



# Sensory Architecture for Safe and Reliable Operation

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

Michal Remper, [michal.remper@soitron.com](mailto:michal.remper@soitron.com)

Roland Rais, [roland.rais@soitron.com](mailto:roland.rais@soitron.com)

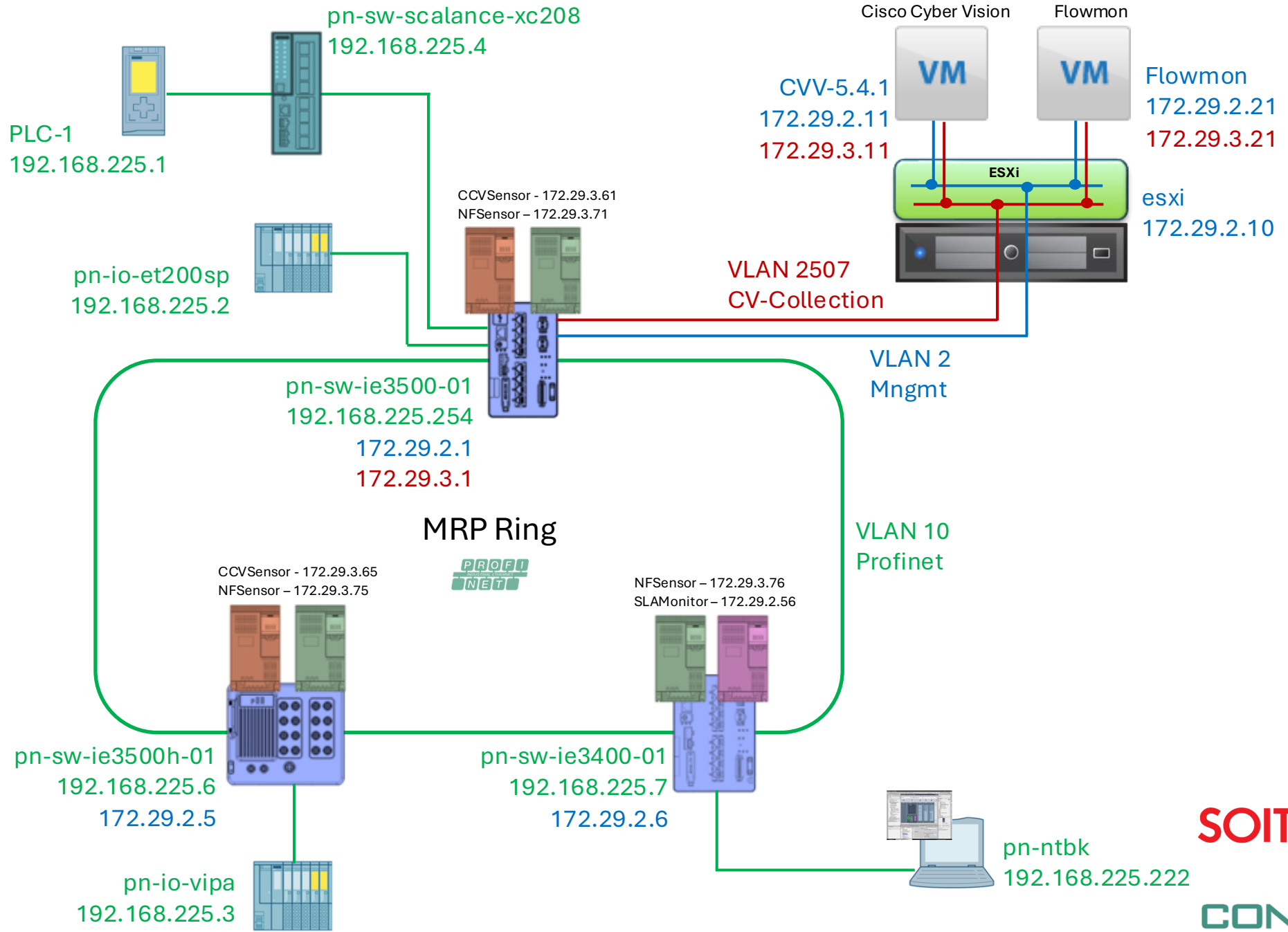
Simon Remper, [simon.remper@gmail.com](mailto:simon.remper@gmail.com)

May 2026



# Today Demo Topology

New Project challenge



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

The screenshot displays the Siemens TIA Portal interface for a project named 'teststand\_V20'. The main workspace shows a network diagram in 'Topology view'. A central horizontal bus labeled 'PN/IE\_1' connects several devices:

- Three DP-NORM devices at the top, each associated with a PLC-1 (IE-3500-8U3X, IE-3500H-14P2T, and IE-3400-8T2S).
- Four devices at the bottom: a PLC-1 CPU 1511F-1 PN, an IO-ET-200SP IM 155-6 PN ST, an IO-VIPA053-1P... 053-1PN01 Prof..., and a PN-Sw-SCALAN... SCALANCE XC208.

