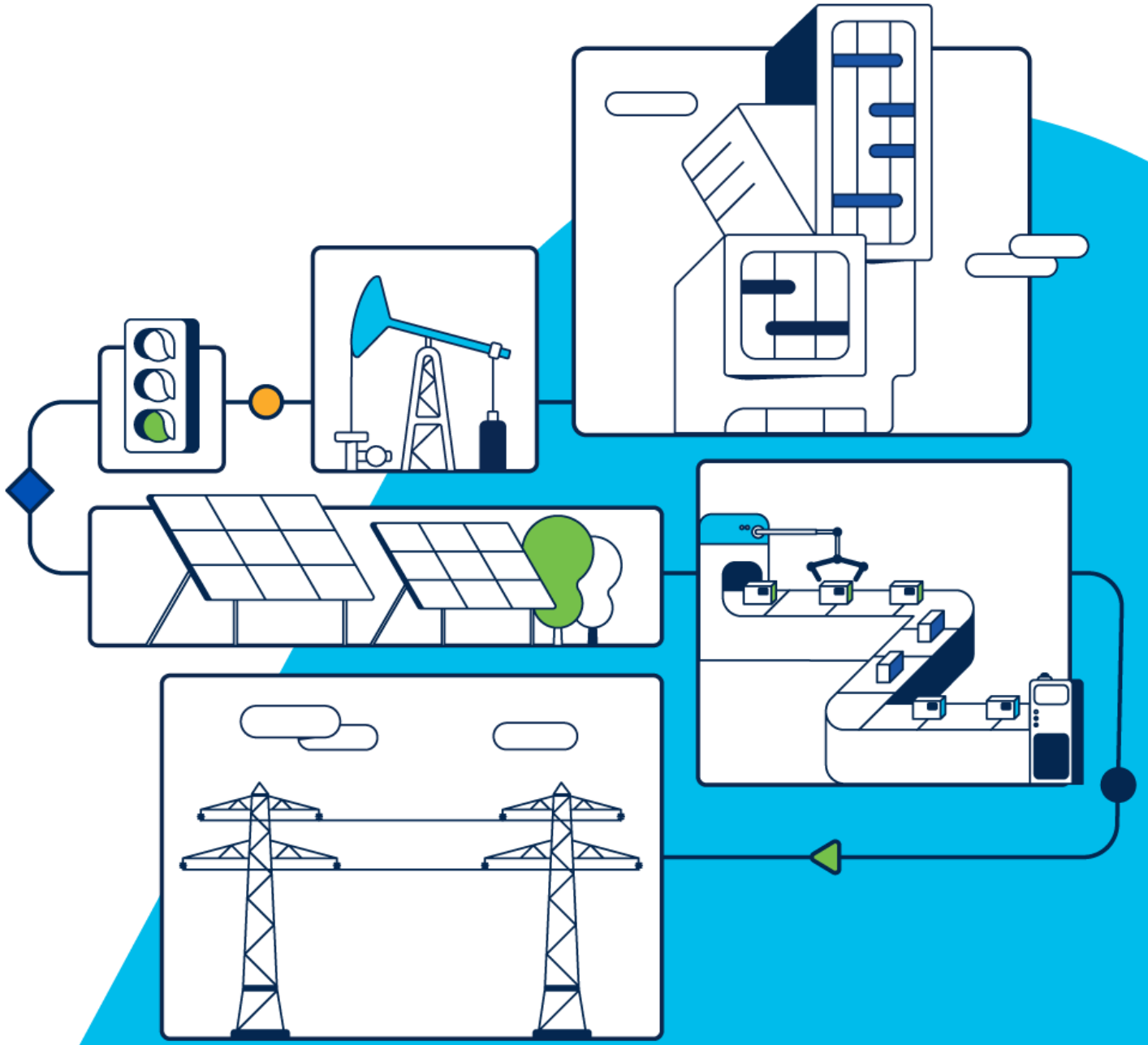
CISCO Industrial

Bratislava 2026

Peter Malic, Cisco
Michal Remper, Soitron



O čom budeme rozprávať

- Cisco Industriálne Portfólio
- OT Security, základné kroky pre zabezpečenie siete
- Cisco Cyber Vision
- Q&A

Industrial IoT networking portfolio Overview

Industrial Ethernet switches
DIN-Rail, IP67, and Stackable Rackmount


IE3500


IE3400


IE3300


IE3200


IE3100


IE3100H


IE3500H


IE3400H


IE9300

Industrial Cybersecurity
Cyber Vision, Secure Equipment Access

Industrial Wi-Fi and Ultra-reliable Wireless Backhaul
For outdoor conditions


IW9165E


IW9165D


IW9167i


IW9167E


IW9167E-HZ


IW9167E-STA

Industrial Routers
Modular 4G/5G – for connecting remote and mobile assets


IR1100


IR1800


IR8300


IR8100

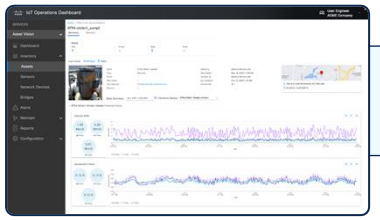
Data Control and Exchange
Edge Intelligence, IOx

Embedded Networking
Embedded routers and switches for industrial Makers

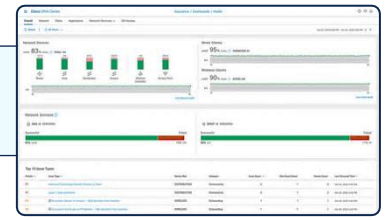

ESR6300


ESS3300


ESS9300



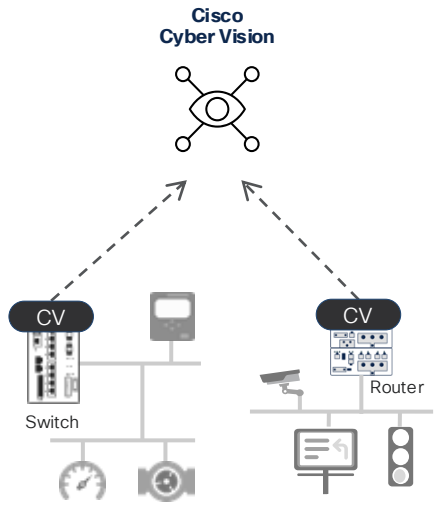
Management and Automation
Cisco Catalyst Center, Cisco Catalyst WAN Manager, Field Network Director, IW Service



Zabezpečenie Siete, 4 Základné Kroky

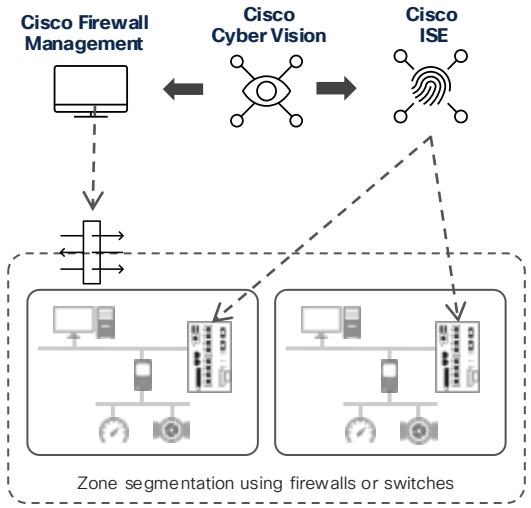
1

Asset Visibility and OT Security Posture



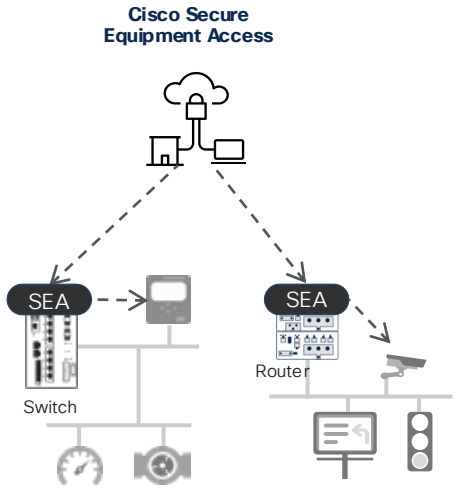
2

Zero Trust Segmentation



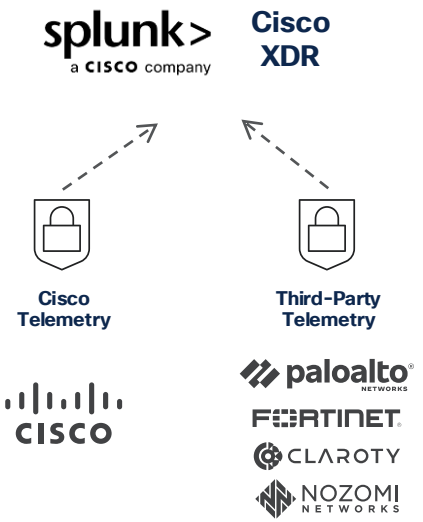
3

Zero Trust Network Access (ZTNA) for OT



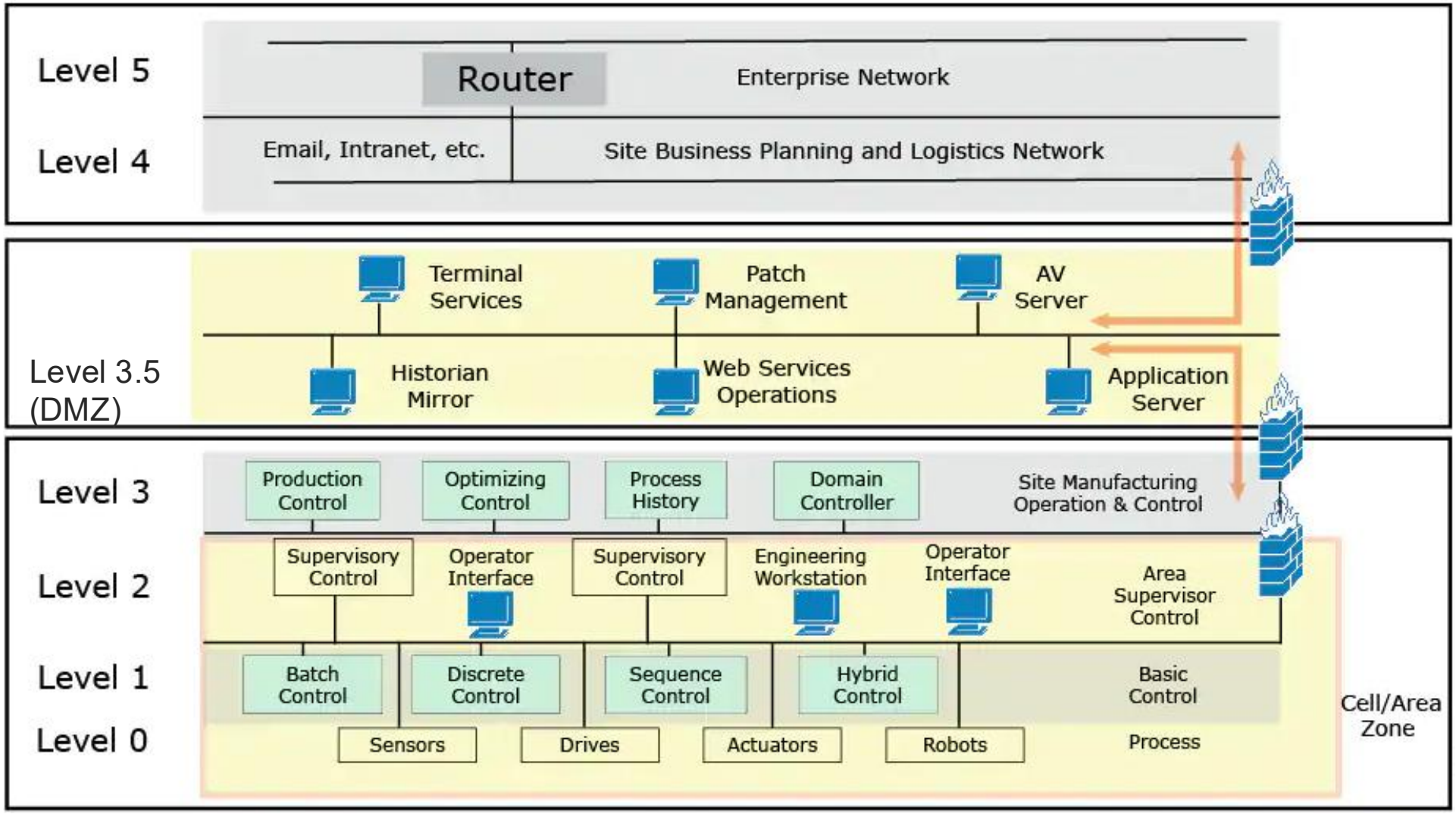
4

Cross-Domain Detection, Investigation & Response



Talos Threat Intelligence + Talos Incident Response

ISA-95 / CIM (Purdue) Model



Extract from CISCO “Oil and Gas Pipeline Security Reference Document”. CIM / ISA model differ in the scope of levels 0-1;

Čo treba zabezpečiť?

