SOITRON industry

CONTROL SYSTEM

# Sensory Architecture for Safe and Reliable Operation

## Reduced monitoring data traffic, ver.1.1, User Case Studies


Michal Remper, michal.remper@soitron.com

Roland Rais, roland.rais@soitron.com

Simon Remper, simon.remper@gmail.com

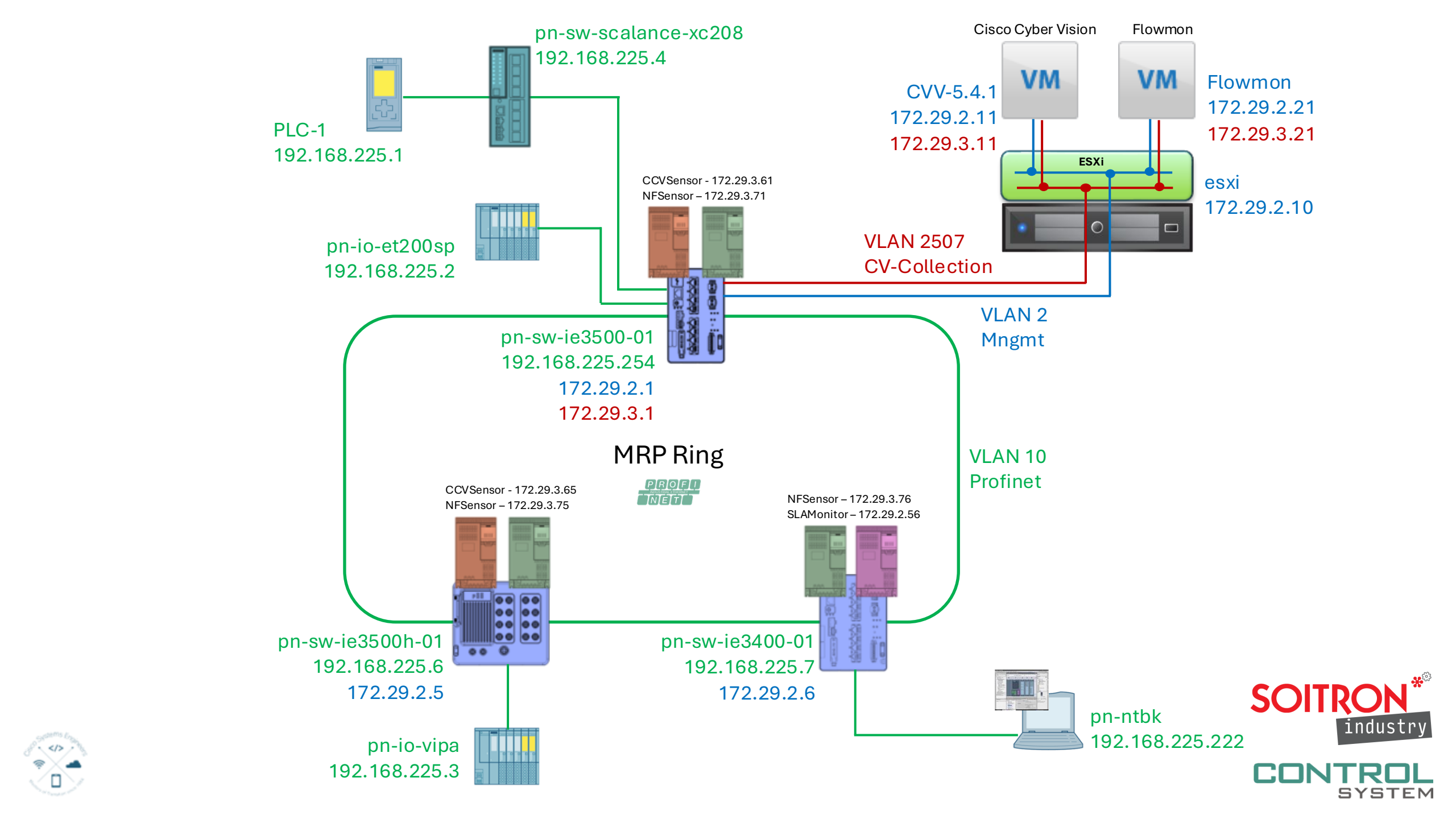

May 2026

EtherNet/IP ODVA

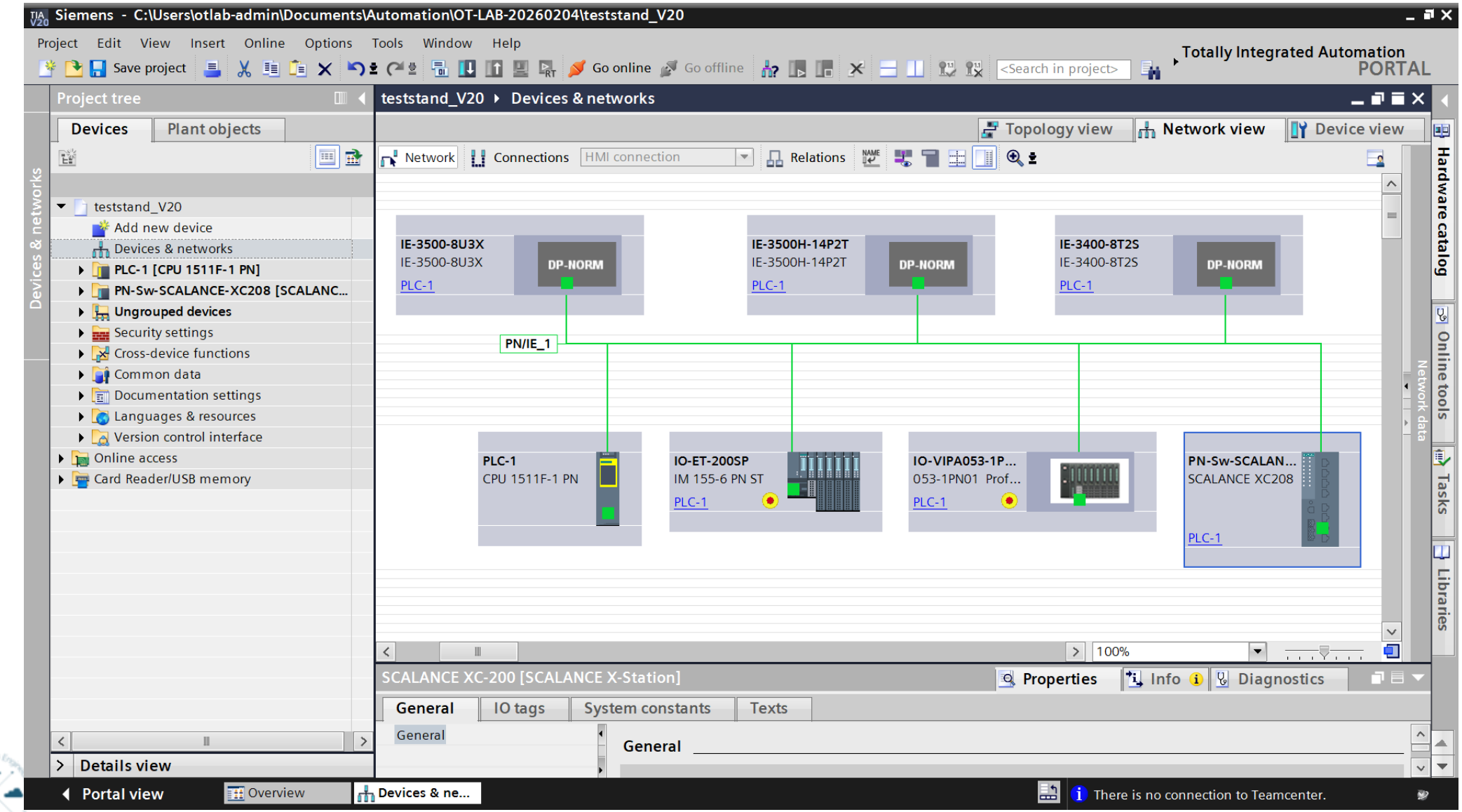
PROFINET INDUSTRIAL ETHERNET

# Today Demo Topology

New Project challenge


pn-sw-scalance-xc208
192.168.225.4
PLC-1
192.168.225.1
Cisco Cyber Vision
Flowmon
VM
VM
CVV-5.4.1
172.29.2.11
172.29.3.11
Flowmon
172.29.2.21
172.29.3.21
ESXi
esxi
172.29.2.10
CCVSensor - 172.29.3.61
NFSensor – 172.29.3.71
pn-io-et200sp
192.168.225.2
VLAN 2507
CV-Collection
VLAN 2
Mngmt
pn-sw-ie3500-01
192.168.225.254
172.29.2.1
172.29.3.1
MRP Ring
VLAN 10
Profinet
CCVSensor - 172.29.3.65
NFSensor – 172.29.3.75
NFSensor – 172.29.3.76
SLAMonitor – 172.29.2.56
pn-sw-ie3500h-01
192.168.225.6
172.29.2.5
pn-sw-ie3400-01
192.168.225.7
172.29.2.6
pn-io-vipa
192.168.225.3
pn-ntbk
192.168.225.222