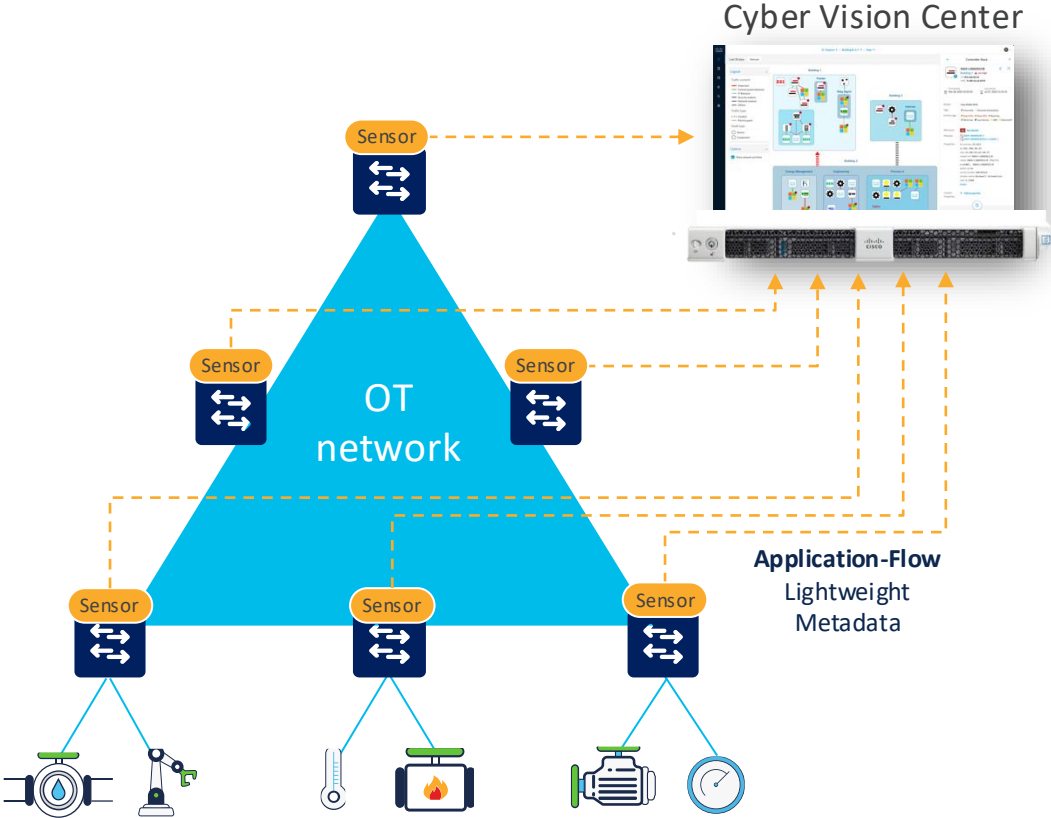
The left sidebar shows the 'Project tree' with a tree view of the project structure. The bottom status bar indicates 'There is no connection to Teamcenter.' The interface includes a menu bar, a toolbar, and a hardware catalog on the right.

# Let's start with our hands-on experiences ...

Intro to our OT/IT Networking journey

# Cisco Cyber Vision

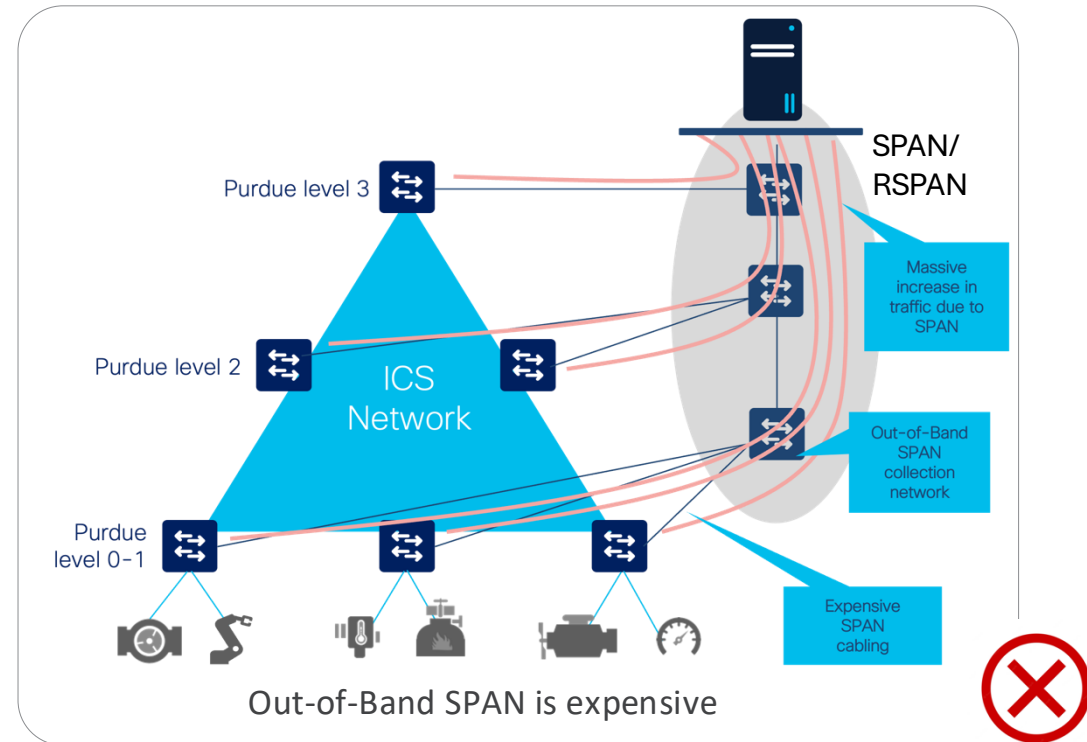
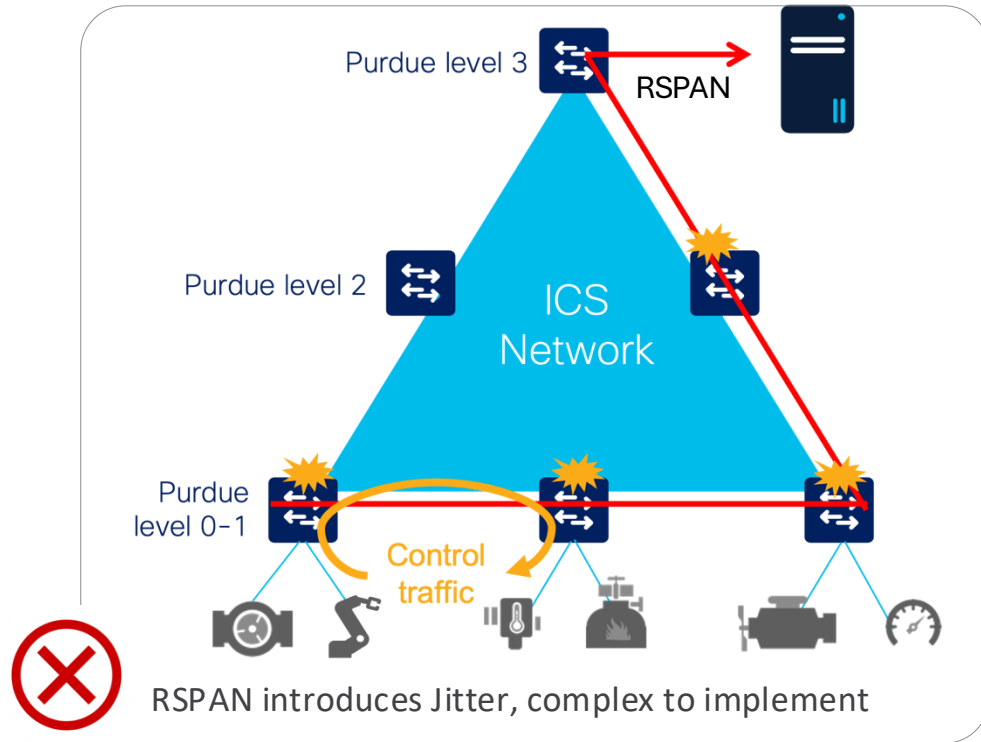
Visibility built into your network infrastructure