Identify OT assets and their communications

Spot vulnerabilities to patch or protect

Segment networks with access policies

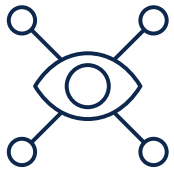
Detect bypass or leaks in the IDMZ

Drive compliance and governance

Visibility helps drive IT/OT collaboration to secure industrial operations

Cisco Cyber Vision

Visibility & Security Platform for the Industrial IoT



Visibility
OT asset inventory
Communication patterns

Security Posture
Device vulnerabilities
Risk scoring

Zone Segmentation
Automate segmentation below
the IDMZ to protect operations

Context and insights that are foundational to building reliable and secure OT networks

Cisco Cyber Vision

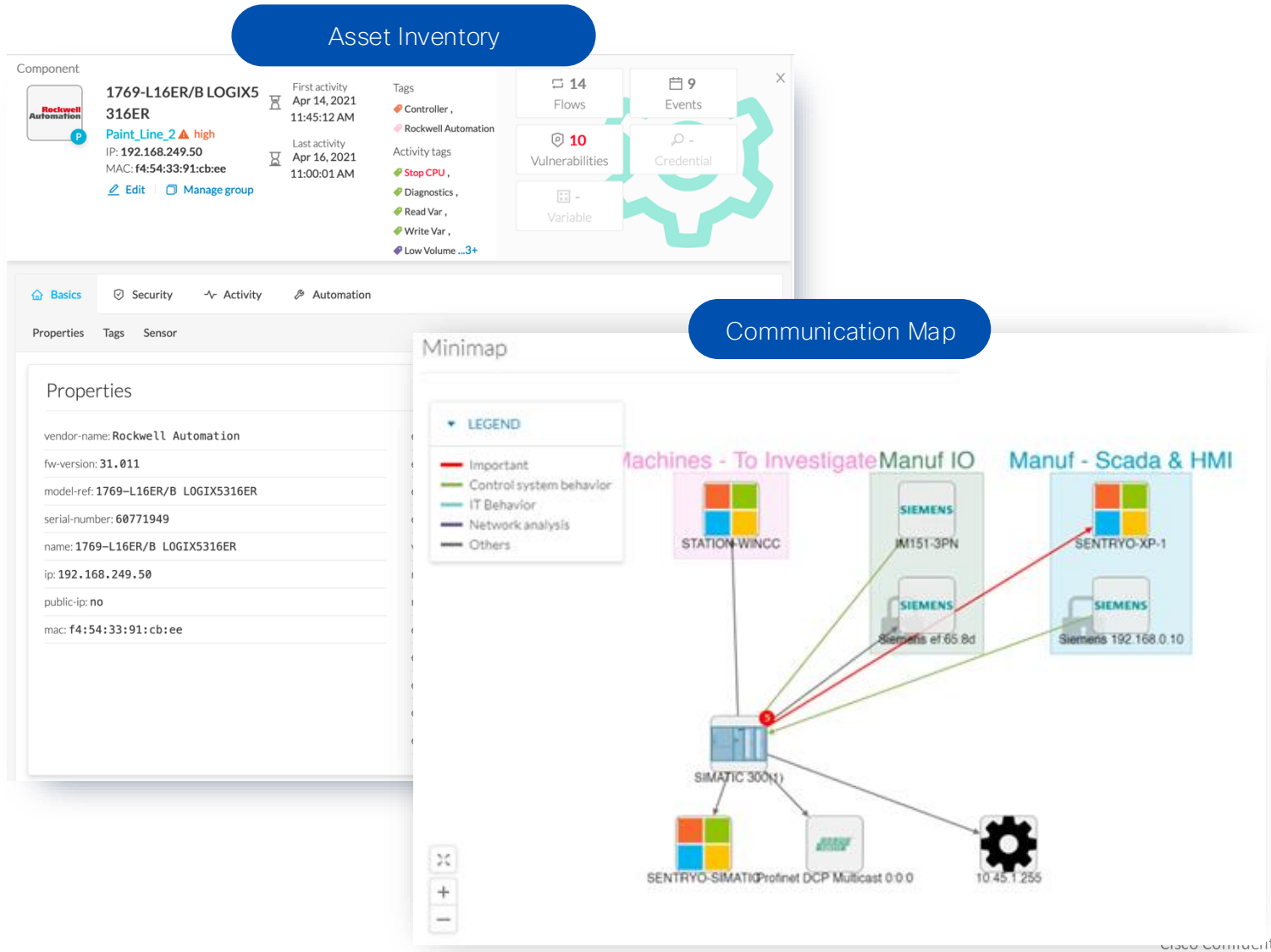
Visibility into connected industrial assets

Asset Inventory

Automated inventory of all assets in your environment with detailed and up to date profile information

Communication Patterns

Dynamic map of all communication activities with detailed application flow level information



Cisco Cyber Vision

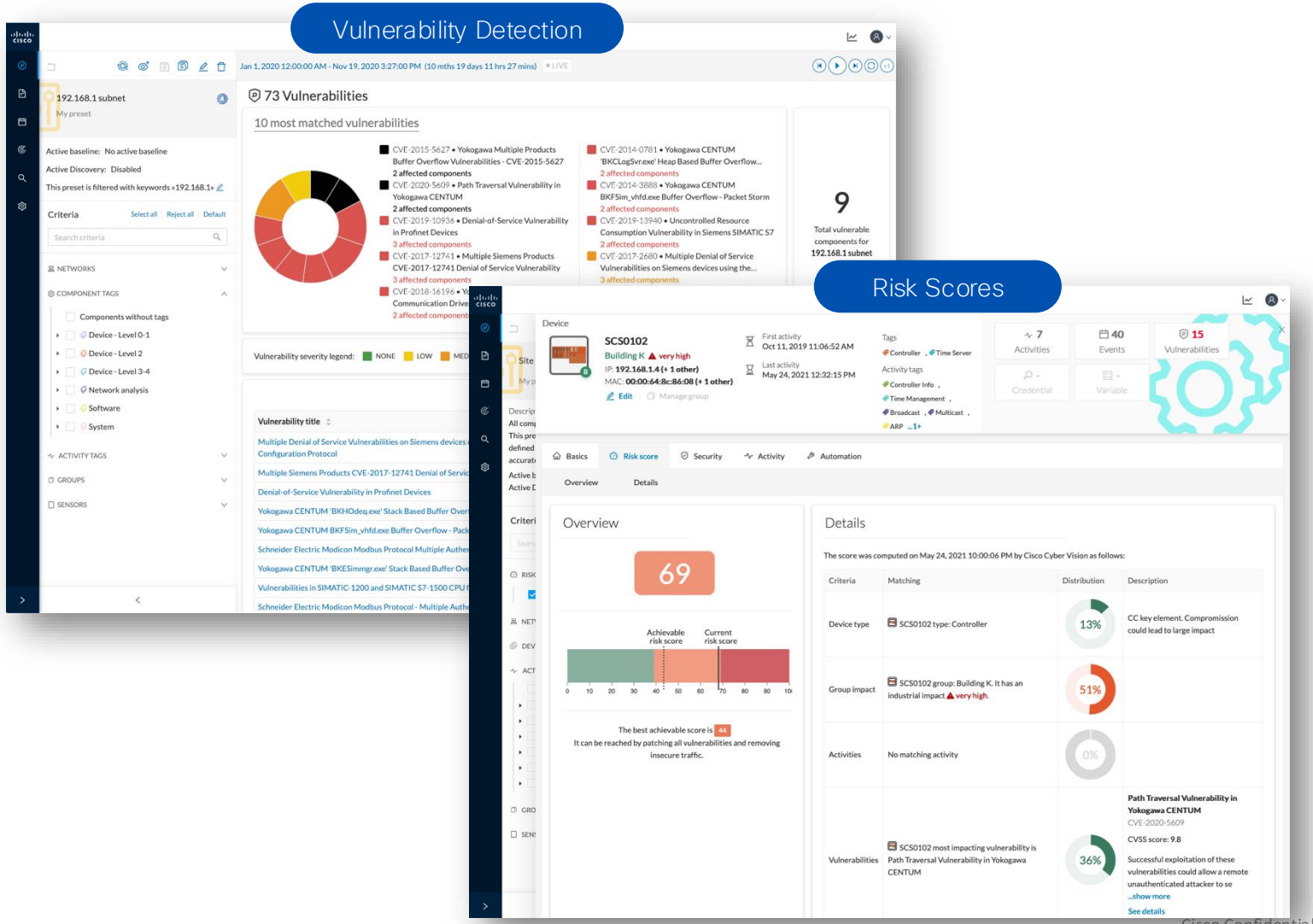
Visibility into the OT security posture

Vulnerability Detection

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

Risk Scoring

Risk scoring for assets, production cells and sites, to help prioritize action and improve governance



Visibility into threats with Snort IDS and Talos

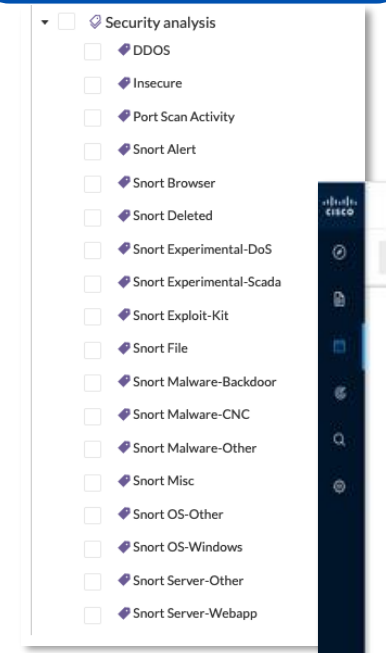
Malware Intrusions

Snort IDS with Talos threat intelligence helps identify malware and intrusions into the OT network

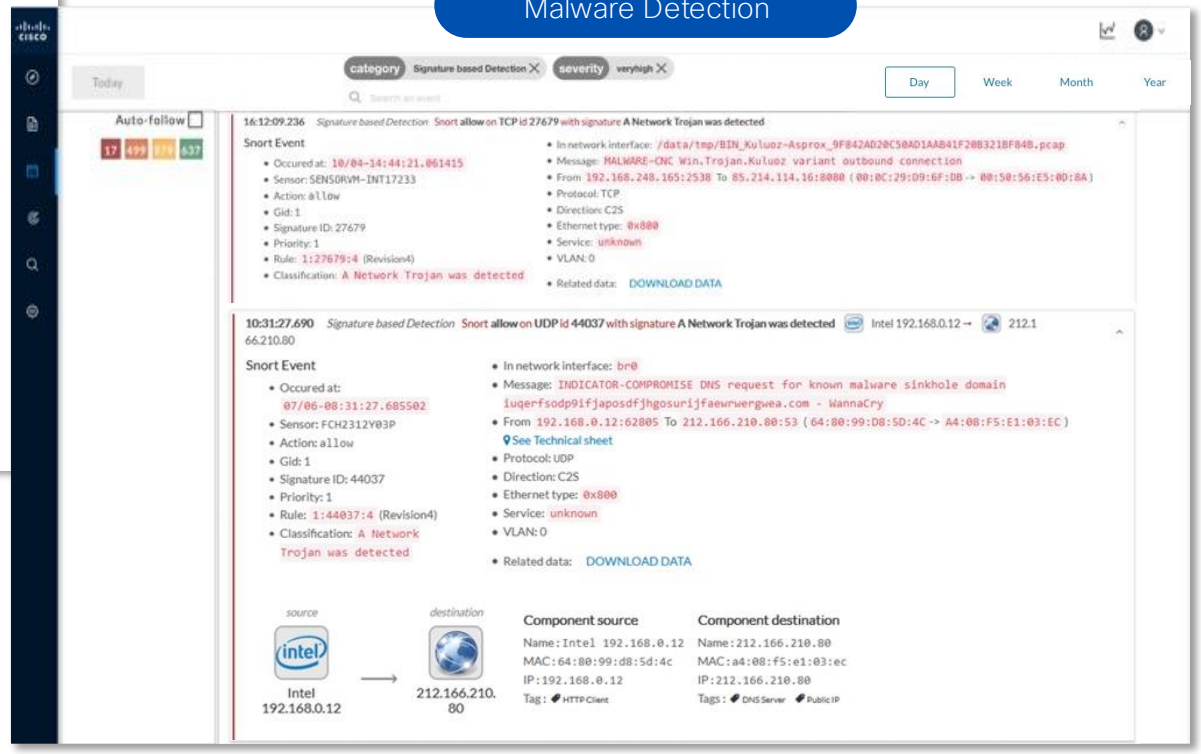
Malicious Traffic

Snort tags automatically associated with network activities to help identify malicious traffic