# All Demo Devices in TIA Portal, Cisco included ...

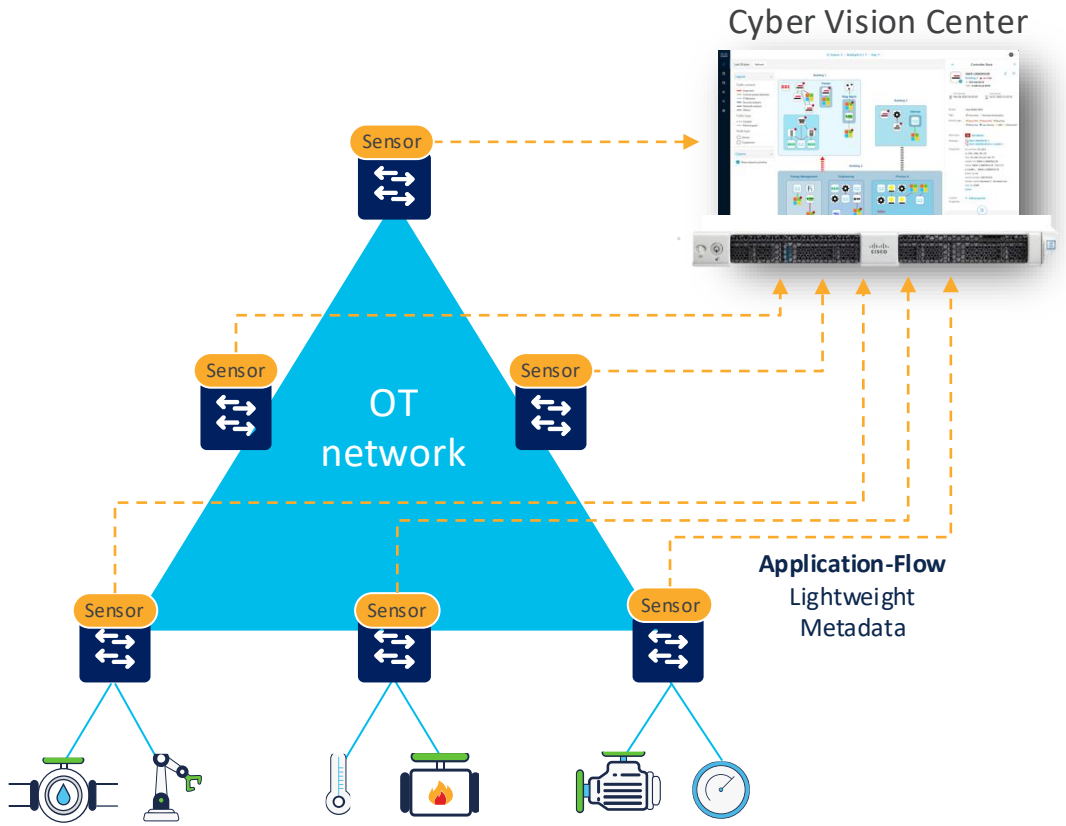


# Let’s start with our hands-on experiences …

Intro to our OT/IT Networking journey

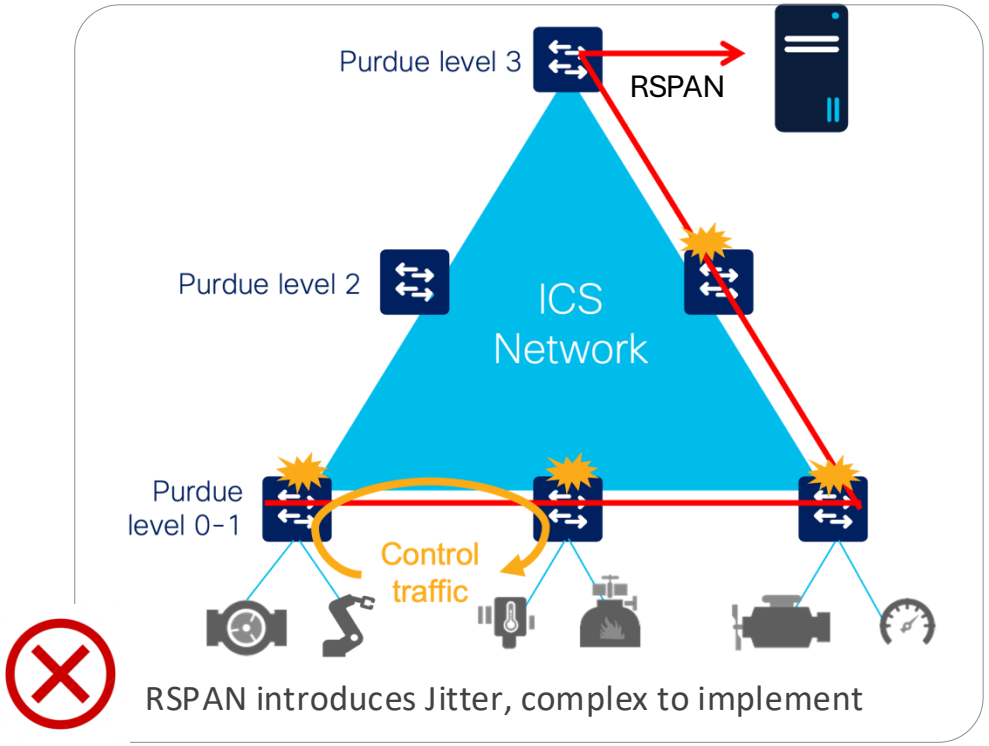
# Cisco Cyber Vision

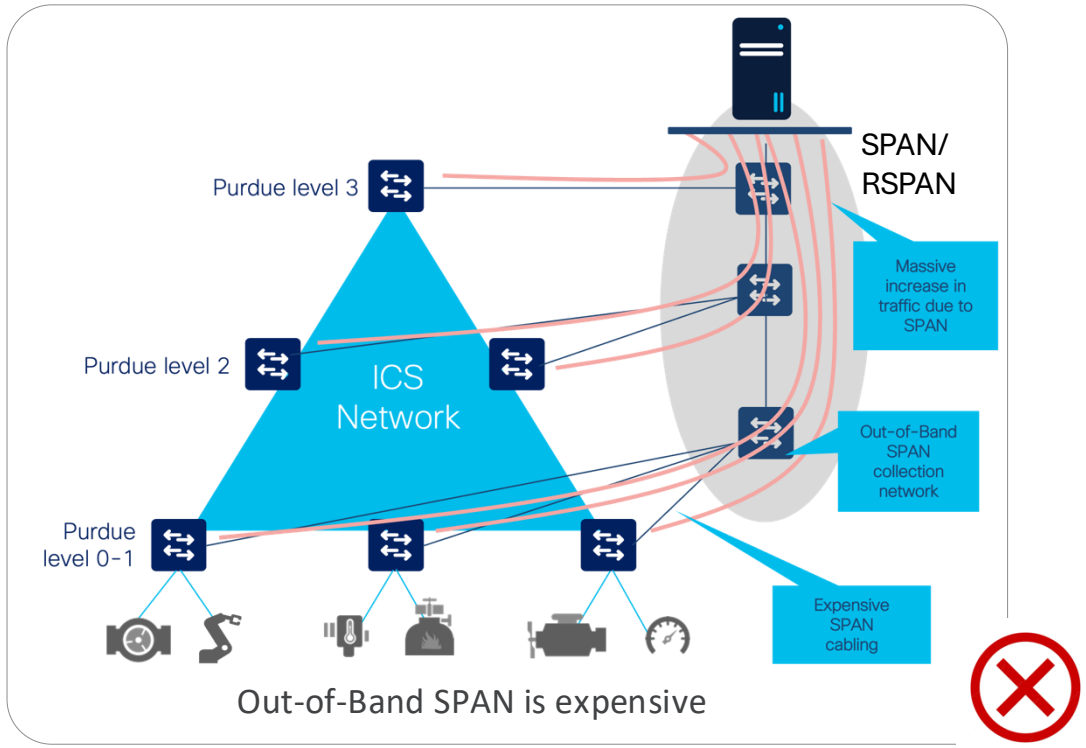
## Visibility built into your network infrastructure




The Cisco industrial network lets you see everything that connects to it

# How to Get Data to Server via RSPAN Infrastructure …




We know, that's complex, risky and expensive, but … we did it like this ….