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



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

Sensor



Catalyst IE3300, IE3400 and IE3500 Switches

Sensor



Catalyst IE3400HD 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 9300/9400 Aggregation Switches

## Network-Sensors

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

Sensor

IDS



x86 or ARM64 Compute

## Docker Sensor

DPI and active discovery via SPAN to support brownfield

Sensor

IDS



IC3000 Industrial Compute

## Hardware-Sensor



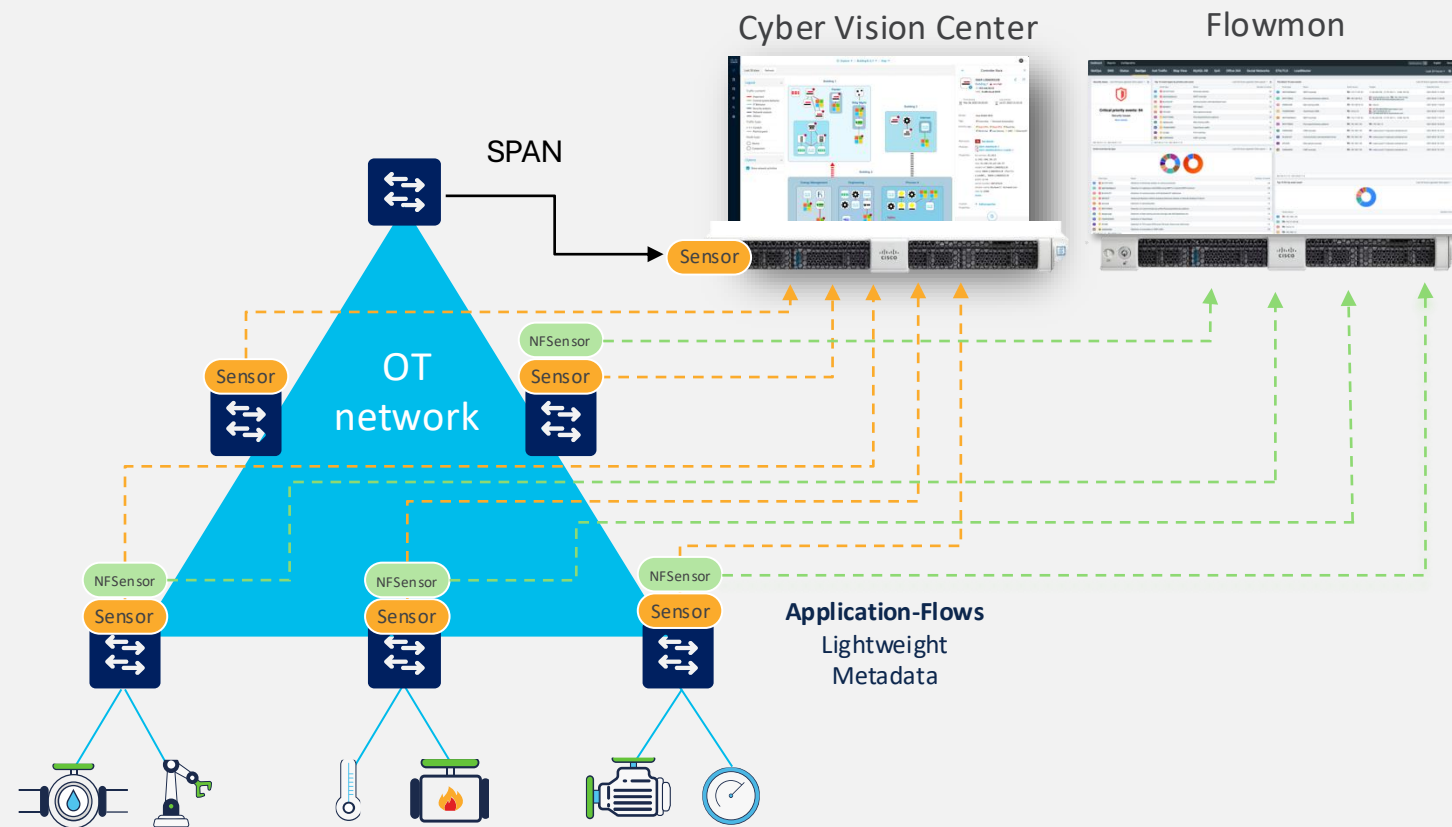
# From Big (mirrored data) to Small (metadata)