Malicious Activities



Malware Detection



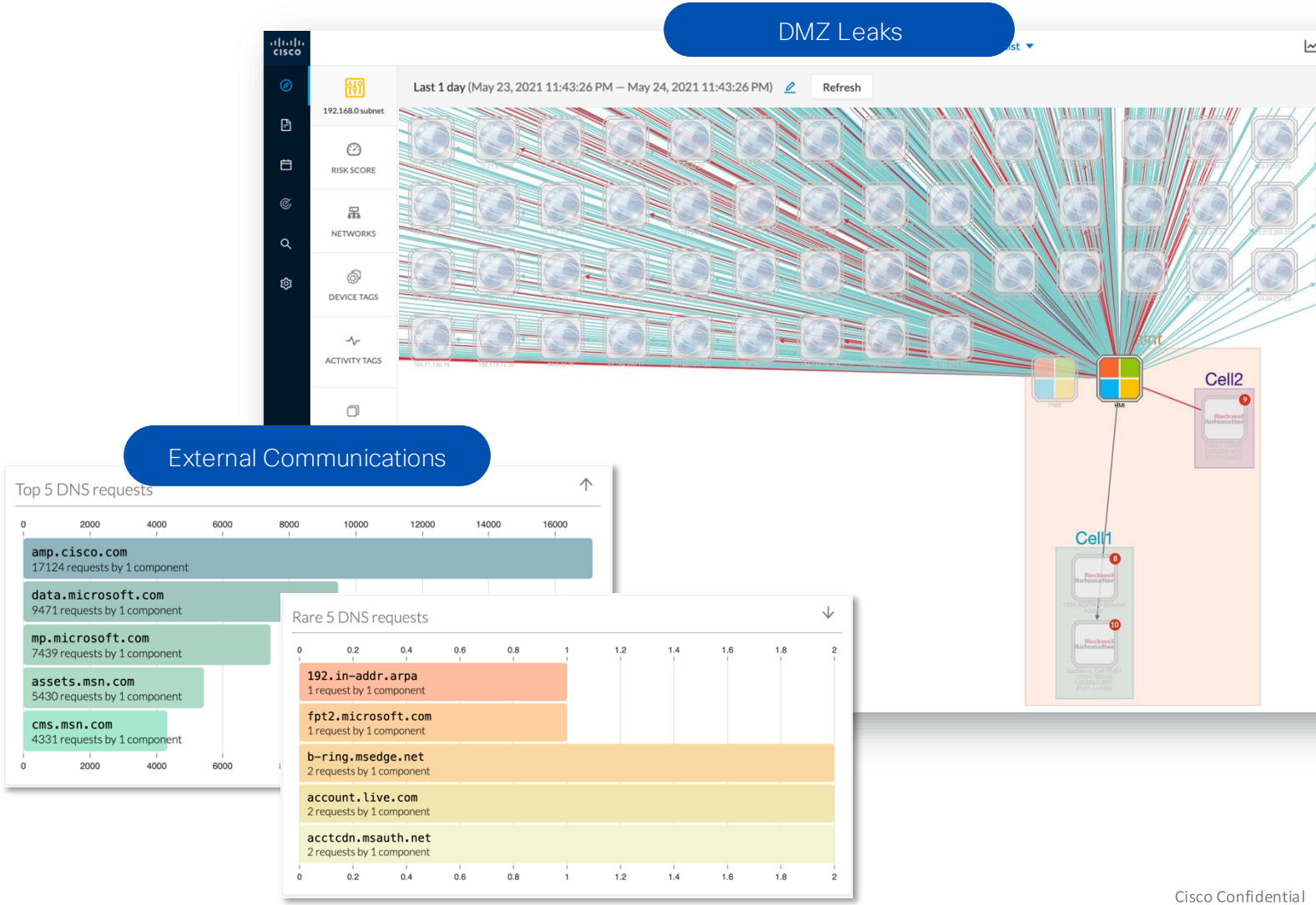
Visibility into external communications

Identify DMZ leaks

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

External communications

Identify assets trying to access external servers to spot malware infections, misconfigurations, and unnecessary traffic



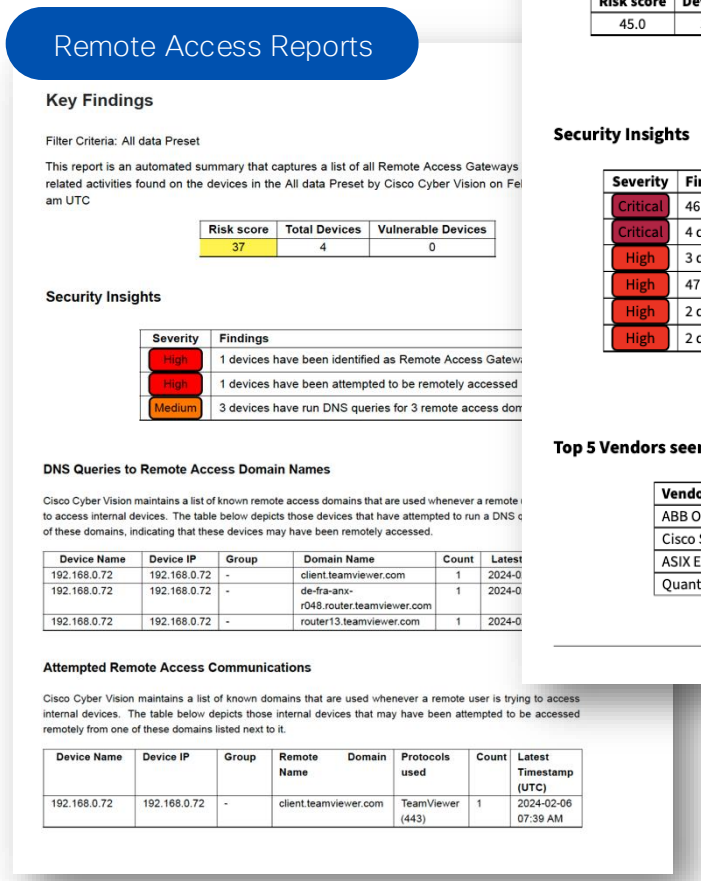
Visibility Reports to help manage risks

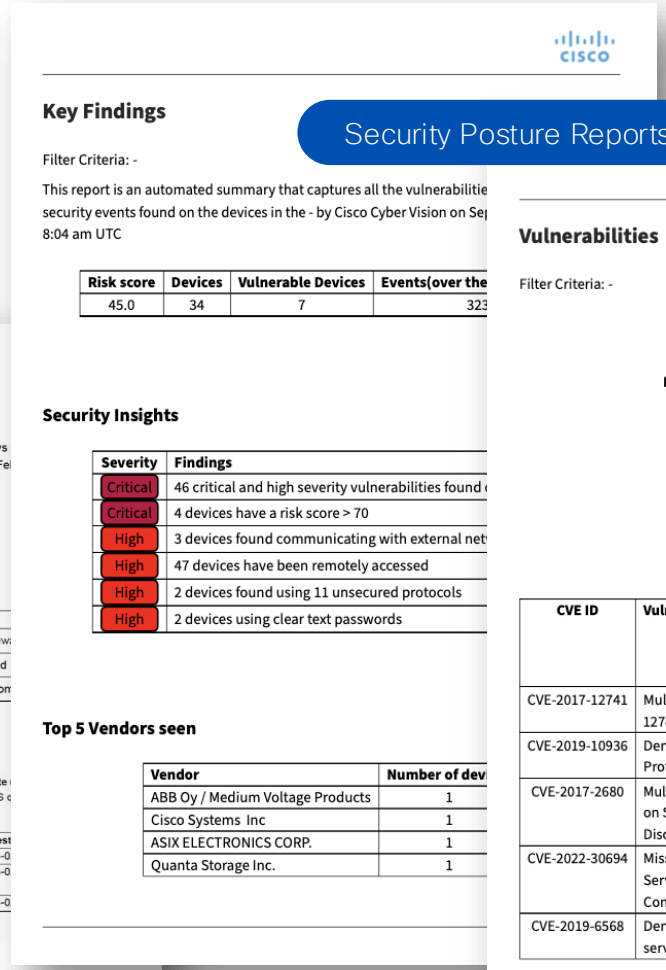
Customizable Reports

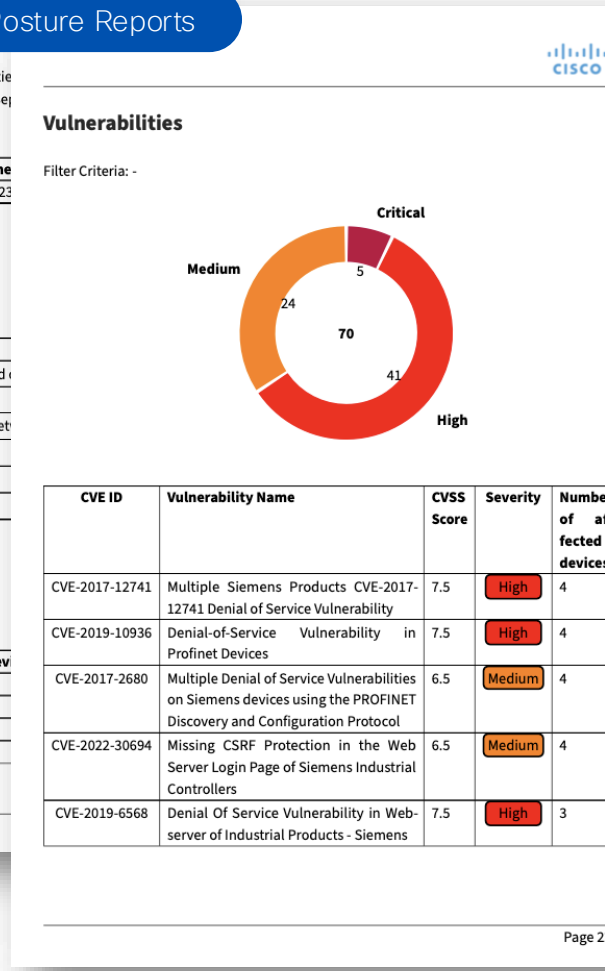
Track risk management improvements and show progress to management with historical reports

Remote Access Reports

Document remote access gateways to engage with operation teams and remove backdoors into the OT network