# Cisco Cyber Vision portfolio – Let's play with sensors ….

## 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

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

Amazon Web Services

Microsoft Azure

**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

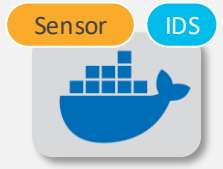

Catalyst IR1800 Cellular Router


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

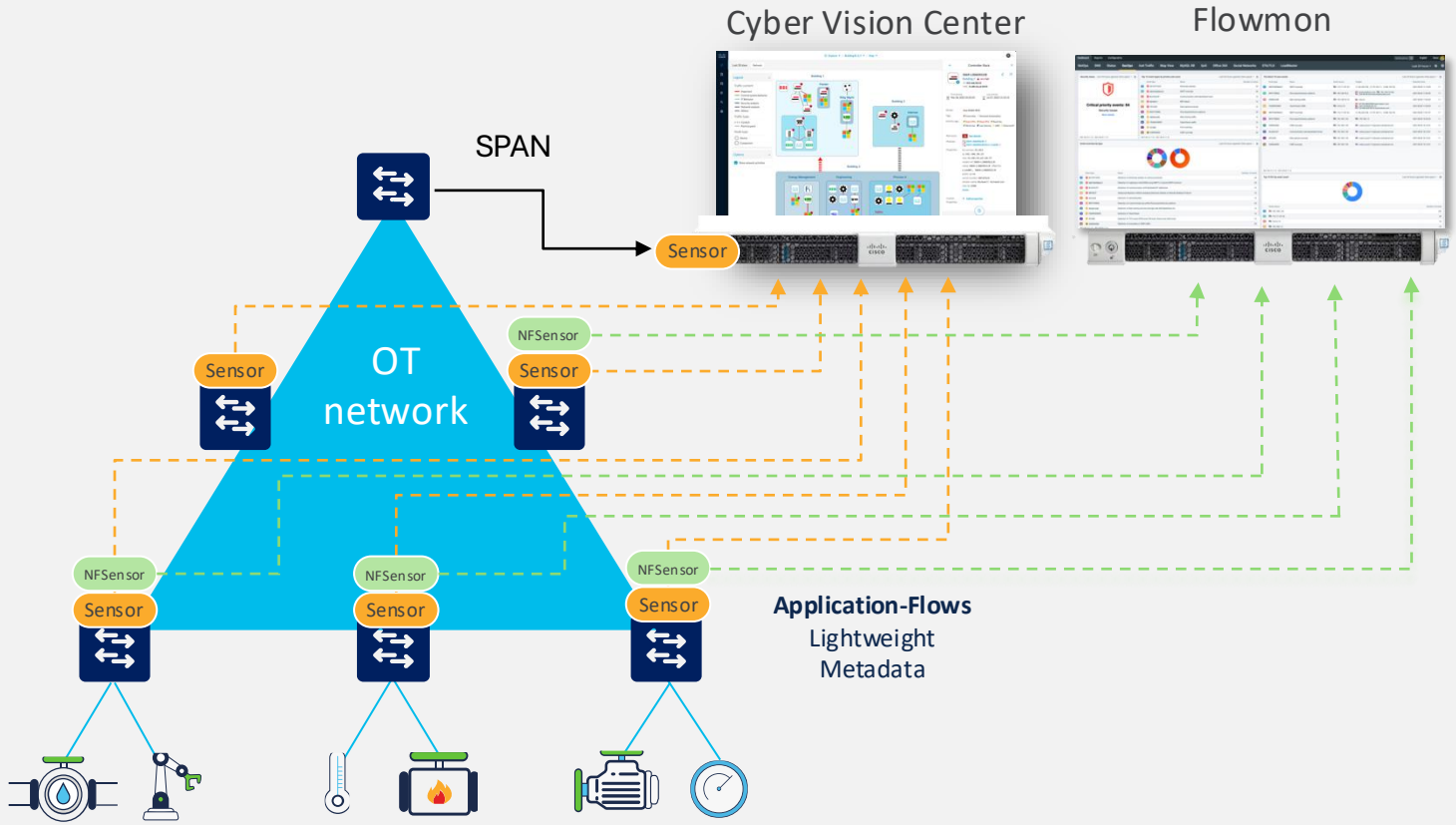
# From Big (mirrored data) to Small (metadata)

Fully Sensory infrastructure Introduction

Embedded Applications Introduction

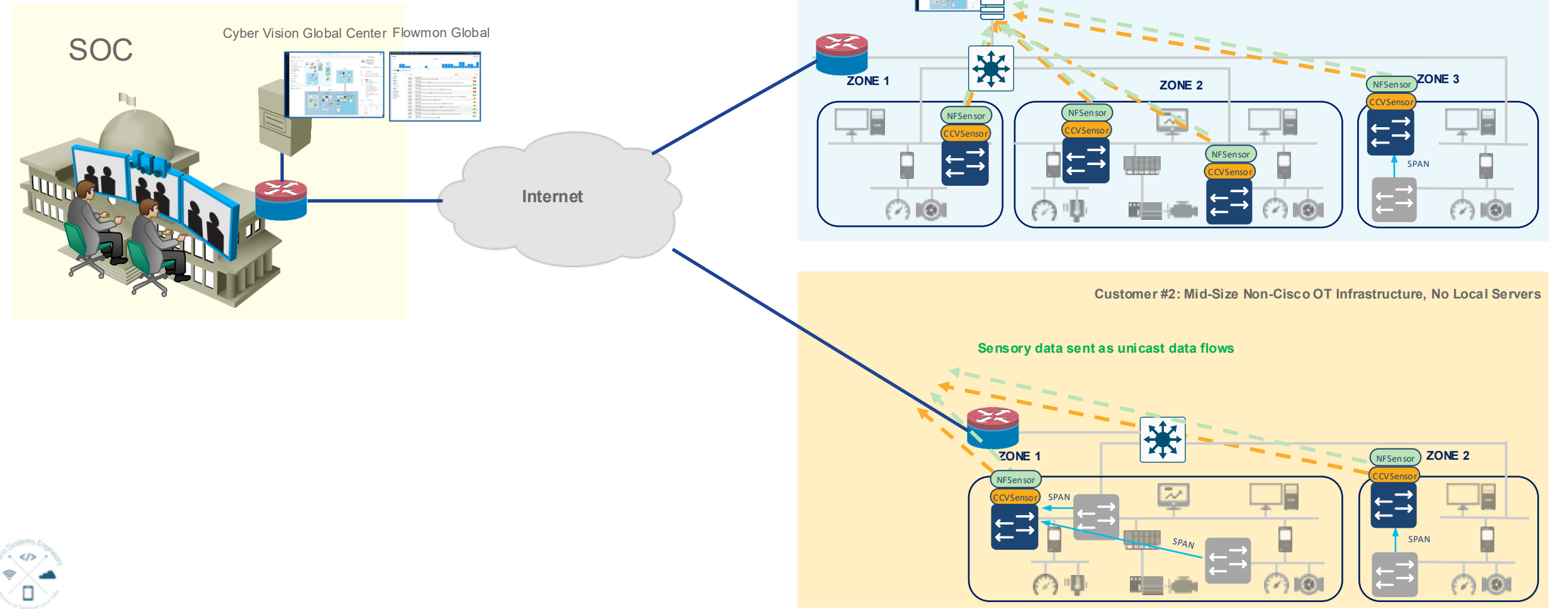
# GOAL :Cisco Cyber Vision and Flowmon in **Fully Sensory Mode**

## Deeper Visibility built into your network infrastructure




Let’s do it a more challenging but effective and innovative way ….