Fully Sensory infrastructure Introduction

Embedded Applications Introduction

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

Deeper **Visibility** built into your network infrastructure

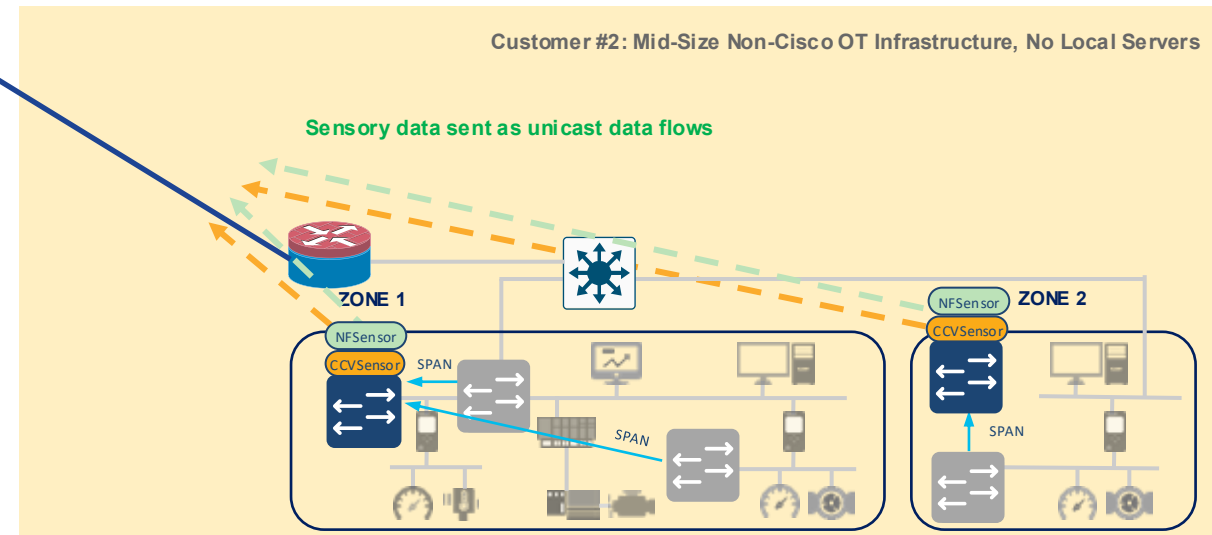
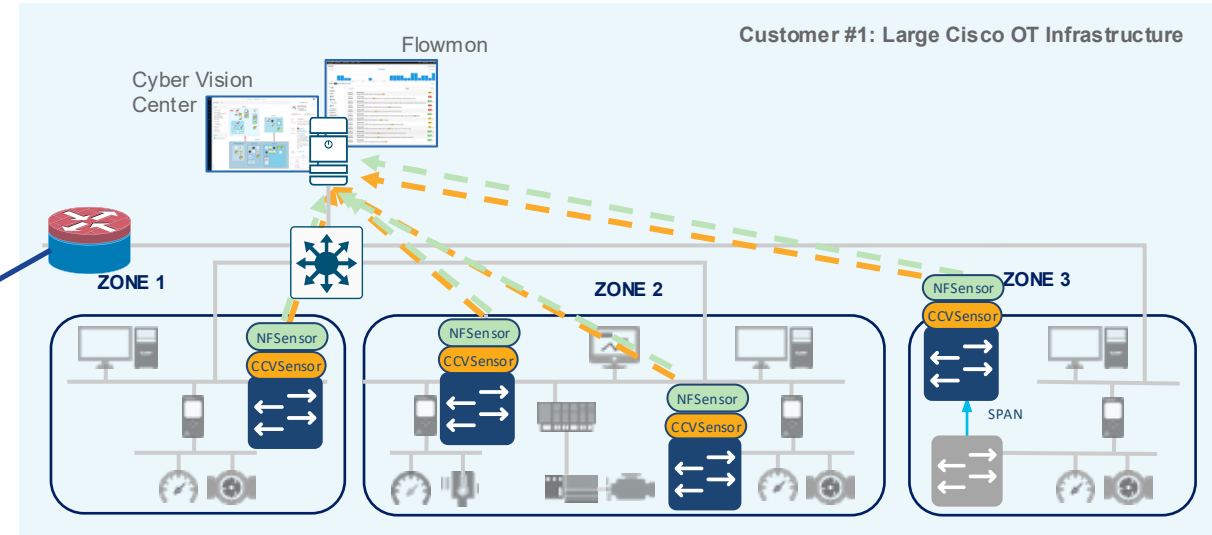
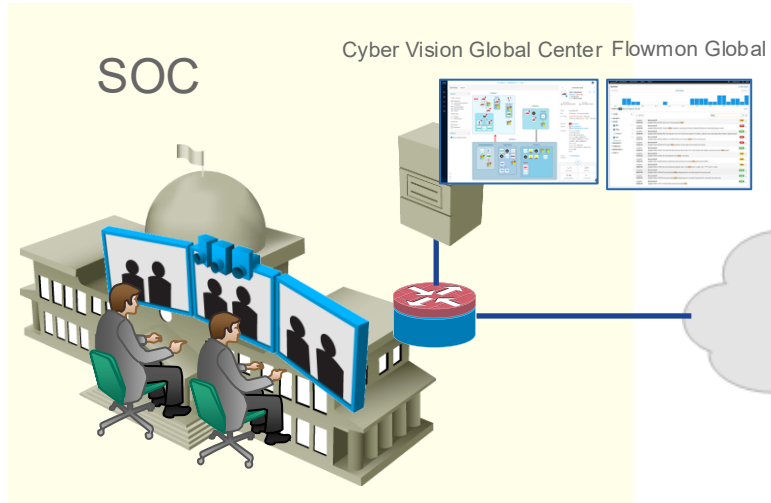


Let's do it a more challenging but effective and innovative way ....