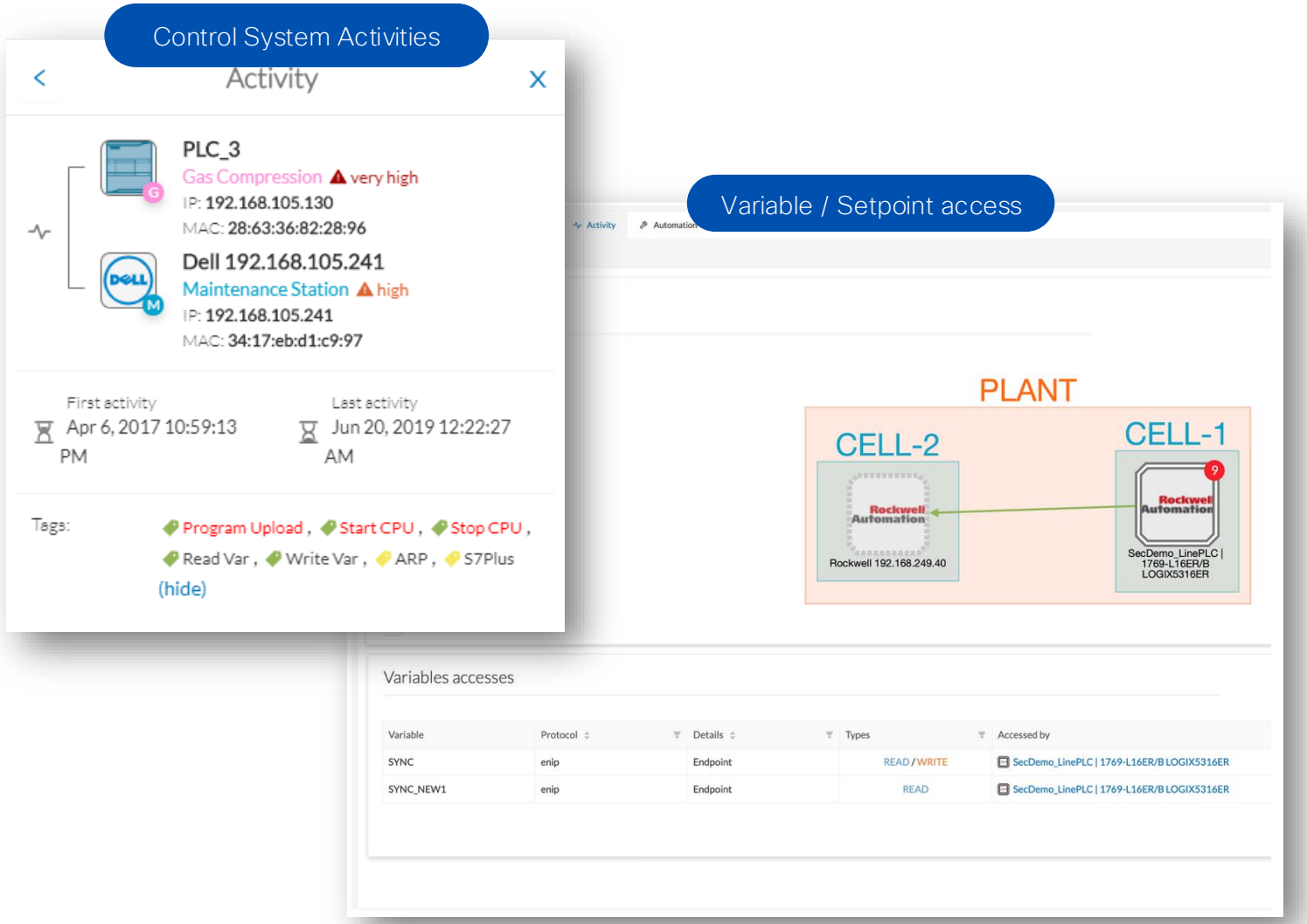
Visibility into operational issues

Control System Activities

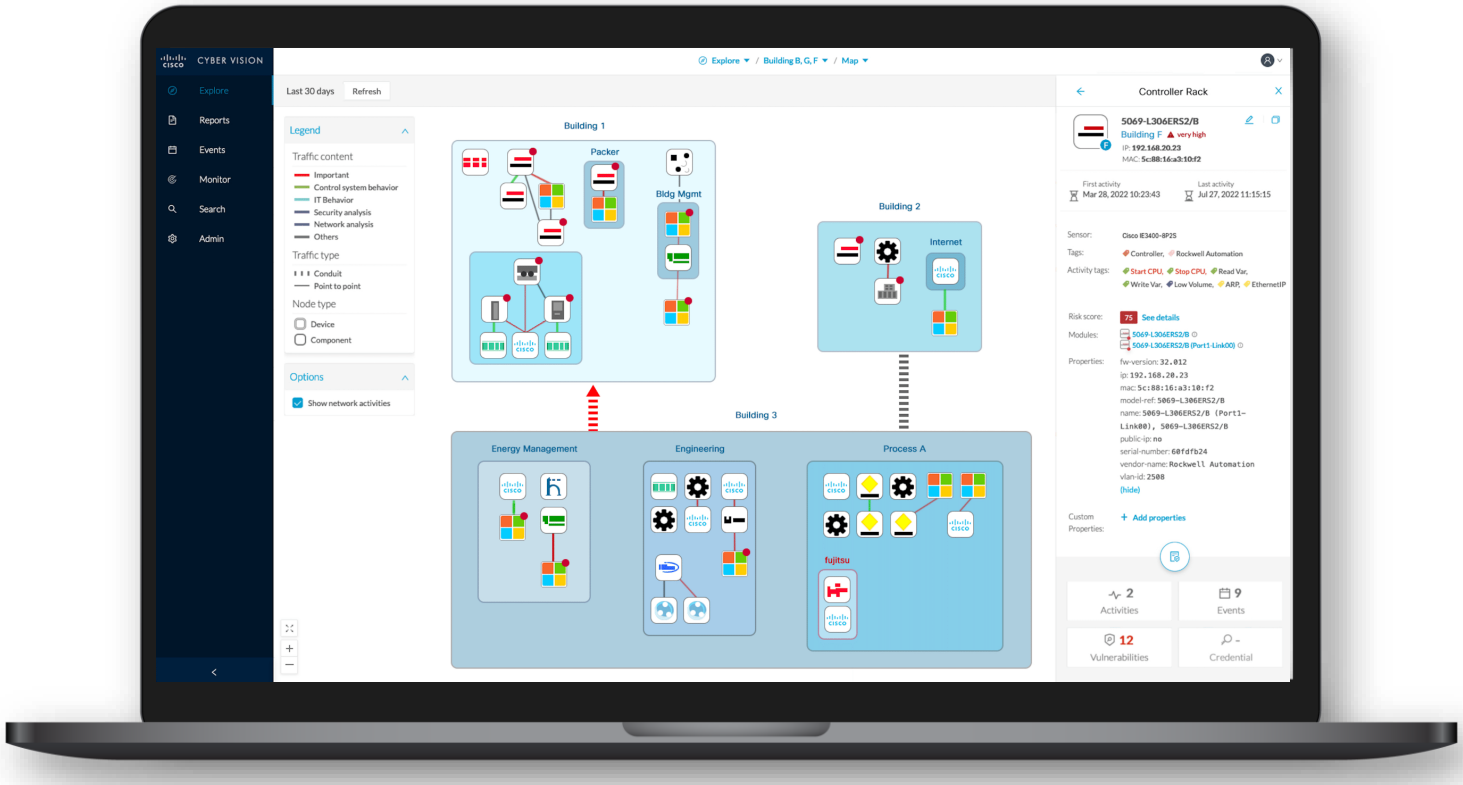
Track process modifications
Identify configuration changes
Record control system events

Variable Access

See which variables, objects, setpoints are being accessed or modified to help OT troubleshoot issues



Leveraging visibility to drive segmentation



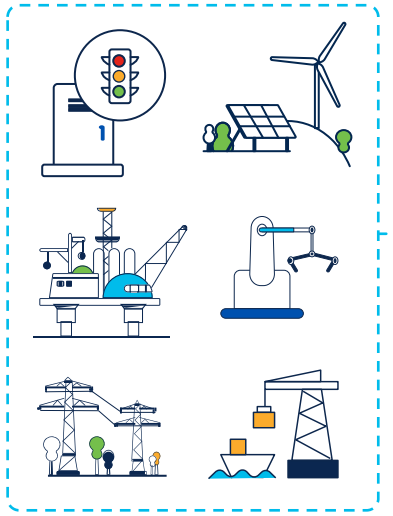
ISA/IEC-62443 virtual segmentation

- Group OT assets into zones
- Visualize conduits
- Identify traffic violations
- Share context with other platforms to enforce segmentation

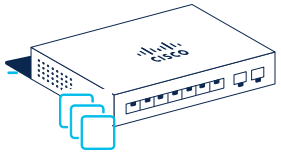
Cisco Cyber Vision: Unique 2-Tier Architecture

OT visibility that can be deployed at scale

OT Assets



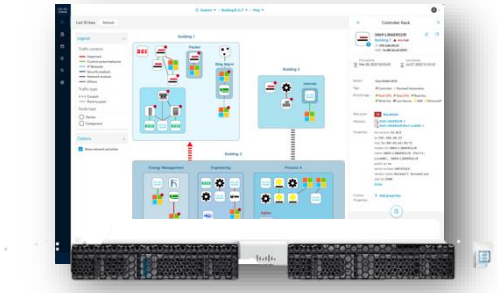
Cisco industrial switches or routers



Lightweight Metadata

Cyber Vision Sensor

- ✓ Software embedded into network equipment
- ✓ Passive discovery via DPI
- ✓ Safe active queries of assets
- ✓ Decodes application flows



Cyber Vision Center

- ✓ Centralize analytics and data storage
- ✓ Detailed OT asset inventory and communications maps
- ✓ Security posture and detection
- ✓ Reporting
- ✓ Centralized Authentication (SAML)

SOC Integrations

SIEM, XDR, NAC, Firewall, CMDB, etc.

- ✓ OT asset profiles in IT security tools
- ✓ OT context and events in SOC
- ✓ Native integrations and specific apps
- ✓ Comprehensive APIs for custom integrations

OT visibility sensors embedded into network equipment sees more and is easier to scale

Cisco Cyber Vision portfolio

Center

Hardware Appliance
UCS based servers with Hardware RAID

CV-CNTR-M6N
- 24 core CPU
- 128 GB RAM
- 3.2TB drives

Software Appliance
Virtual Machines

VMWare ESXi OVA

HyperV VHD

Amazon Web Services

Microsoft Azure

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

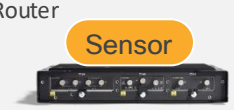
Minimum requirements
x386 server CPU, 10 cores
32GB RAM and 1TB SSD
1 or 2 network interfaces

Sensors

Catalyst IE3300, IE3400 and **IE3500** Switches

Catalyst IE3400HD IP67 Switch

Catalyst IR1101 Cellular Router



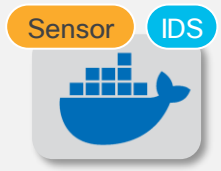
Catalyst IR1800 Cellular Router

Catalyst IR8300 Multiservice Router

Catalyst IE9300 Rugged Switches

Catalyst 9300/9400 Aggregation Switches

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



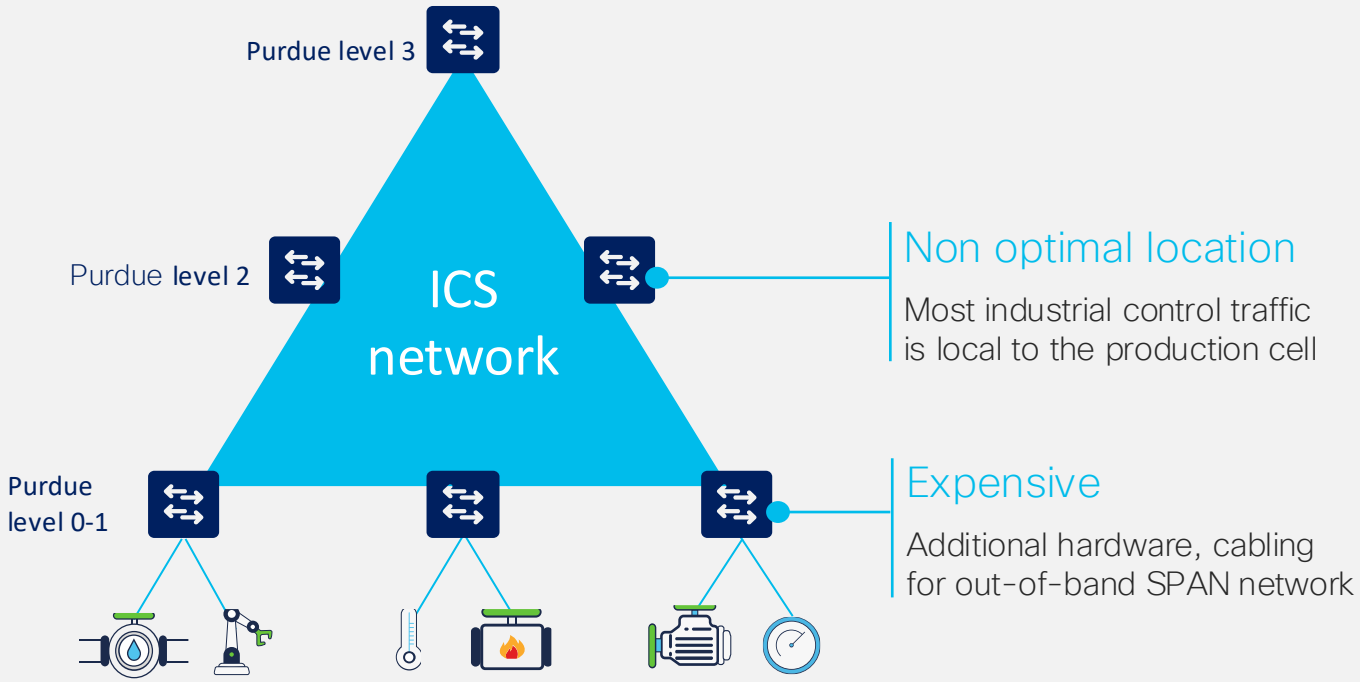
x86 or ARM64 Compute

IC3000 Industrial Compute

Docker Sensor Hardware-Sensor
DPI and active discovery via SPAN to support brownfield

Why is a network-sensor important?