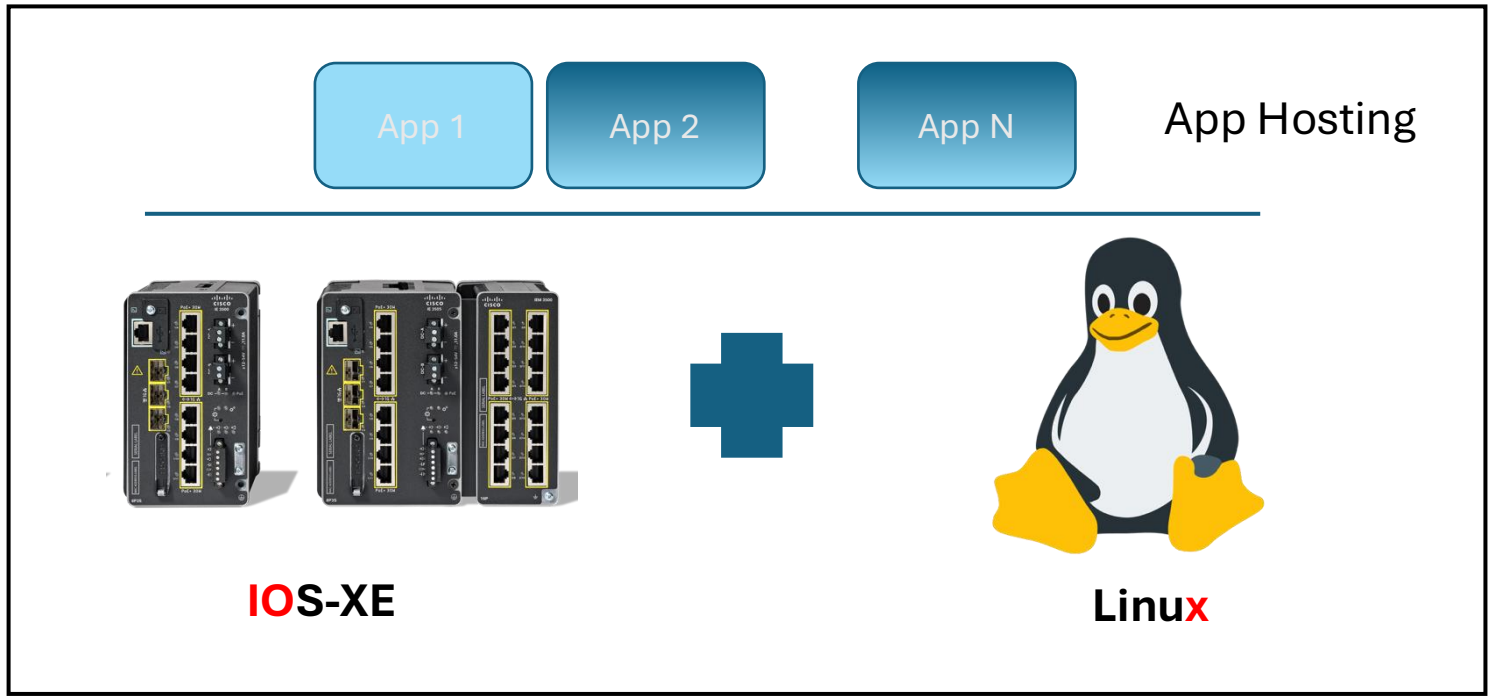
# Why ?
# To Be Ready for Future OT Networks Remote Support



# Cisco Cyber Vision Sensor as a Docker App on IE-3400/3500

Embedded Application Architecture Introduction

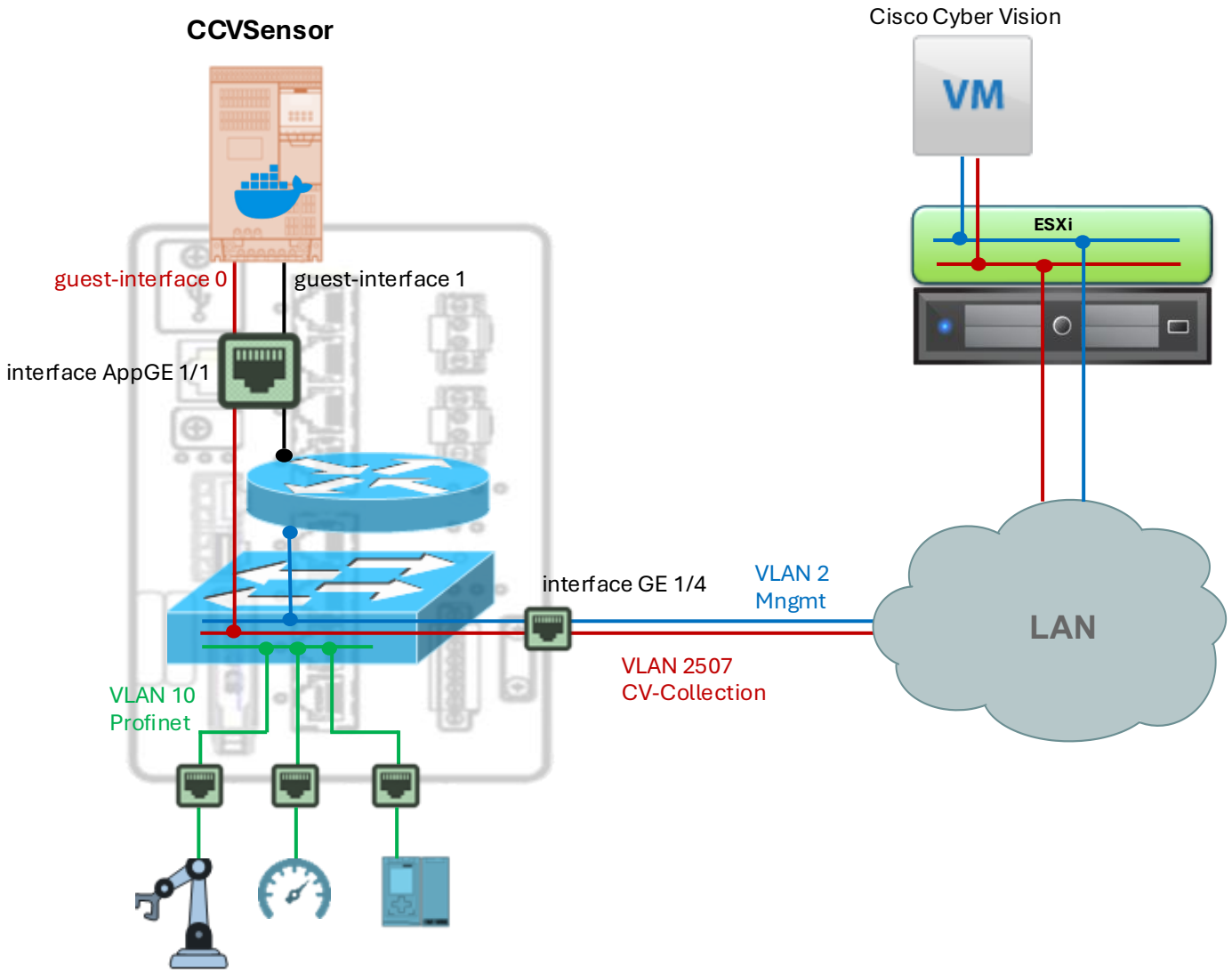
# Cisco IOX Concept for **Embedded Apps**





- IE3x00 with Dockerized App
- **Round-trip-Time Measurement** and Visualization App of IT and OT part of the Deployed Remote App Solution

# CCVSensor SOI IOx Architecture



# Flowmon Probe/NFSensor

## Fully Sensory SOI CyberSec/Analytical Infrastructure

May 2026

# Flowmon Short Intro

### Full network visibility

For NPMD, troubleshooting and capacity planning with full analytics drilldown.

### Dashboards and visualization

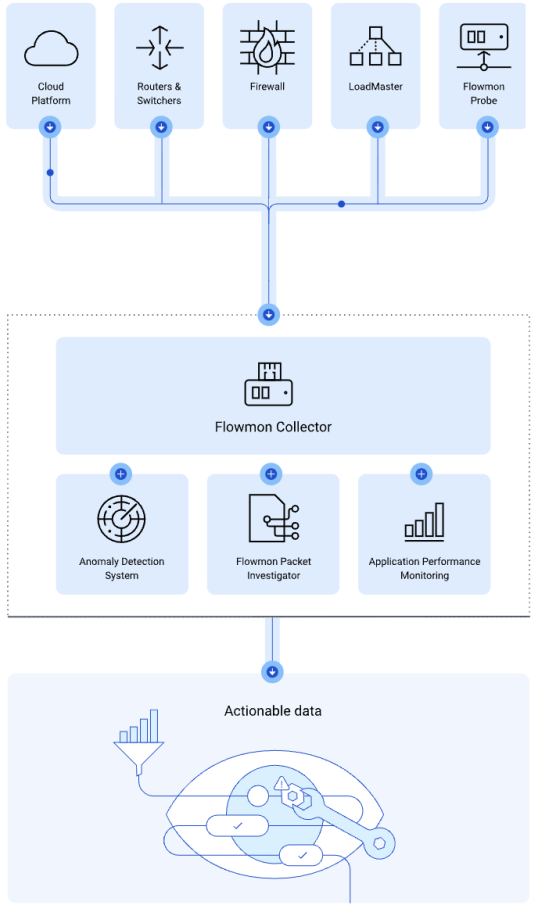
Customizable interface for the noise-free visualization of traffic structure or performance metrics.

### Stop threats

Ransomware, malware, insider & unknown threats, SUNBURST Trojan Attack, etc.

### No security gaps

Between perimeter and endpoint protection. Leverage AI/ML to detect threats others miss.




## 1. Generate Input Data

- Flowmon solution can ingest data from various sources and devices.
- Flow technology support (NetFlow, IPFIX, sFlow, jFlow, cflowd, NetStream, all RFC flow formats) and cloud native FlowLogs support (Azure, AWS, Google Cloud Platform).
- Leverage Flowmon sensors to generate L2-L7 enriched NetFlow data.

Learn more: Flowmon Probe

## 2. Collect & Analyze

- Data are processed by the Flowmon Collector.
- Visualize and analyze network telemetry from various sources in dashboards, reports, root-cause analysis.
- Extending software modules available on-demand.