# Why ?

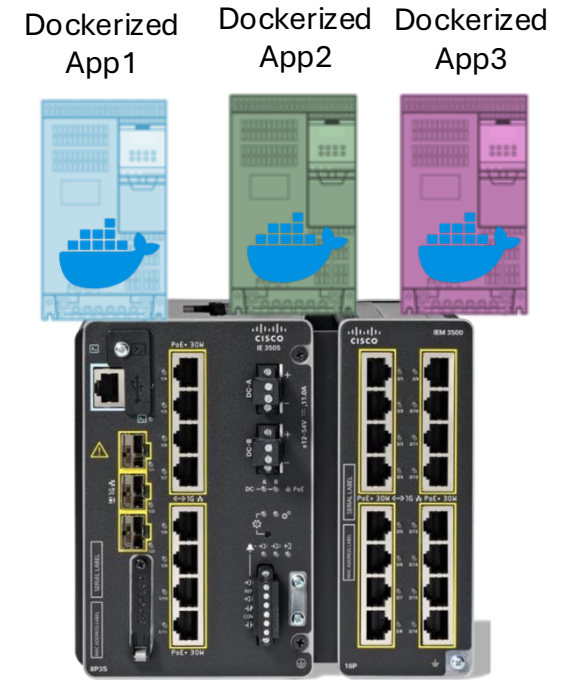
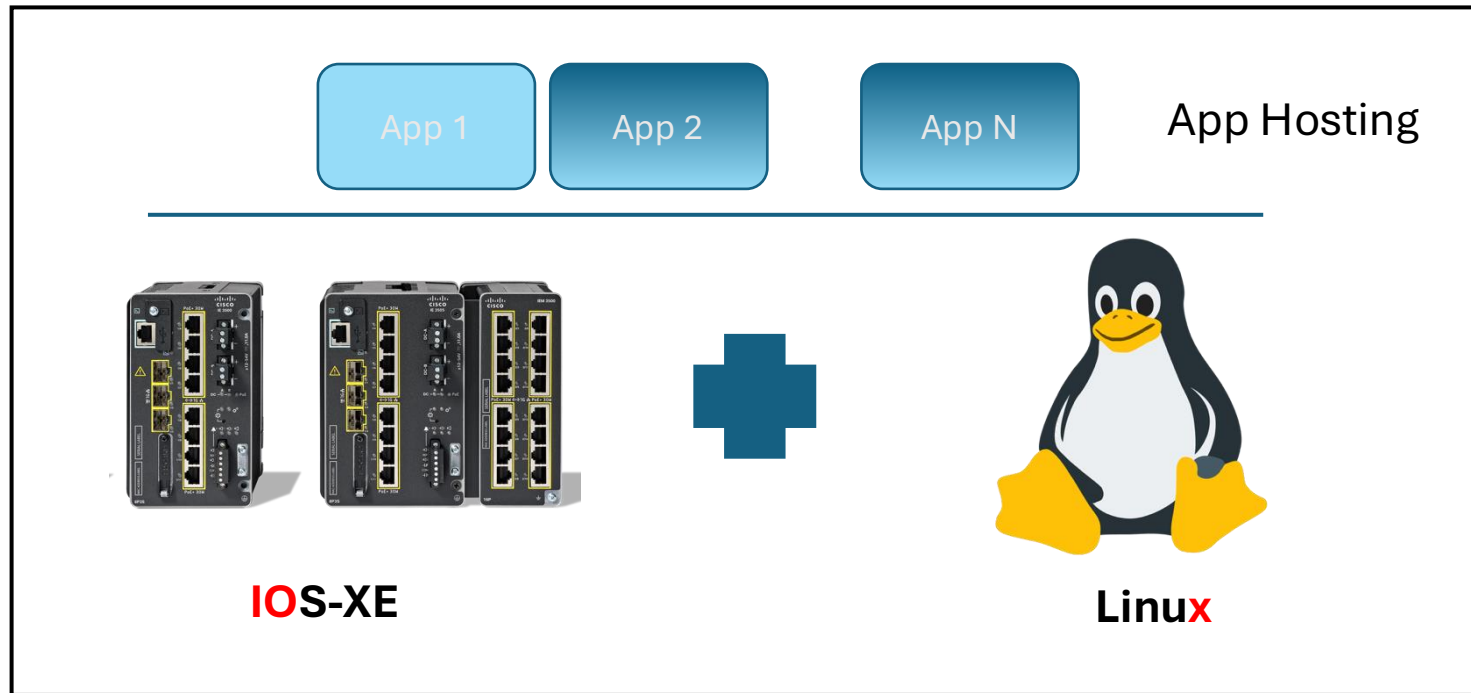
## To Be Ready for Future OT Networks Remote Support