Most industrial network traffic is East-West, not North-South



Non optimal location

Most industrial control traffic is local to the production cell

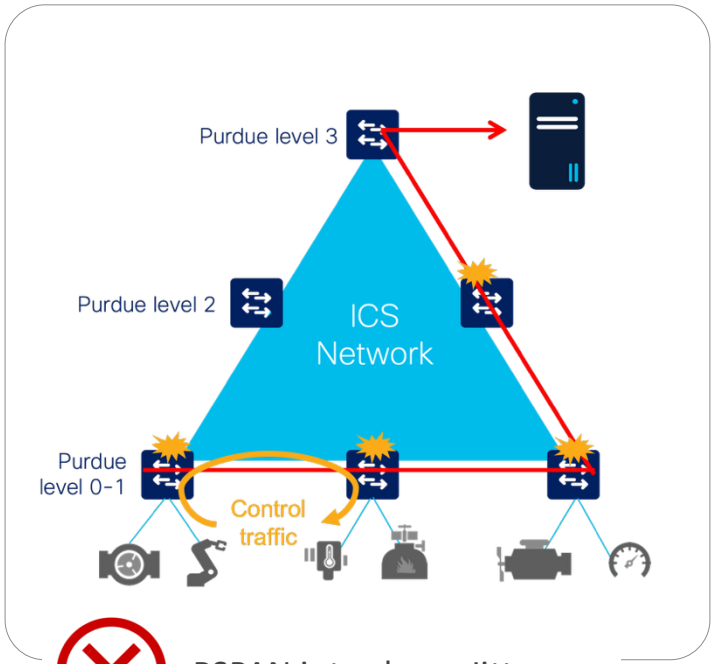
Expensive

Additional hardware, cabling for out-of-band SPAN network

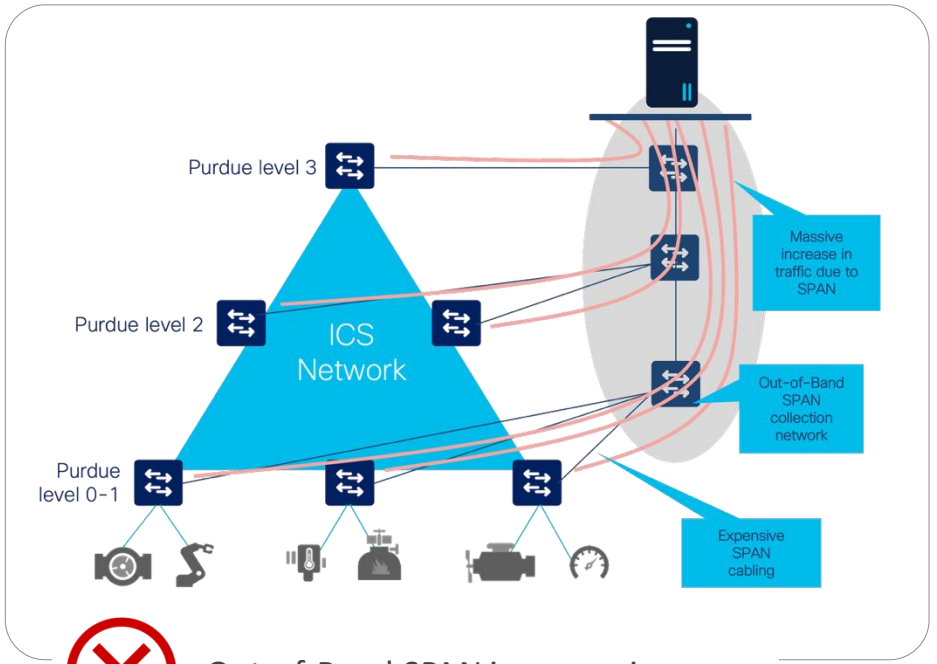
Sensors embedded in the network see everything that attaches to it

Cisco Confidential

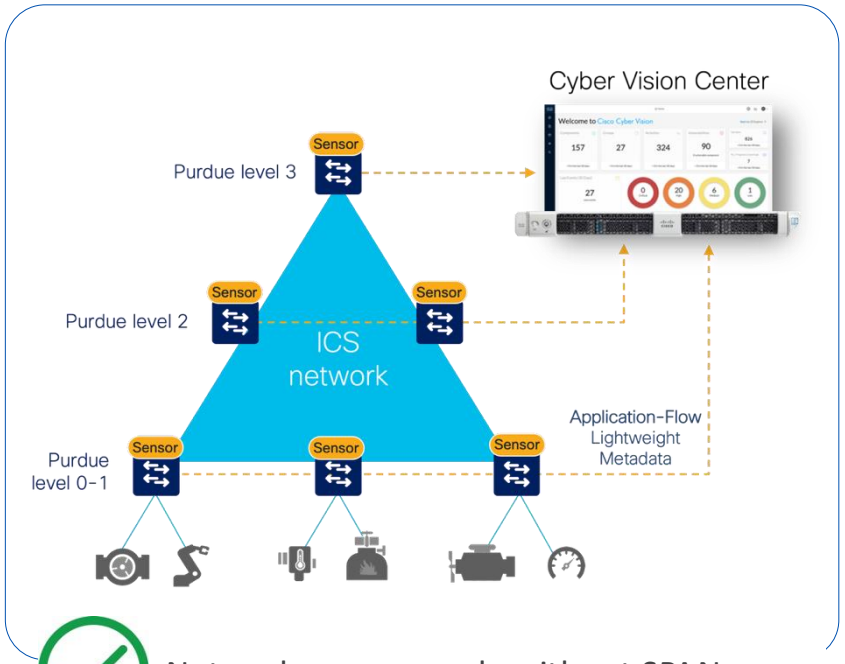
Leverage the network as a sensor to lower cost and complexity



RSPAN introduces Jitter



Out-of-Band SPAN is expensive



Network sensors scale without SPAN

OT visibility sensors embedded into network equipment sees more and is easier to scale

On-Center Sensor offers extra deployment flexibility

Central DPI and IDS capabilities

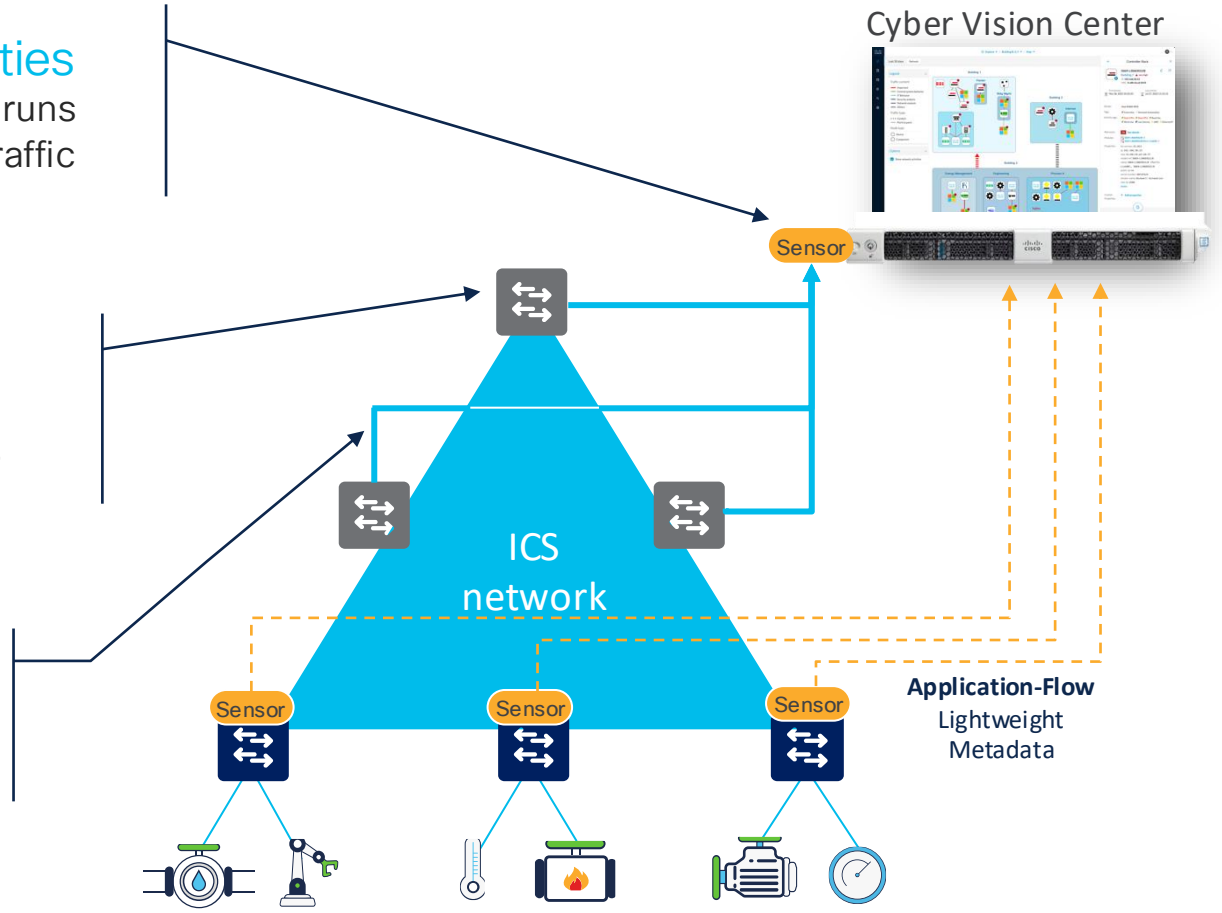
Sensor built into the Cyber Vision Center runs DPI and IDS on raw industrial network traffic

Collect traffic from the datacenter

Needs only 1-hop SPAN from the aggregation switch to the Cyber Vision Center

Leverage existing SPAN infrastructures

Makes deployment super easy if the collection network is already in place

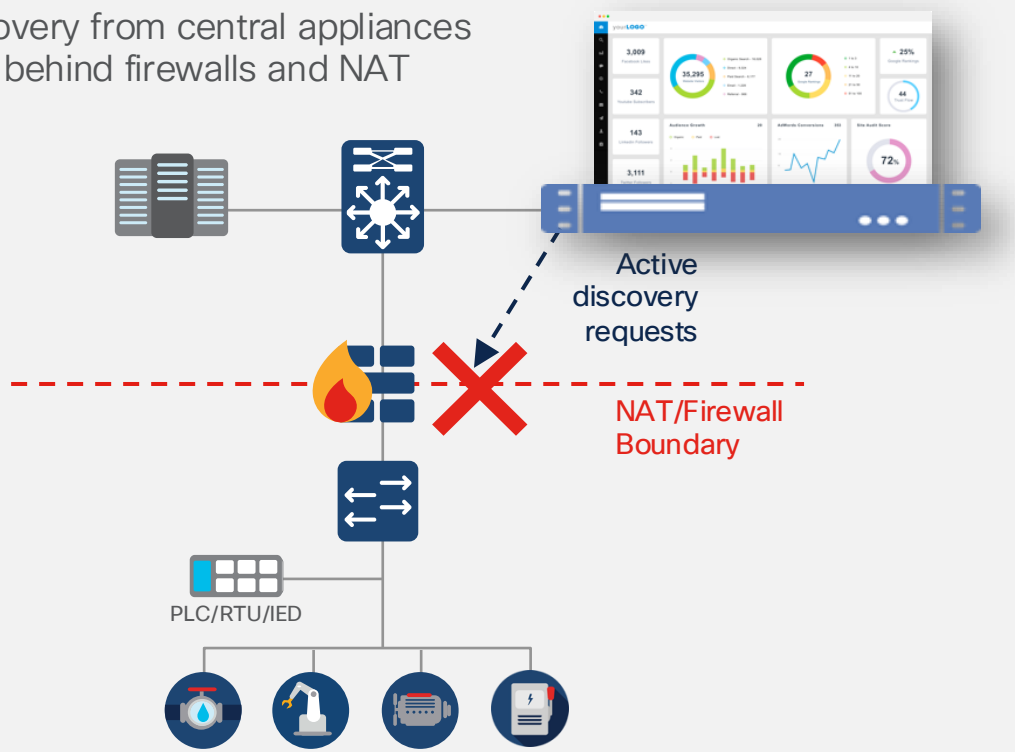


Why is a network-sensor important?

Sensors embedded in the network can see more

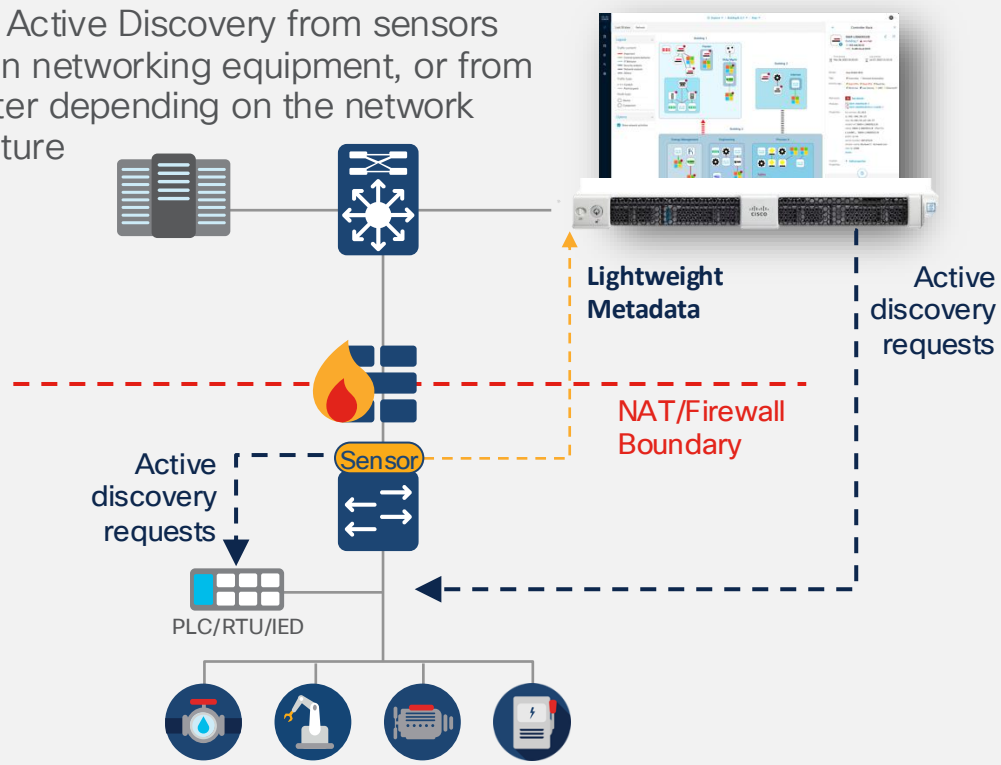
Other solutions

Active discovery from central appliances cannot see behind firewalls and NAT boundaries