Learn more: Flowmon Collector

## 3. Act

- Stop breaches, prevent harm.
- Move from reactive to proactive troubleshooting.
- Streamline routine network operations.

Learn more: Flowmon ADS, Flowmon FPI, Flowmon APM

# Flowmon Probe

FLOWMON PROBE

## NetFlow and IPFIX Exporter

The Flowmon Probe is the most powerful flow data exporter on the market that generates data down to the application level and measures performance.

LAUNCH DEMO


### Flowmon Probe Benefits

- **Use It Anywhere**
  Hardware, virtual or cloud, from 10 Mb/s to 100 Gb/s.
- **Stay Non-Intrusive**
  The Probe connects passively through a SPAN port or network TAP.
- **Reduce Noise**
  Network data is pre-filtered to enable clearer analysis and visualization.

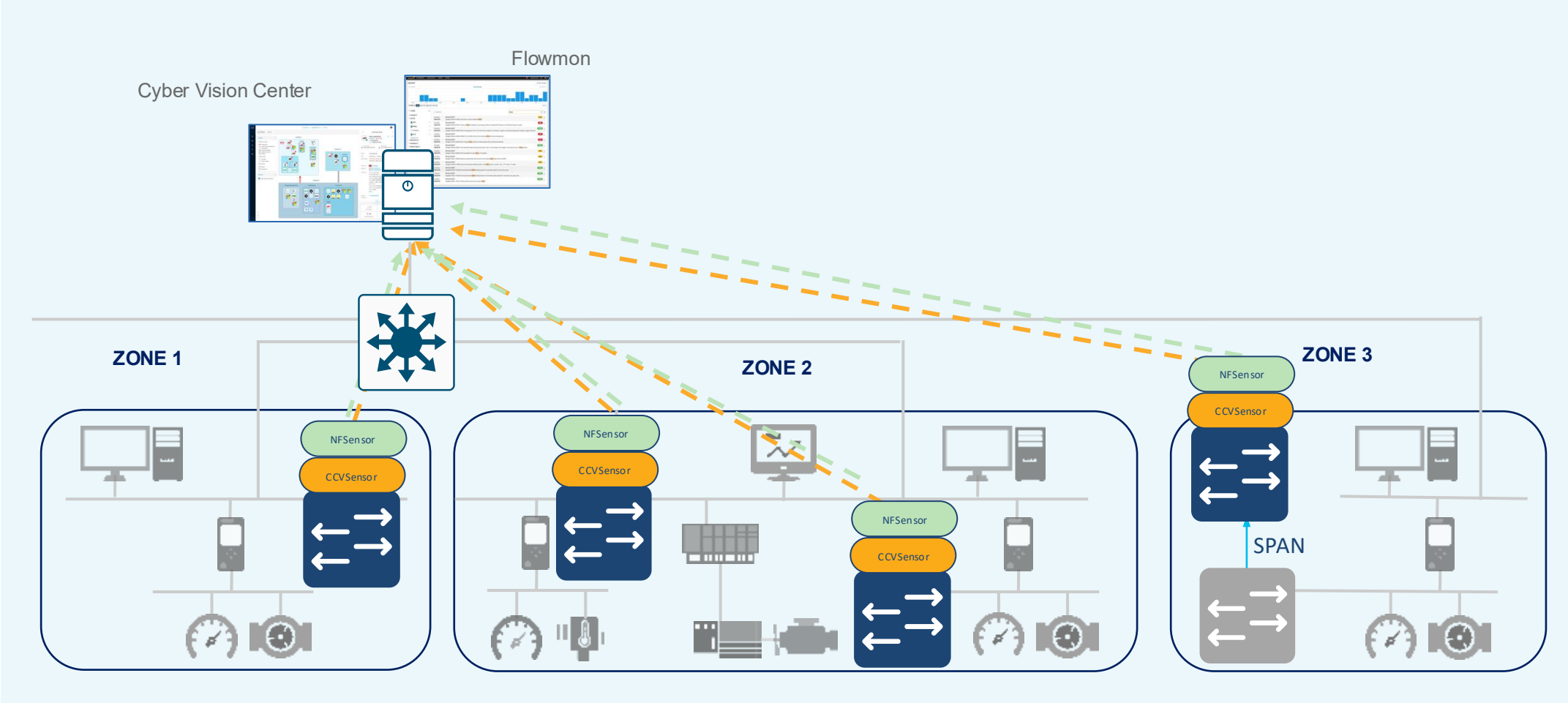
## Flowmon Probe

Flowmon Probe is a high-performance appliance that monitors network traffic and generate IP flow statistics. The flow statistics are then exported to storage for further analysis by a Flowmon Collector or other NetFlow/IPFIX compatible application. The Probe provides NetFlow/IPFIX data necessary for network operations, troubleshooting, performance, and security monitoring.

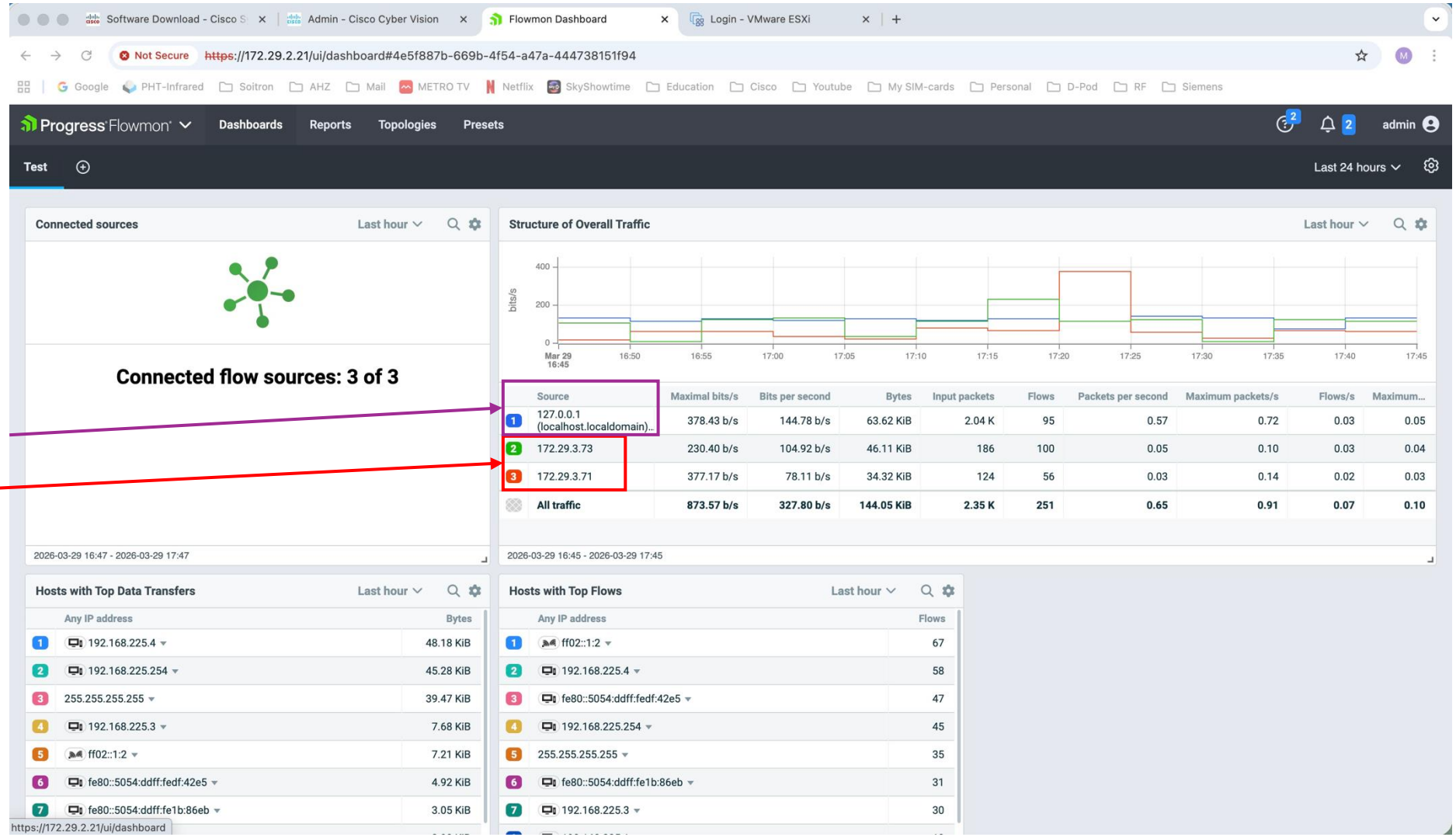
Flowmon Probe is available in the form of a hardware appliance of 1U rack unit size and as a virtual appliance for deployment into VMware, Hyper-V, and KVM virtual environments.

