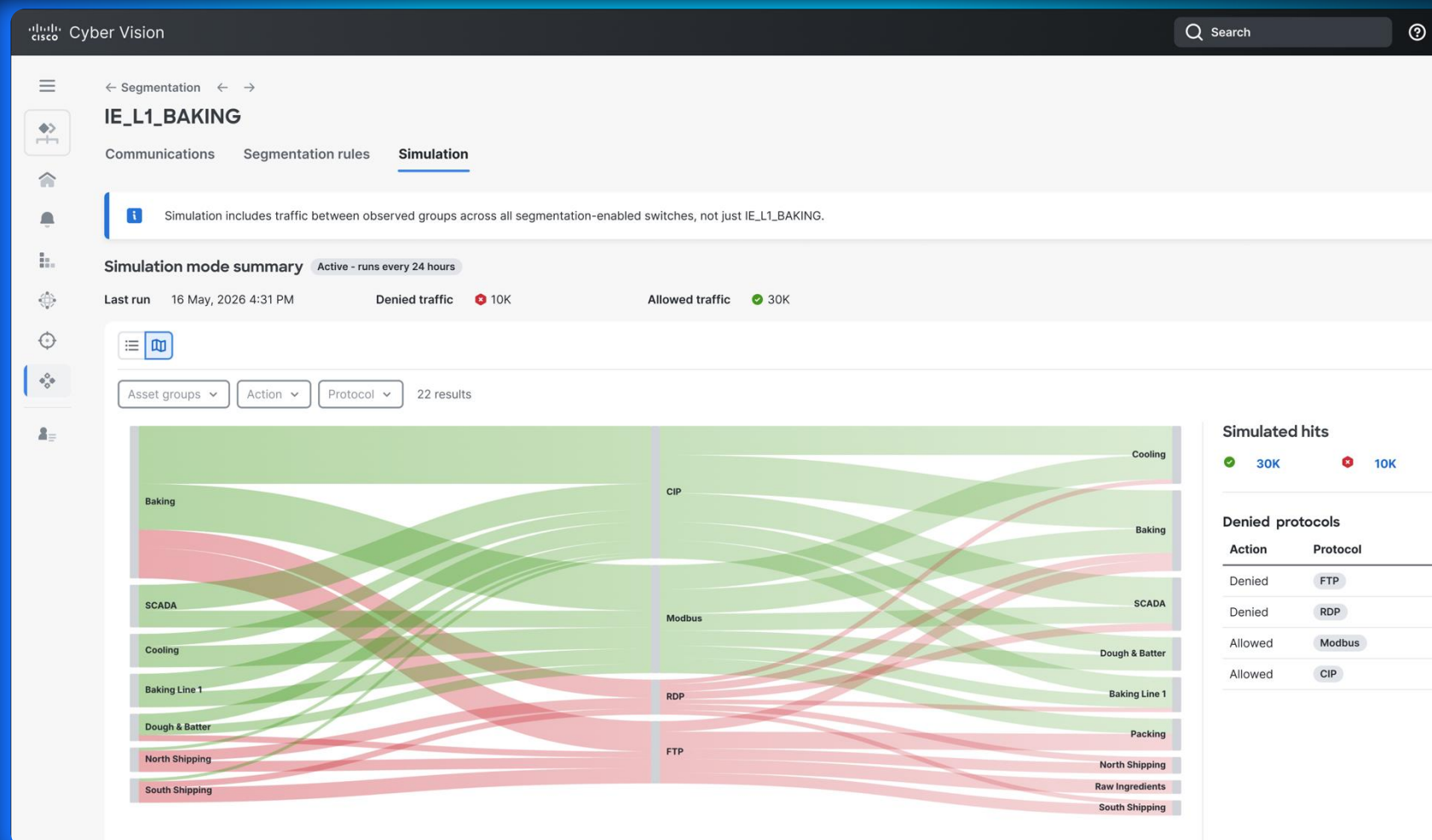
```
1 IPv4 Role-based permissions from group 1 to group 2:
2   ACL_BAKING_TO_INTERLOCK-01
3 IPv4 Role-based permissions from group 2 to group 1:
4   ACL_INTERLOCK_TO_BAKING-02
5
6 --- Baking --> Baking interlock ---
7 permit udp dest eq 2222
8 permit tcp dest eq 443
9 permit tcp dest eq 22
10 permit tcp established
11 deny ip
12
13 --- Baking interlock --> Baking ---
14 permit udp dest eq 2222
15 permit tcp dest eq 443
16 permit tcp dest eq 22
17 permit tcp dest eq 502
18 permit tcp established
19 deny ip
20
```

Cancel Discard recommendation

Cisco Cyber Vision

Segmentation Policy Simulations

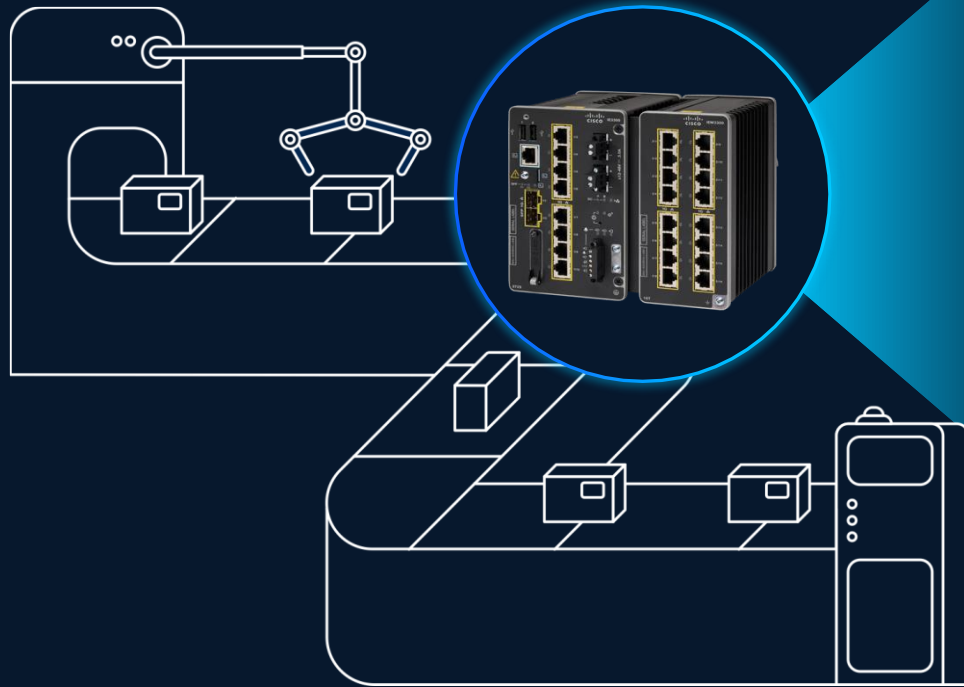
- Simulation shows the impact of rules against live traffic
- Helps identify legitimate traffic being blocked that was missed during rule creation
- Users can modify segmentation policy to fix issues identified



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