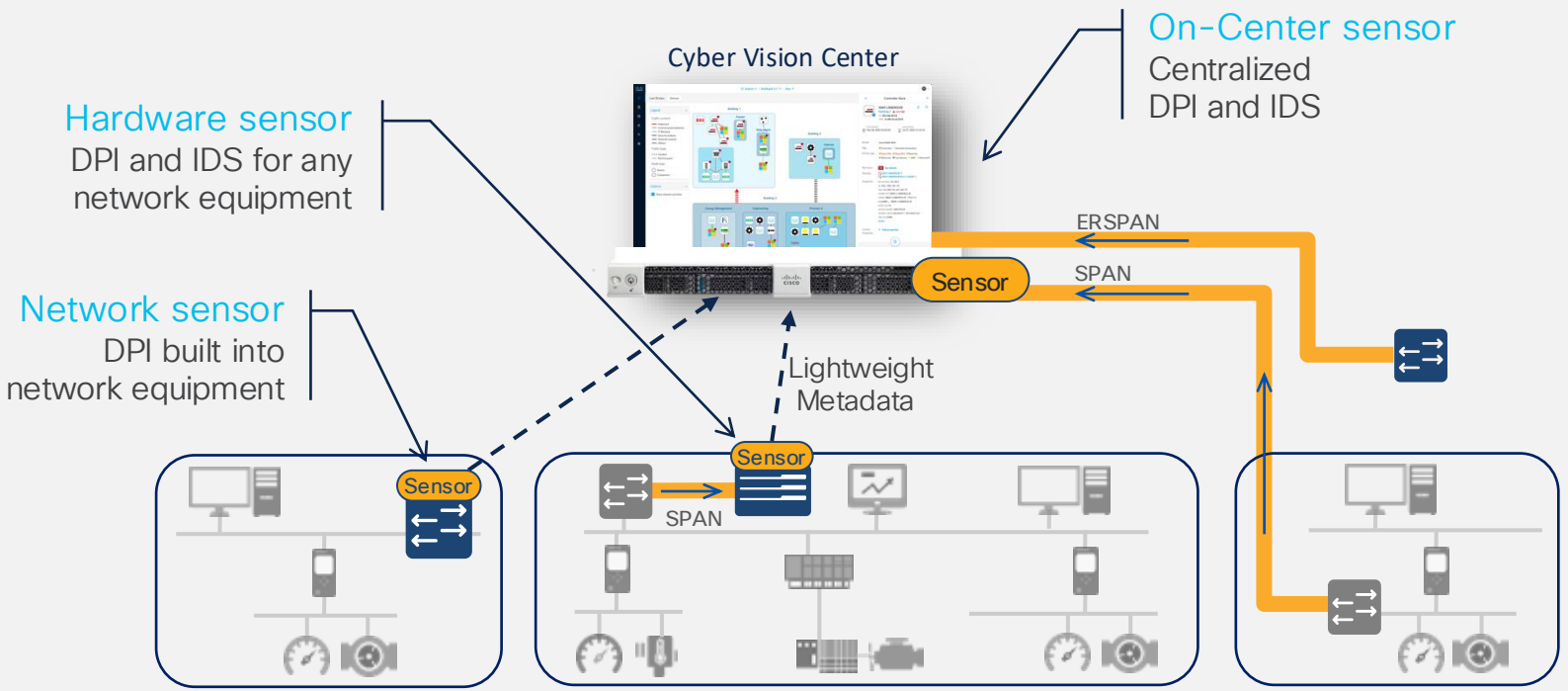
Cisco Cyber Vision

Flexible Active Discovery from sensors hosted in networking equipment, or from the center depending on the network architecture



Active discovery requests are not blocked by NAT and firewall boundaries

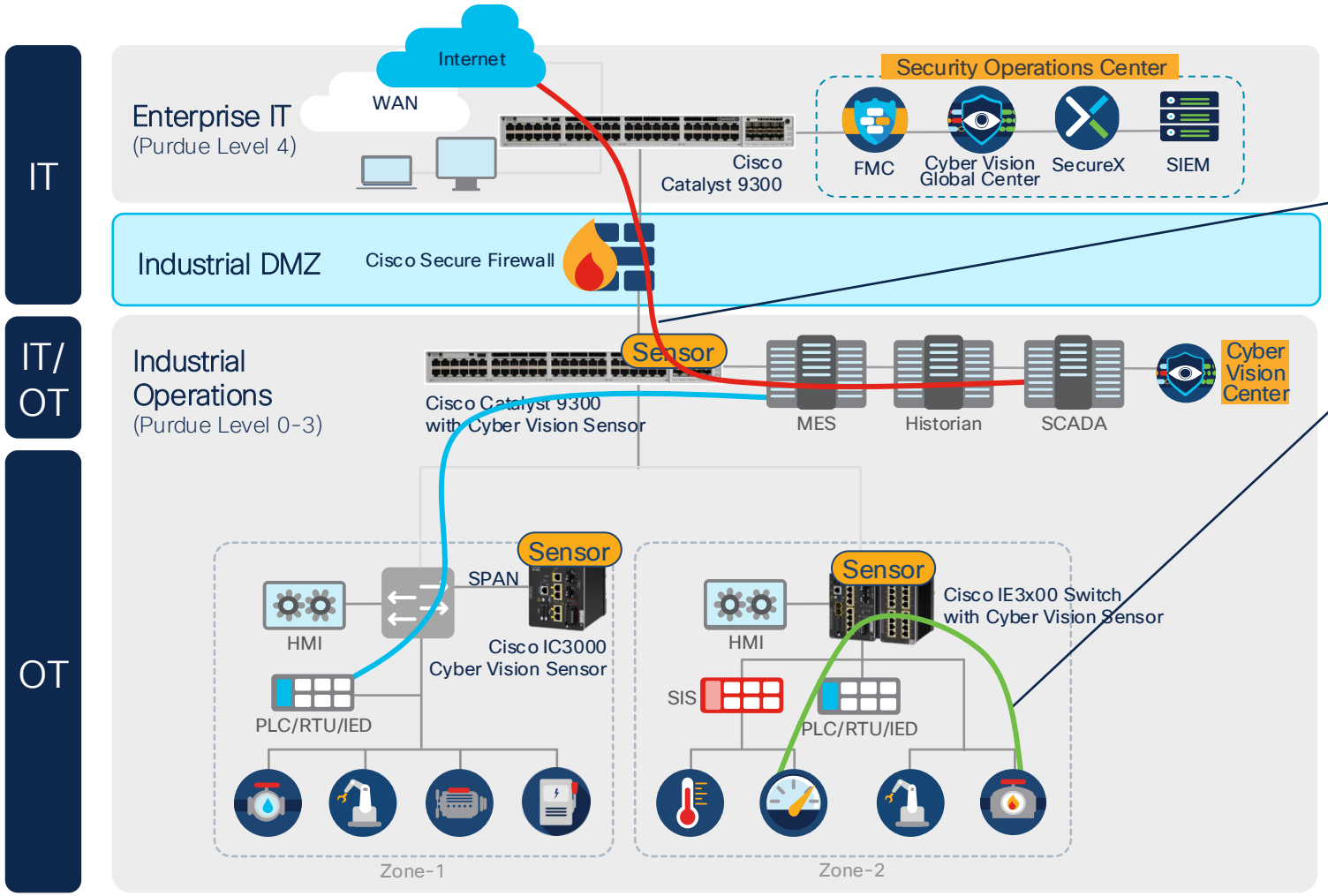
Cyber Vision offers flexible deployment options



- **Network sensors** embedded in Cisco networking for simple and highly scalable deployments
- **Hardware sensors** capturing traffic on any switch with a single hop SPAN to support brownfield deployments
- **On-Center sensor** to leverage existing SPAN infrastructures, or collect traffic within the datacenter, including ERSPAN to the center network interfaces

Cyber Vision can mix architectures to best fit your constraints

Do you need a Sensor on every switch?



Sensor at aggregation sees North-South traffic

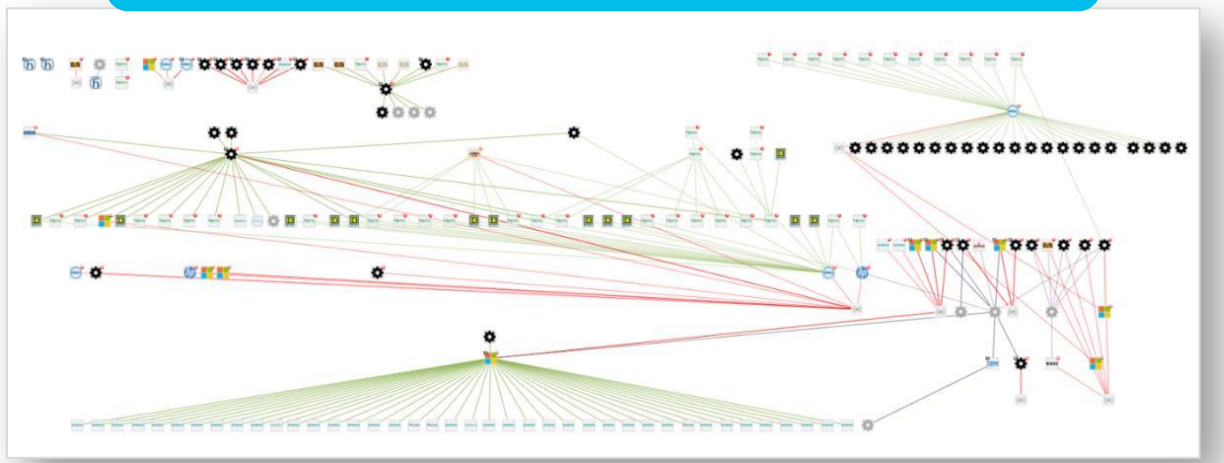
Sensor at the edge sees East-West traffic

Remember: Cyber Vision is licensed per endpoint, not per sensor!

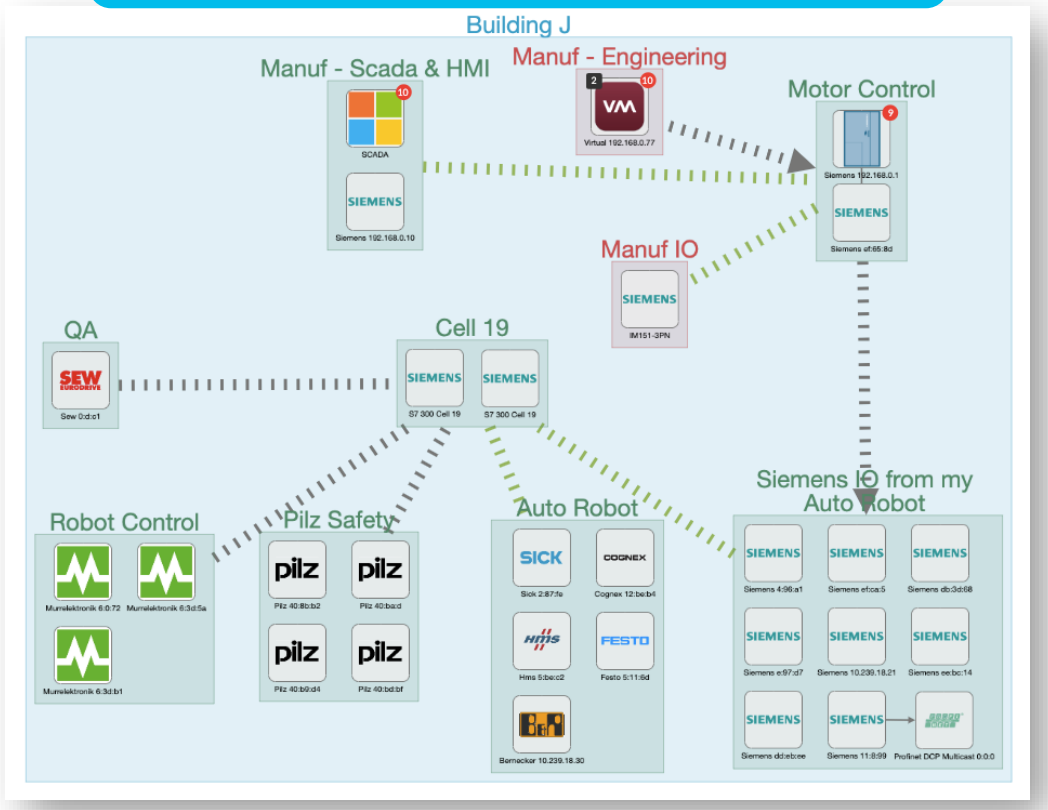
Rule of thumb: All flows must go through at least one sensor. Every networking equipment should have a sensor.