vmware KVM Microsoft Hyper-V

# Not to use RSPAN to Flowmon,
# But to use IOx for NFSensor on IE-3500



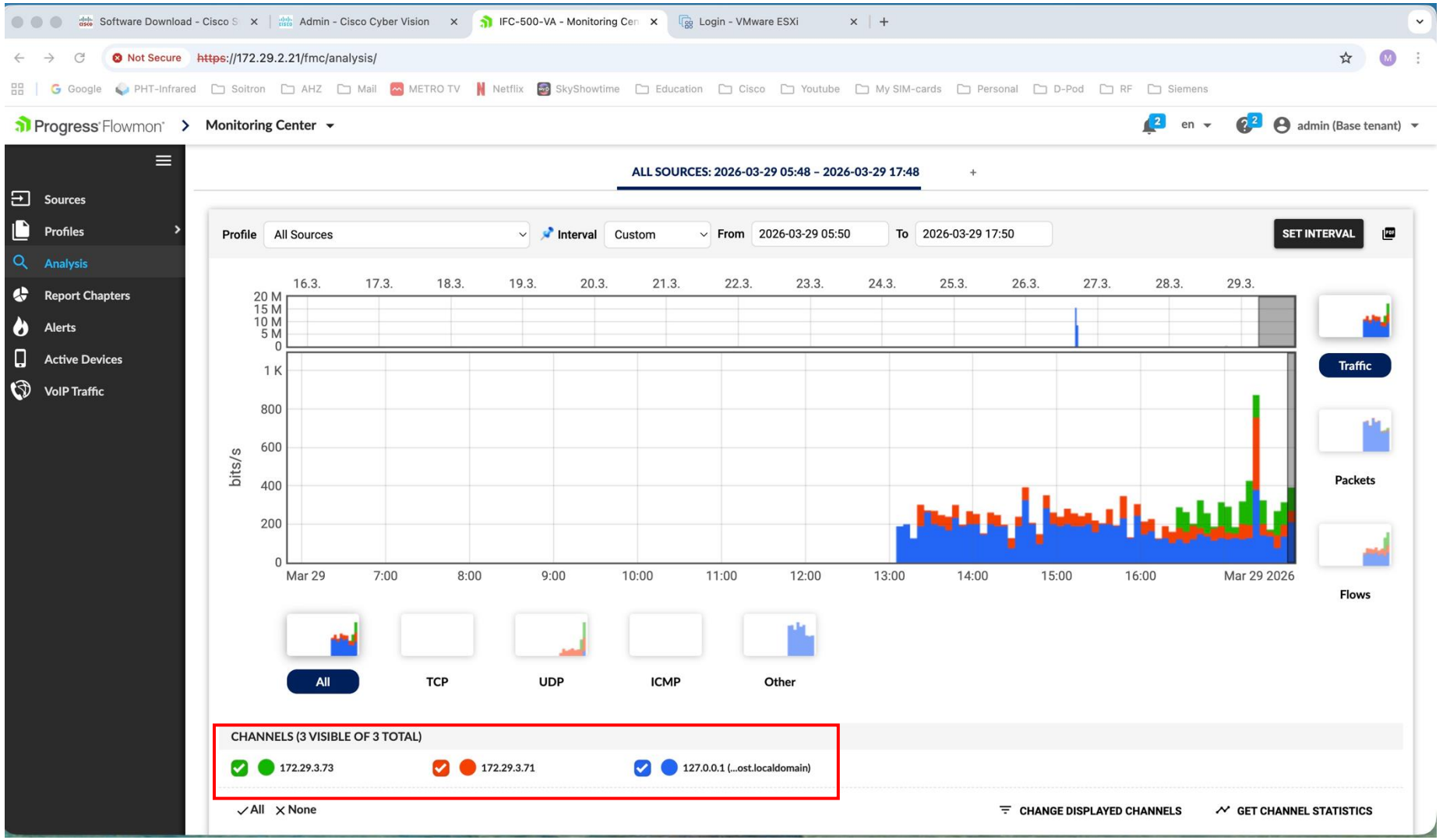
# Flowmon - Sources




Flowmon Collector

NFSensors

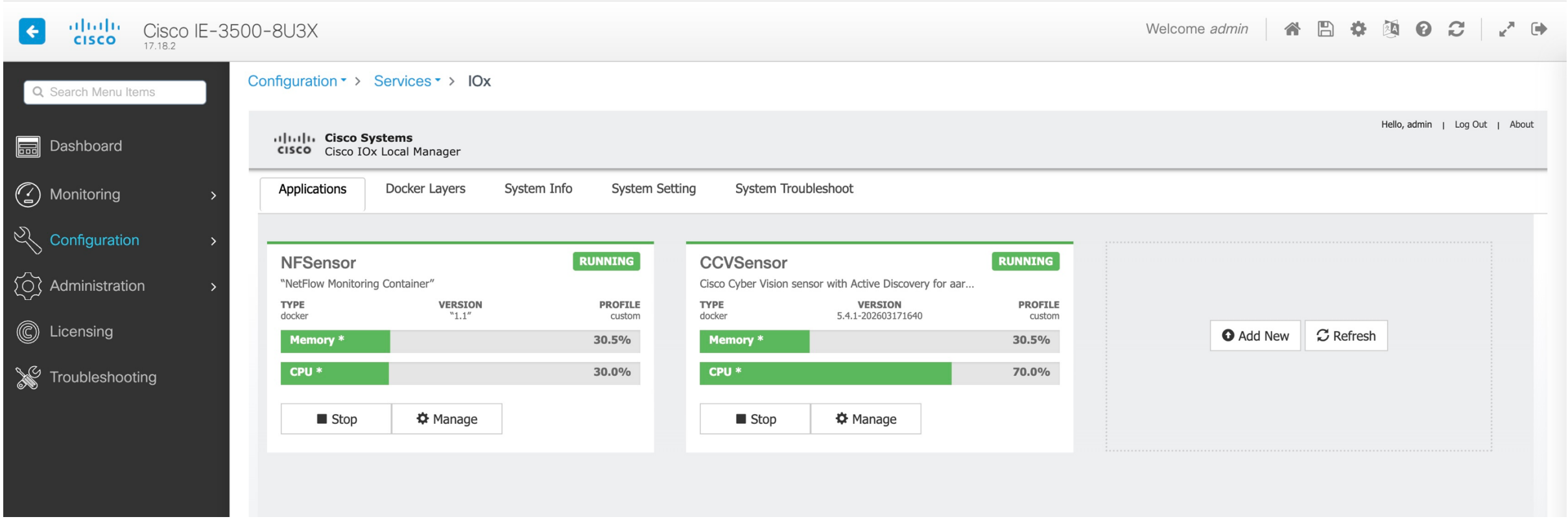
# Flowmon – Analysis from NFSensors Sources



# Fully Sensory CyberSec/Analytical Infrastructure on IE-3x00 switch

May 2026

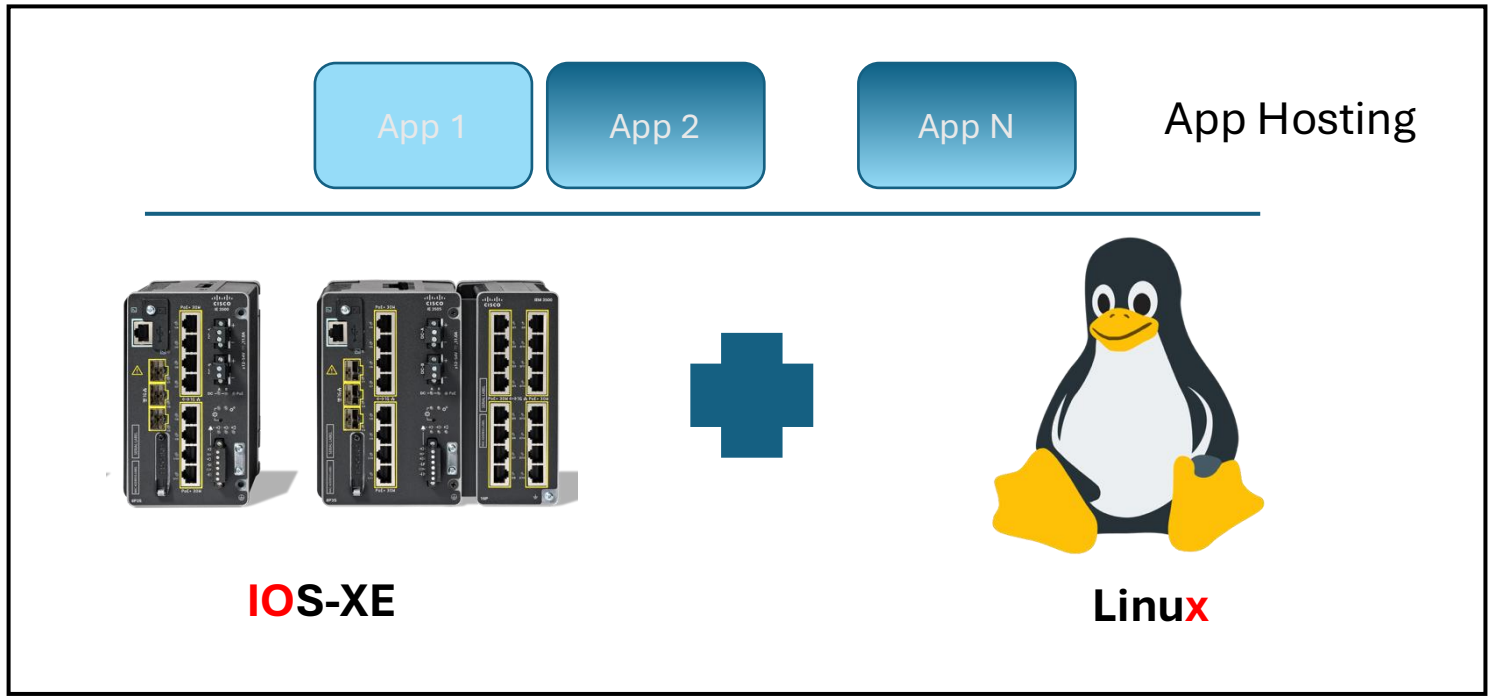
# Fully Sensory Architecture – IE-3500, SOI Lab