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

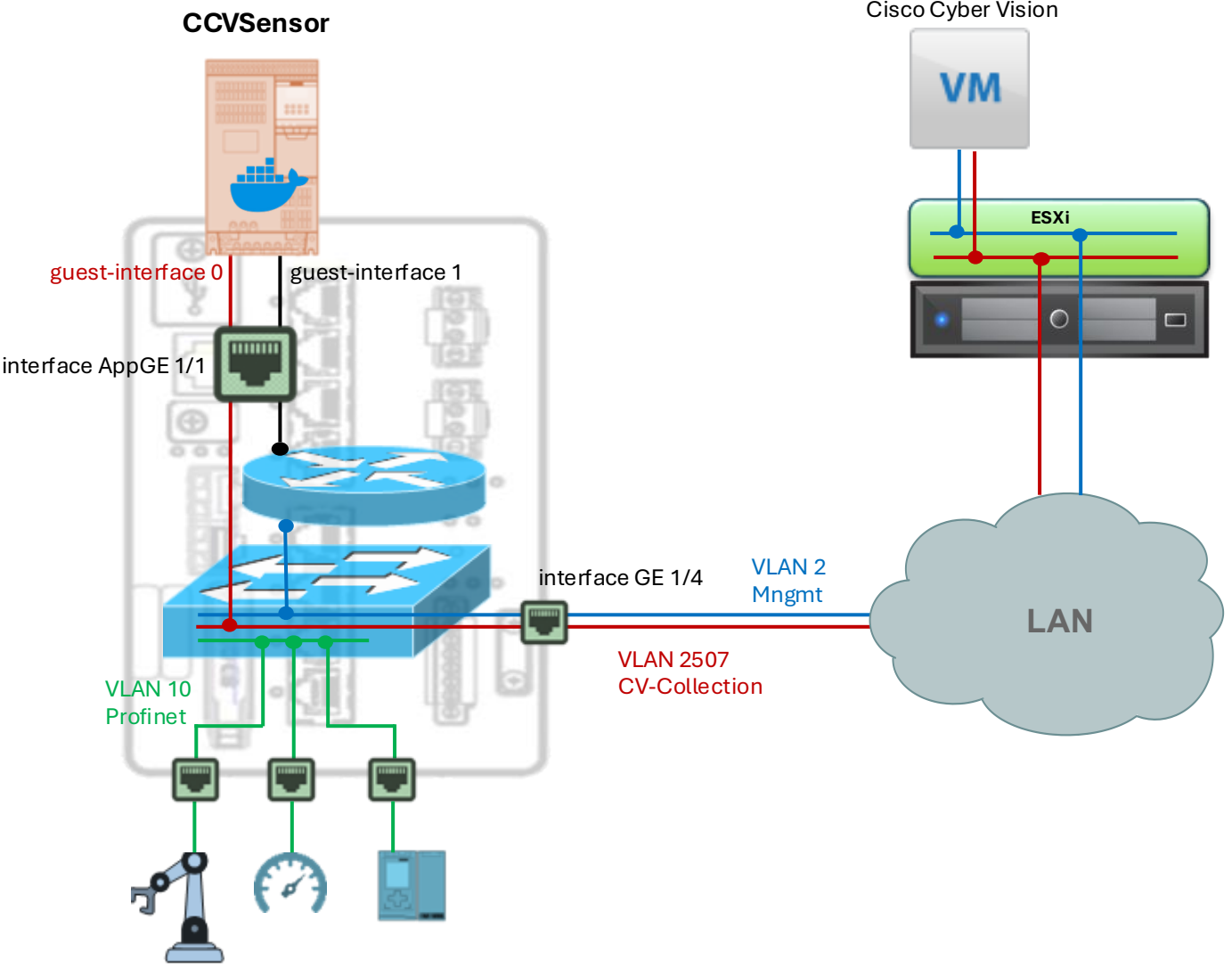
Embedded Application Architecture Introduction

# 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

# CCV Sensor 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

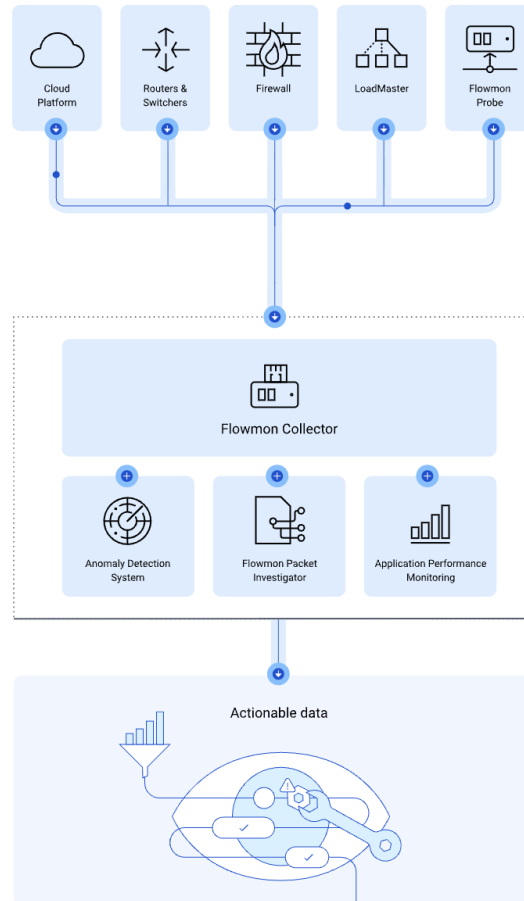
Customizable interface for the noise-free visualization of traffic structure or performance metrics.