Leveraging Visibility to Drive Segmentation

Cyber Vision discovers all connected assets…



…and groups them into logical zones

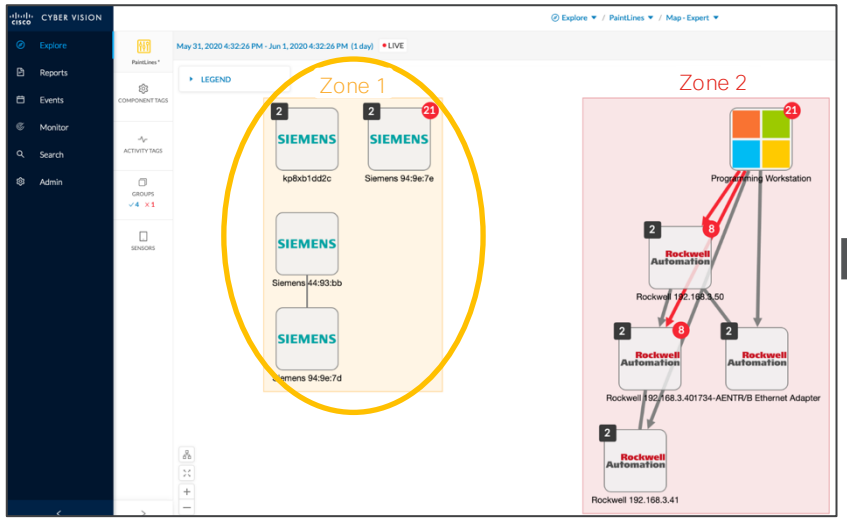


Give OT the tool they need to document ISA/IEC-62443 zones and conduits

Automated Segmentation **Informed by Visibility**

This user interface understands industrial processes.
I can group assets into zones

I now have OT context to build the right network access policies



Cisco Cyber Vision Map View

	Zone 1	Zone 2	PLC	MES
Zone 1	✓	✗	✓	✗
Zone 2	✗	✓	✓	✗
PLC	✓	✓	✓	✓
MES	✗	✗	✓	✓

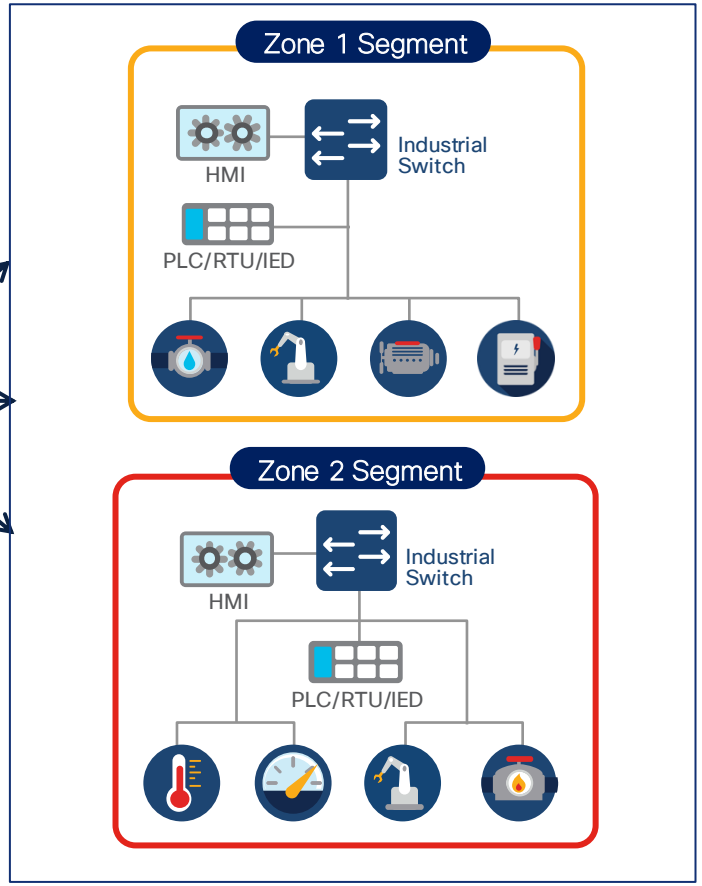
Cisco Firewall Policy Rules
or
Cisco ISE Policy Matrix

dACL

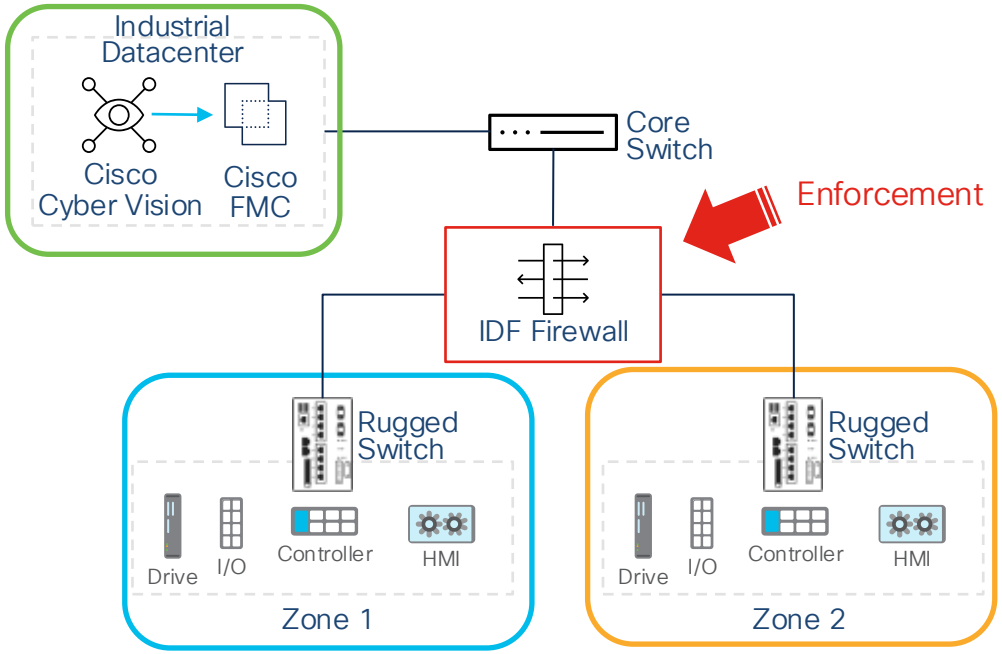
SGT

VLAN

Segmentation of industrial network



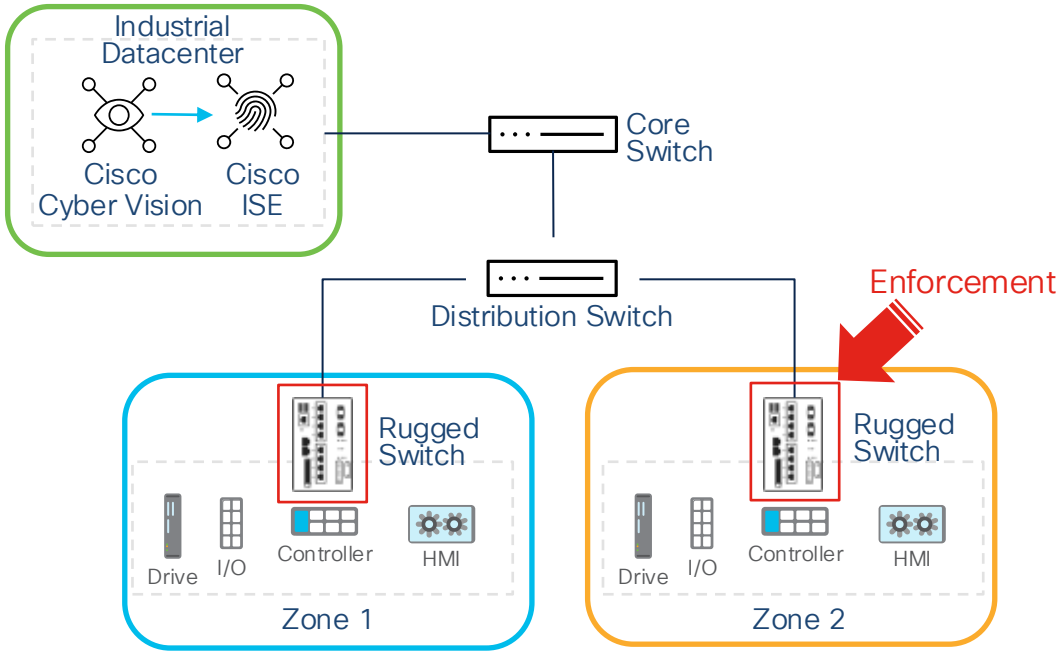
Automated Segmentation **Enforced using Firewalls**



- All VLANs in the OT network terminate at the firewall installed in the distribution network (IDF)
- Traffic that crosses VLAN boundaries is subject to firewall rules
- Take advantage of application firewall rules such as enabling read only access across zones or denying specific OT commands
- Cisco Firewall Management Center (FMC) centralizes policy definition for all firewalls

Firewall policies automatically updated when OT modifies Cyber Vision groups

Automated Segmentation **Enforced using Switches**

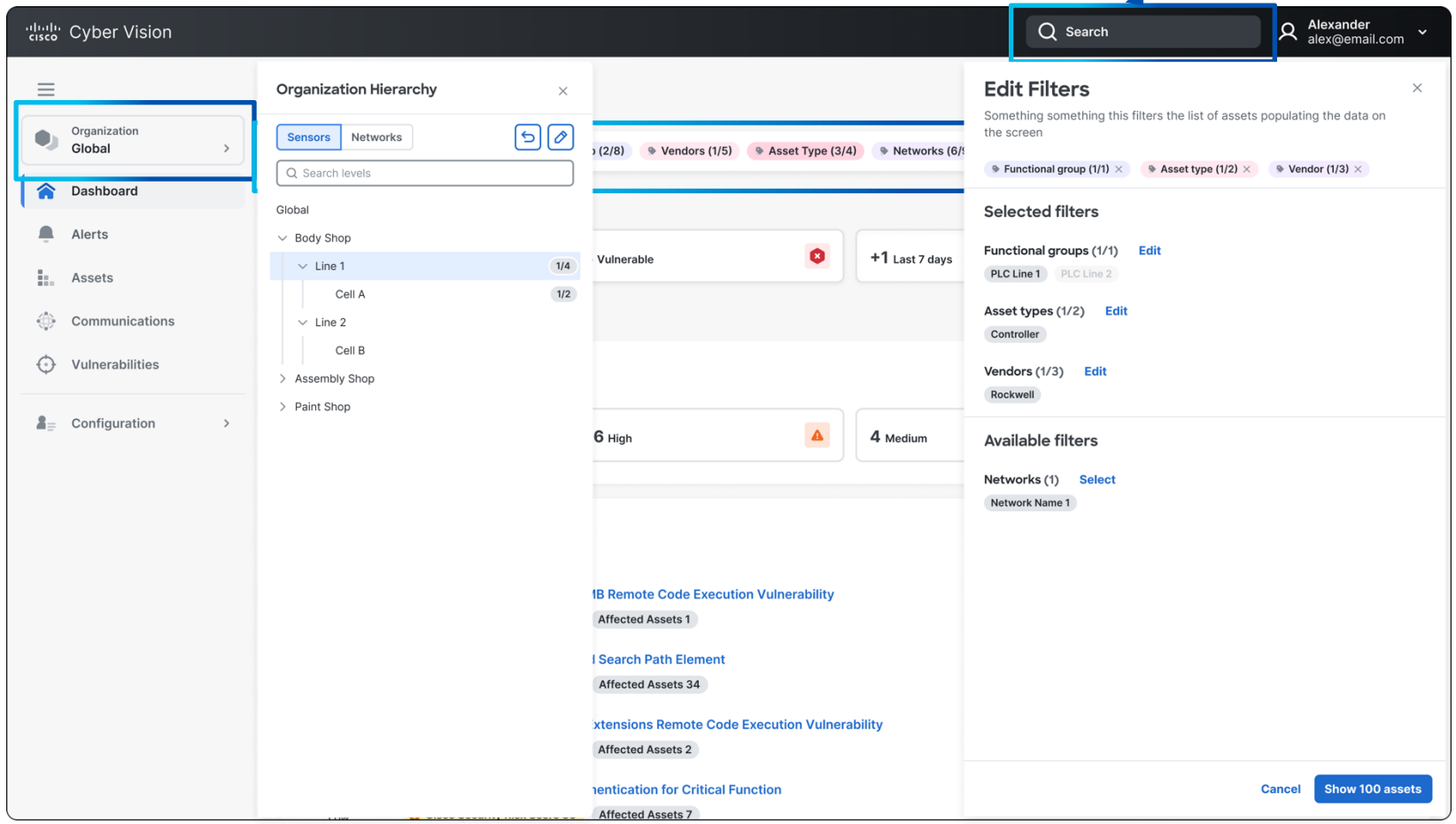


- Cisco Identity Services Engine (ISE) receives devices' profiles from Cyber Vision and associates a network access policy to each
- Policies are pushed to network switches for enforcement at the port level
- Network switches allow/deny assets to communicate based on their profile, not their IP address
- Deny by default is applied to assets not profiled