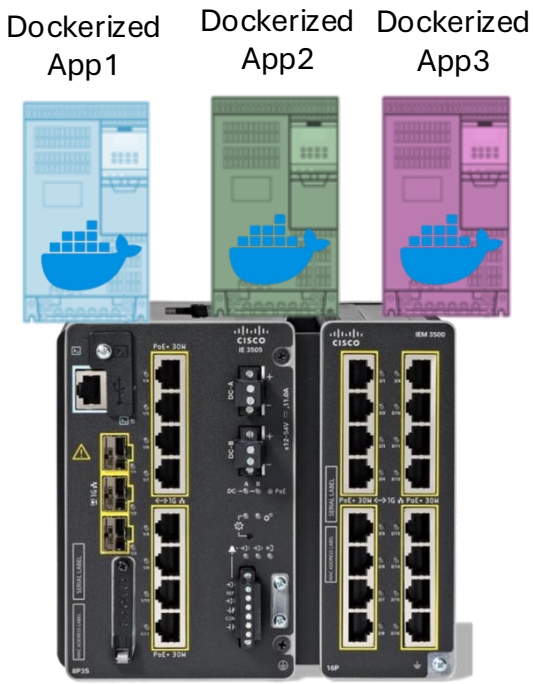


# App Responsiveness Measurement - SLAMonitor App

Embedded App for SLA App/Servers Monitoring

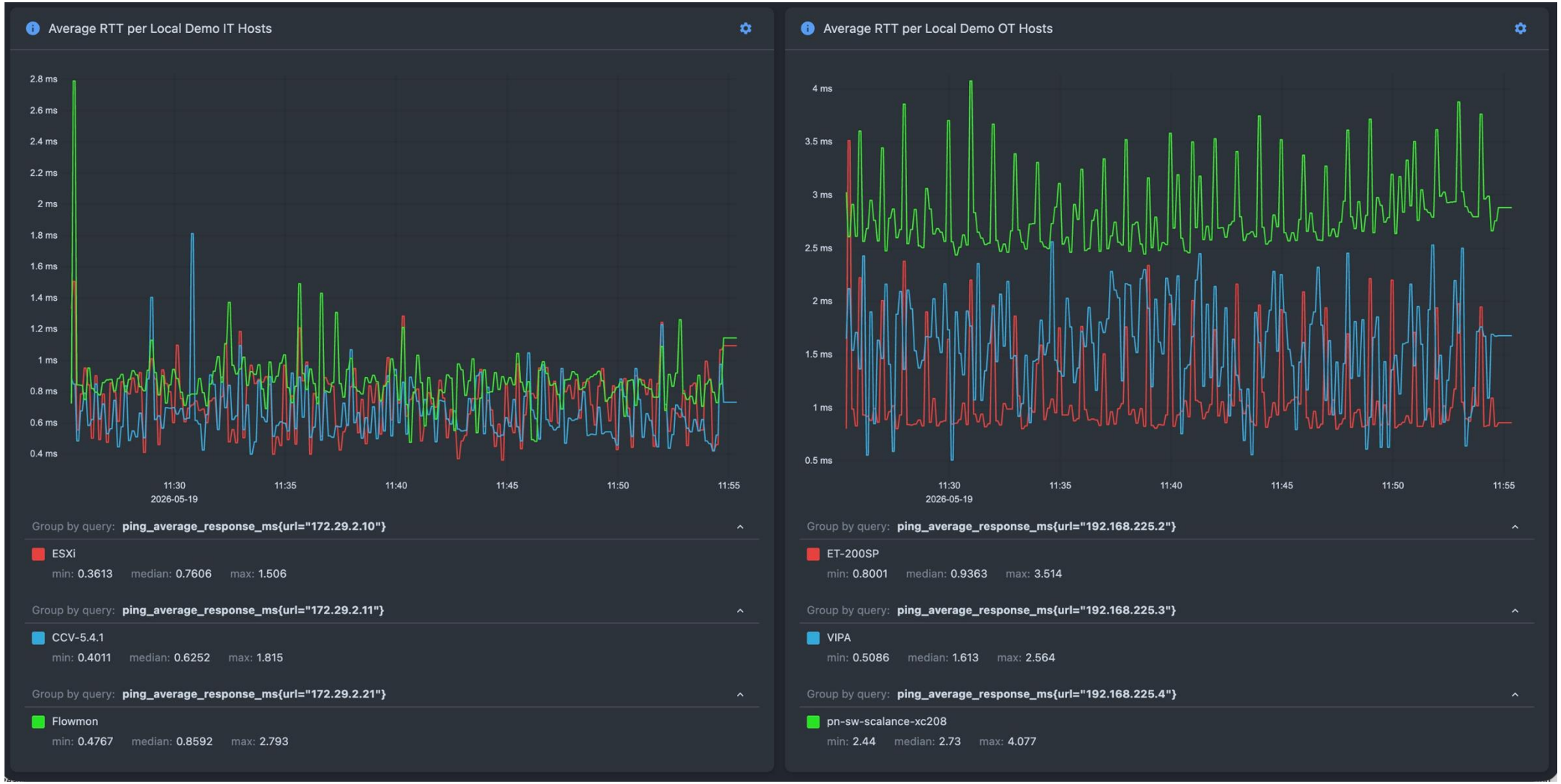
# Cisco IOX Concept for Critical Apps Operation Diagnostics and Monitoring