## 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.



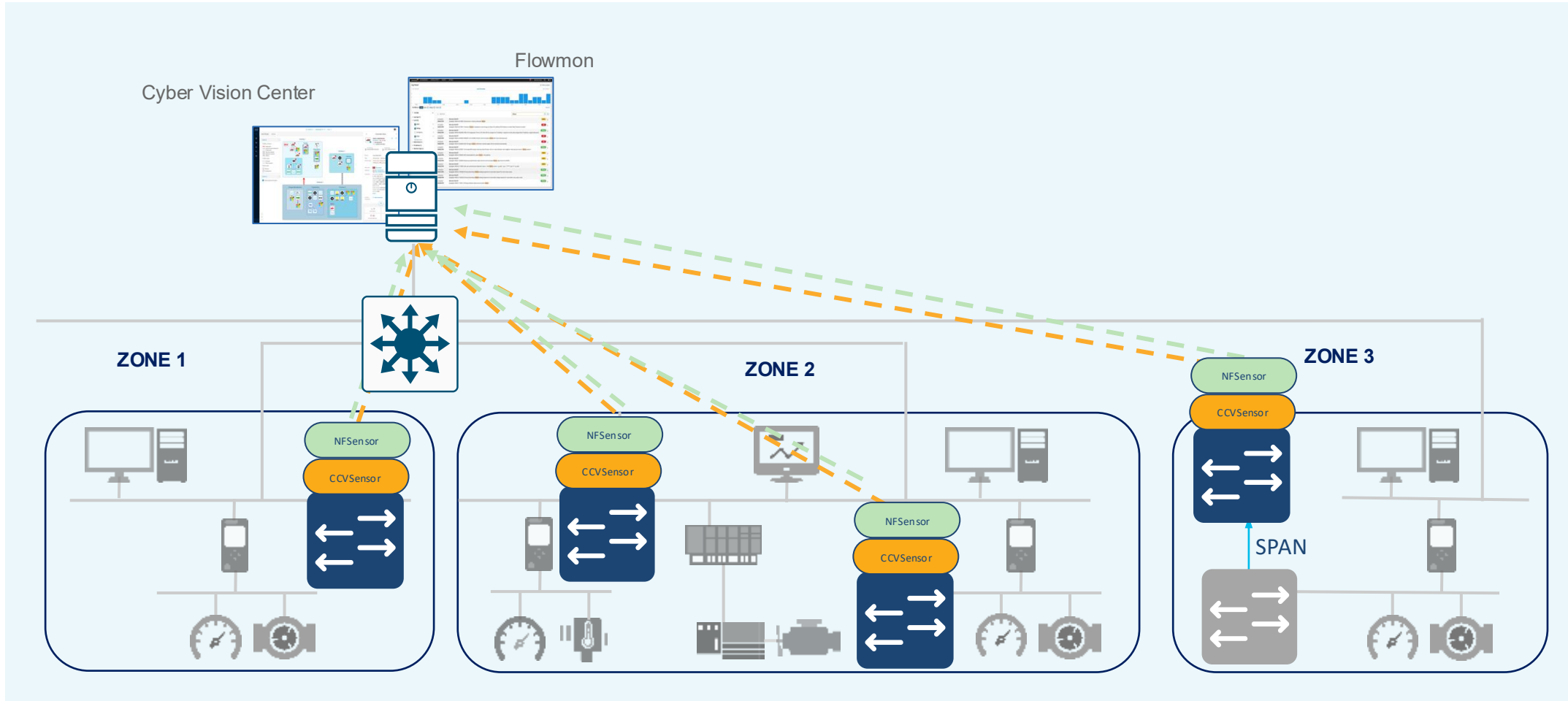
vmware



Microsoft Hyper-V



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



# Flowmon - Sources

The screenshot displays the Flowmon dashboard interface. The top navigation bar includes 'Progress Flowmon', 'Dashboards', 'Reports', 'Topologies', and 'Presets'. The main content area is divided into several sections:

- Connected sources:** Shows 'Connected flow sources: 3 of 3'. A purple arrow labeled 'Flowmon Collector' points to the first source, and a red arrow labeled 'NFSensors' points to the second source.
- Structure of Overall Traffic:** A line graph showing traffic volume in bits/s over time. Below the graph is a table with the following data:

Source	Maximal bits/s	Bits per second	Bytes	Input packets	Flows	Packets per second	Maximum packets/s	Flows/s	Maximum...
1 127.0.0.1 (localhost.localdomain)...	378.43 b/s	144.78 b/s	63.62 KiB	2.04 K	95	0.57	0.72	0.03	0.05
2 172.29.3.73	230.40 b/s	104.92 b/s	46.11 KiB	186	100	0.05	0.10	0.03	0.04
3 172.29.3.71	377.17 b/s	78.11 b/s	34.32 KiB	124	56	0.03	0.14	0.02	0.03
All traffic	873.57 b/s	327.80 b/s	144.05 KiB	2.35 K	251	0.65	0.91	0.07	0.10