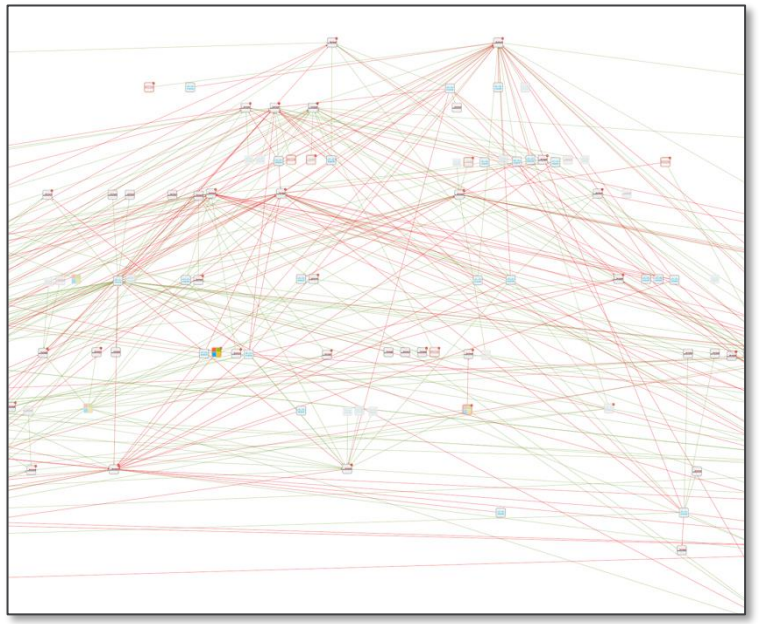
Network access policies automatically updated when OT modifies Cyber Vision groups

Simplified Navigation

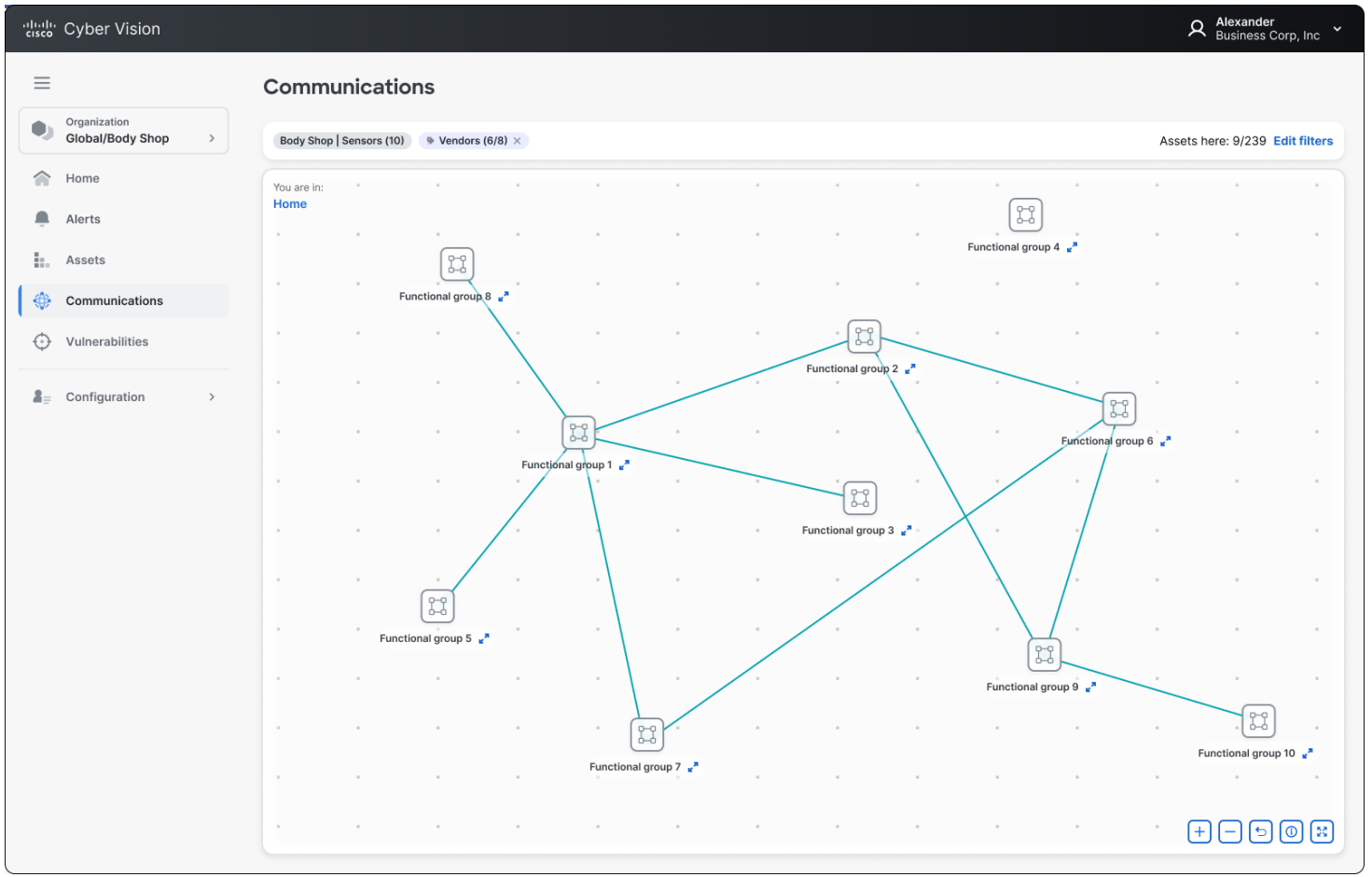
- Hierarchy-based navigation to organize your OT assets based on subnets or sensor placement
- Filters (Active View) to focus on specific data
- Rapidly find your asset with Quick search



AI-driven asset clustering

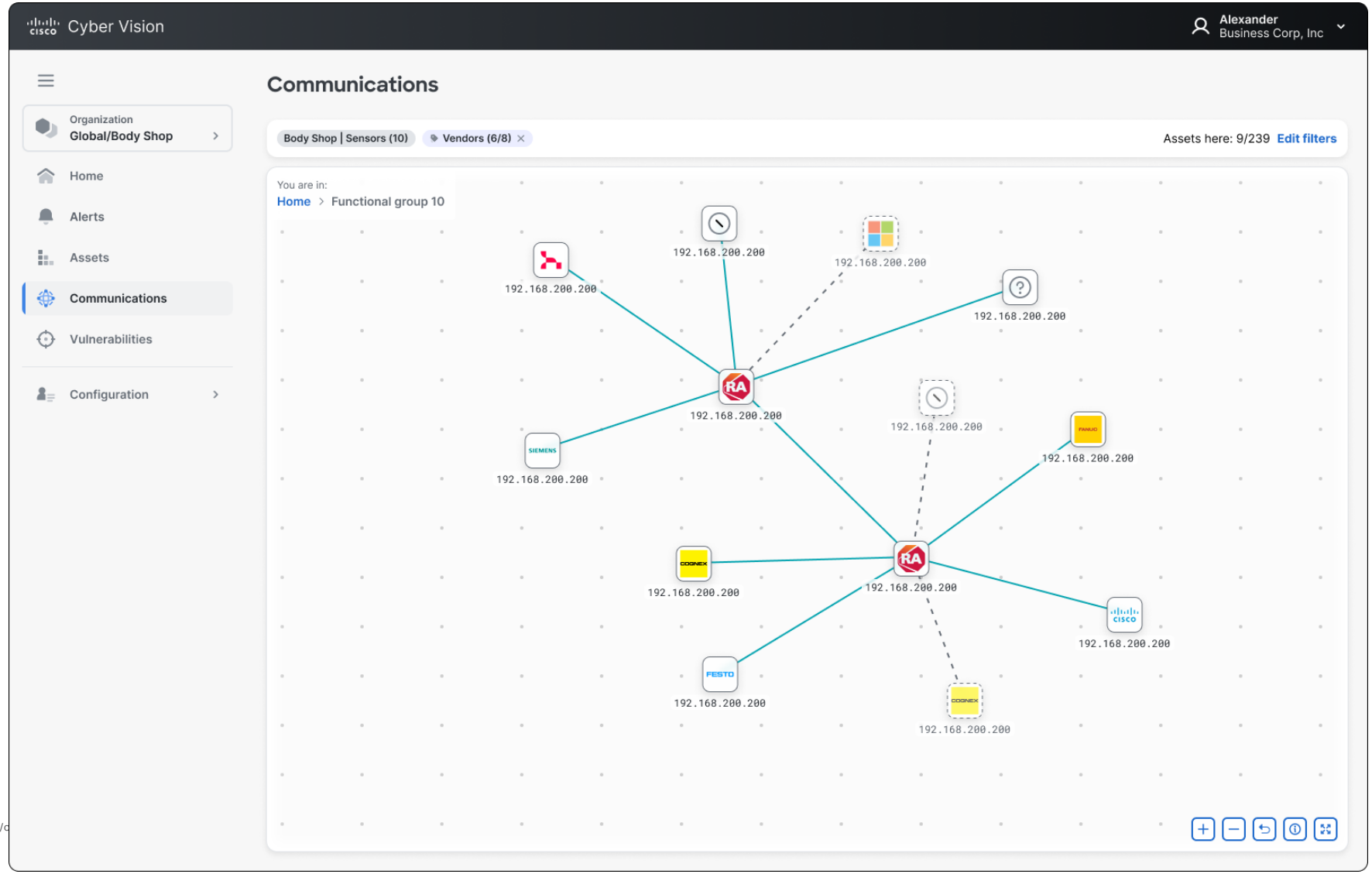


OT asset inventory projects highlight flat, unsegmented networks

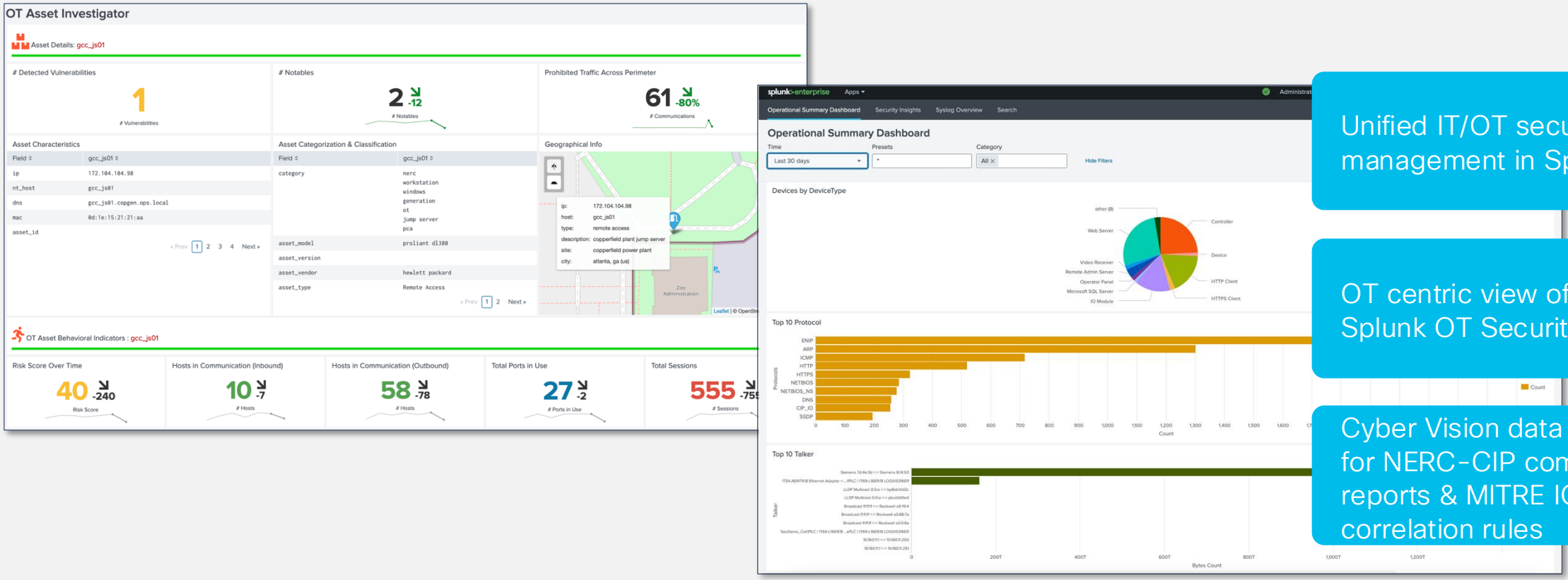


Cisco Cyber Vision ML-driven auto-grouping automatically creates security zones to drive network segmentation using Firewalls or NAC

Internal group communication



Splunk Integration



Unified IT/OT security events management in Splunk SIEM

OT centric view of assets in Splunk OT Security Add-on

Cyber Vision data in Splunk for NERC-CIP compliance reports & MITRE ICS correlation rules

Syslog and REST API integration with Splunk SIEM and OT Security Add-on