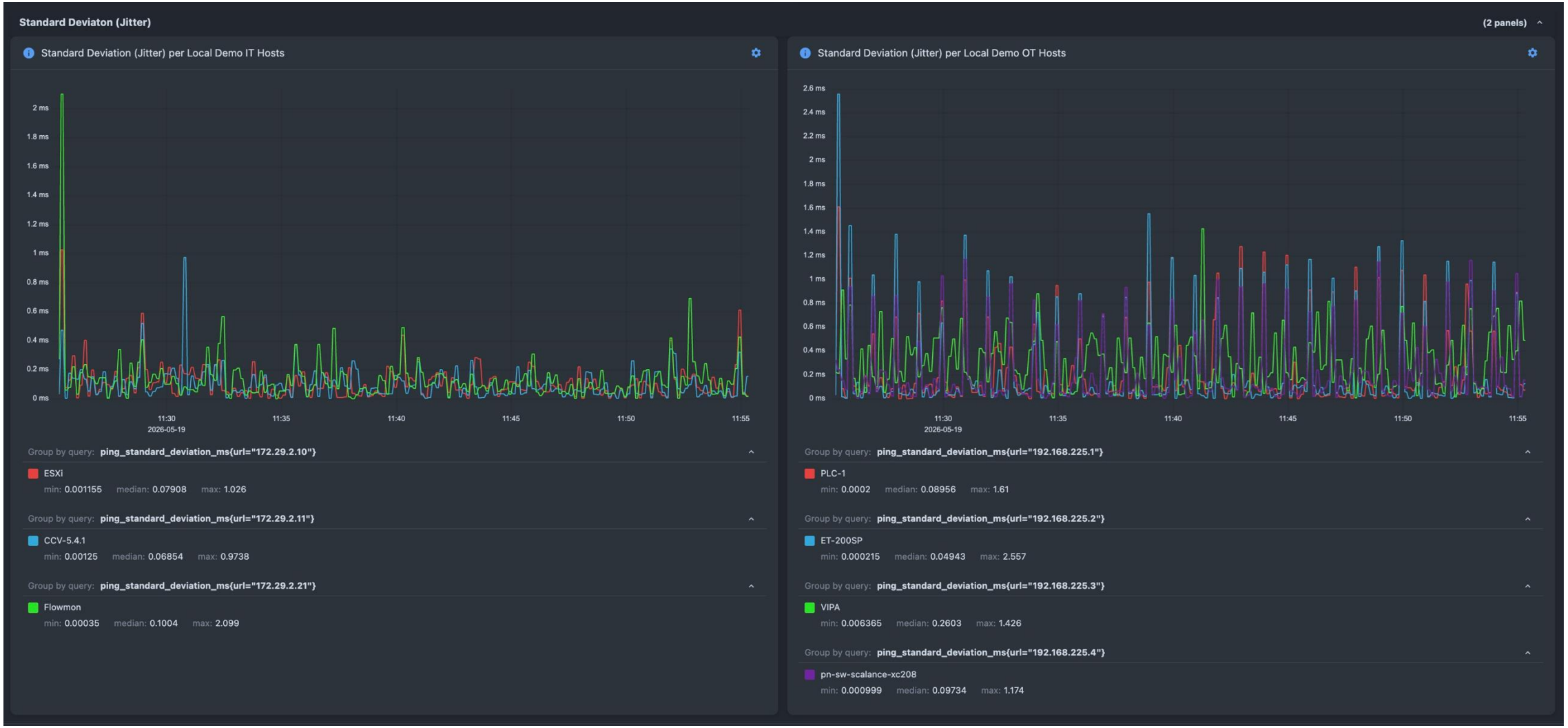




- IE3x00 with Dockerized App
- **Round-trip-Time Measurement** and Visualization App of IT and OT part of the Deployed Remote App Solution

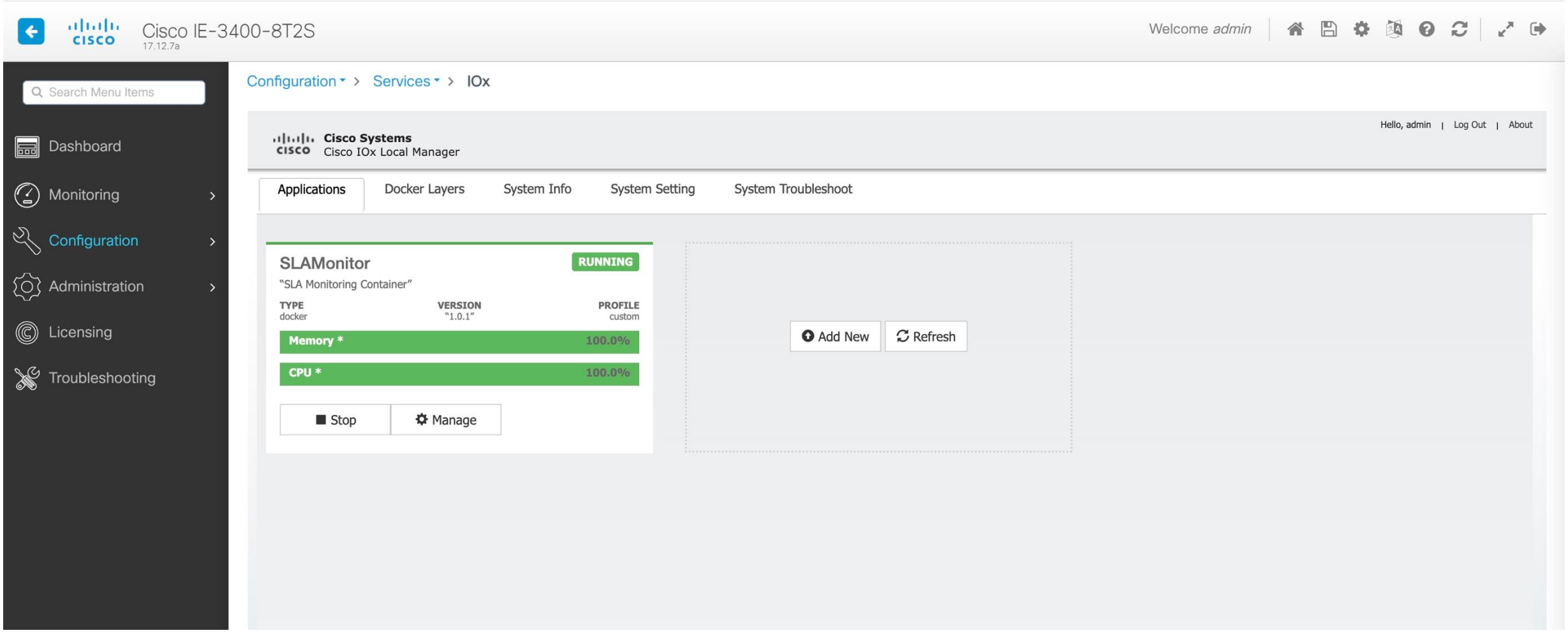
# SLAMonitor App on IE3400 – RTT Per IT/OT Groups



# SLAMonitor App – Jitter Per IT/OT Groups



# SLAMonitor App on IE3400 – App Resources



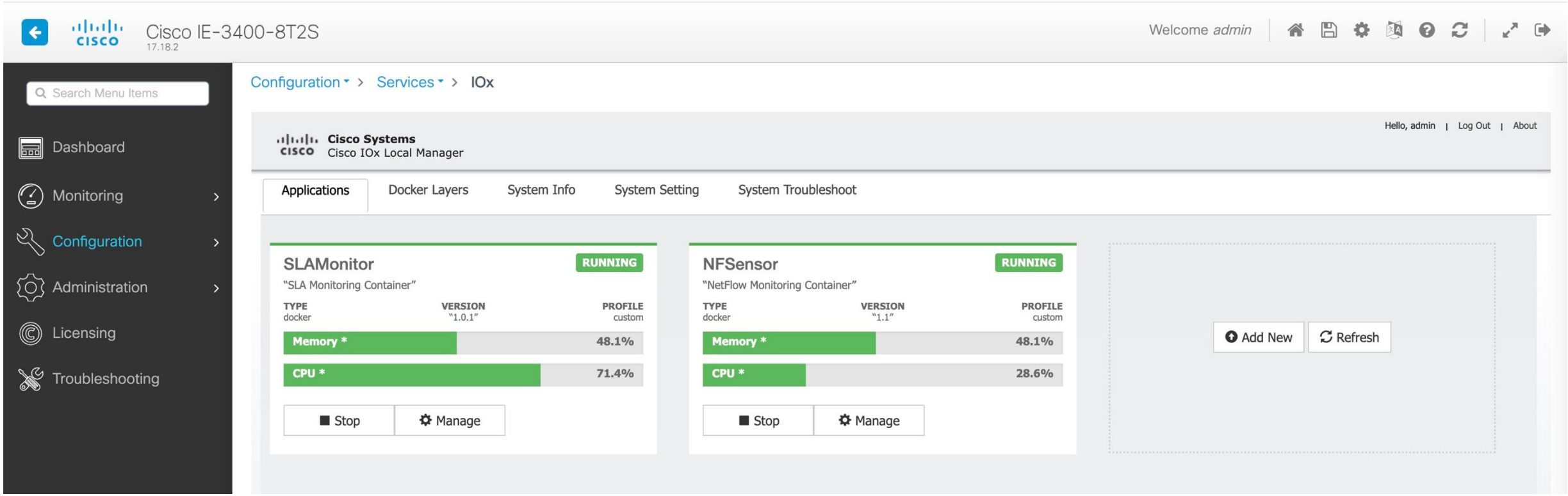
# SLAMonitor App on IE3400 – Utilization from cli …

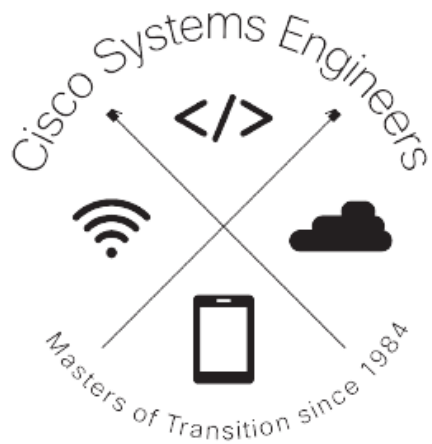
```
IE3400#sh app-hosting utilization appid SLAMonitor
Application: SLAMonitor
CPU Utilization:
  CPU Allocation: 1400 units
  CPU Used:       0.57 %
  CPU Cores:      0-3

Memory Utilization:
  Memory Allocation: 1248 MB
  Memory Used:       70928 KB
Disk Utilization:
  Disk Allocation: 3000 MB
  Disk Used:       0.62 MB

IE3400#
```

# SLAMonitor and NFSensor Apps on IE3400






SOITRON industry

CONTROL SYSTEM