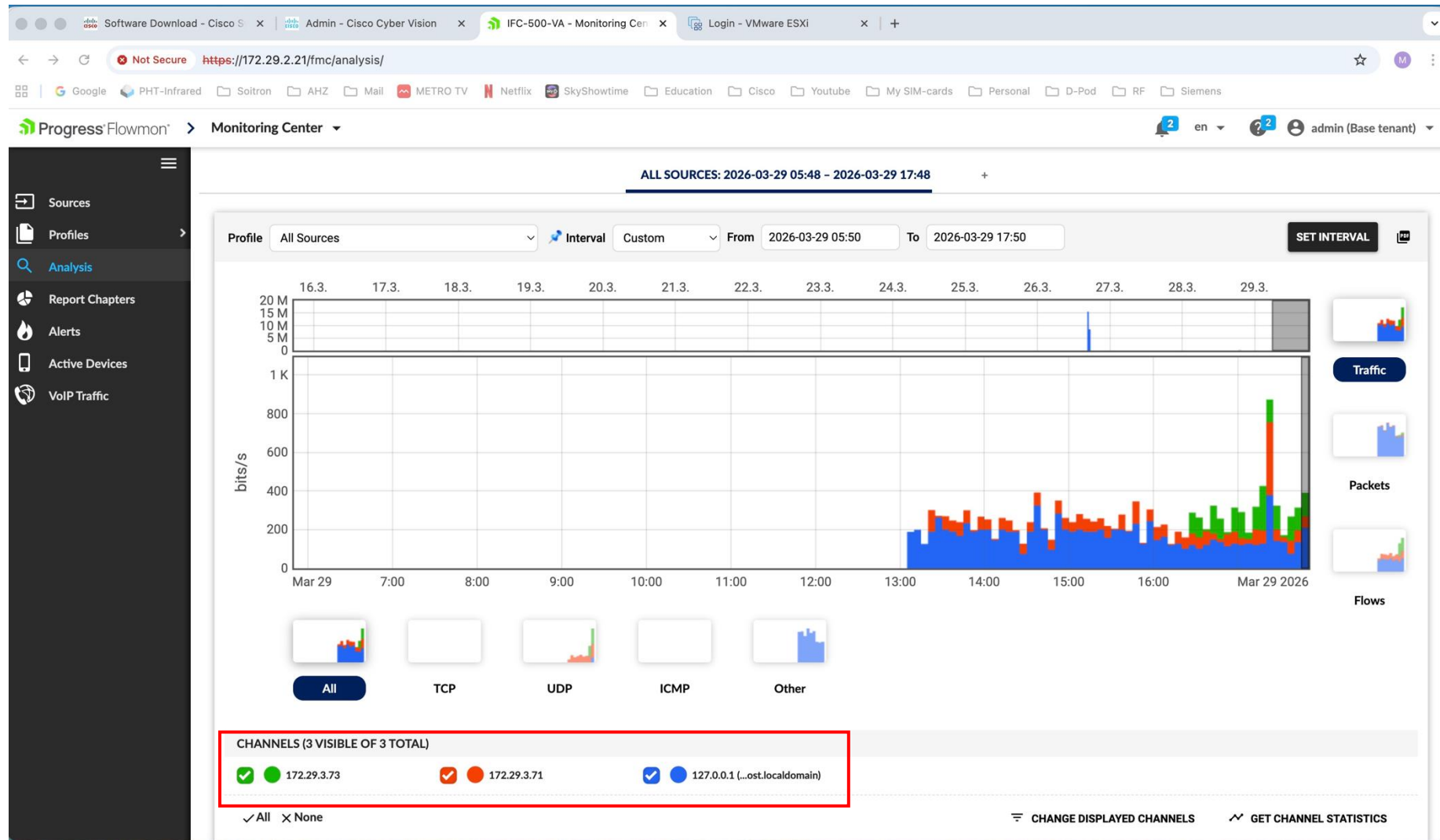
- Hosts with Top Data Transfers:** A table listing hosts and their data transfer volume in bytes.
- Hosts with Top Flows:** A table listing hosts and their number of flows.

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

The screenshot displays the Cisco IOx Local Manager web interface. The top navigation bar includes the Cisco logo, the device name "Cisco IE-3500-8U3X" with version "17.18.2", and a "Welcome admin" message with navigation icons. A left sidebar contains menu items: Dashboard, Monitoring, Configuration (highlighted), Administration, Licensing, and Troubleshooting. The main content area shows the breadcrumb "Configuration > Services > IOx" and a sub-header "Cisco Systems Cisco IOx Local Manager". Below this is a navigation menu with "Applications", "Container Layers", "System Info", "System Setting", and "System Troubleshoot". The "Applications" tab is active, showing two running containers: "NFSensor" and "CCVSENSOR".

Container Name	Description	Status	Type	Version	Profile	Memory *	CPU *	Actions
NFSensor	"NetFlow Monitoring Container"	RUNNING	docker	"1.1"	custom	30.5%	30.0%	Stop, Manage
CCVSENSOR	Cisco Cyber Vision sensor with Active Discovery for aar...	RUNNING	docker	5.4.1-202603171640	custom	30.5%	70.0%	Stop, Manage

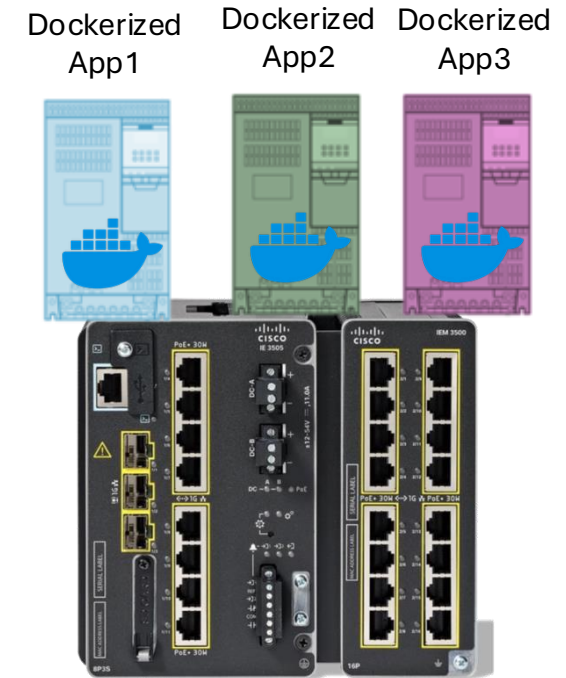
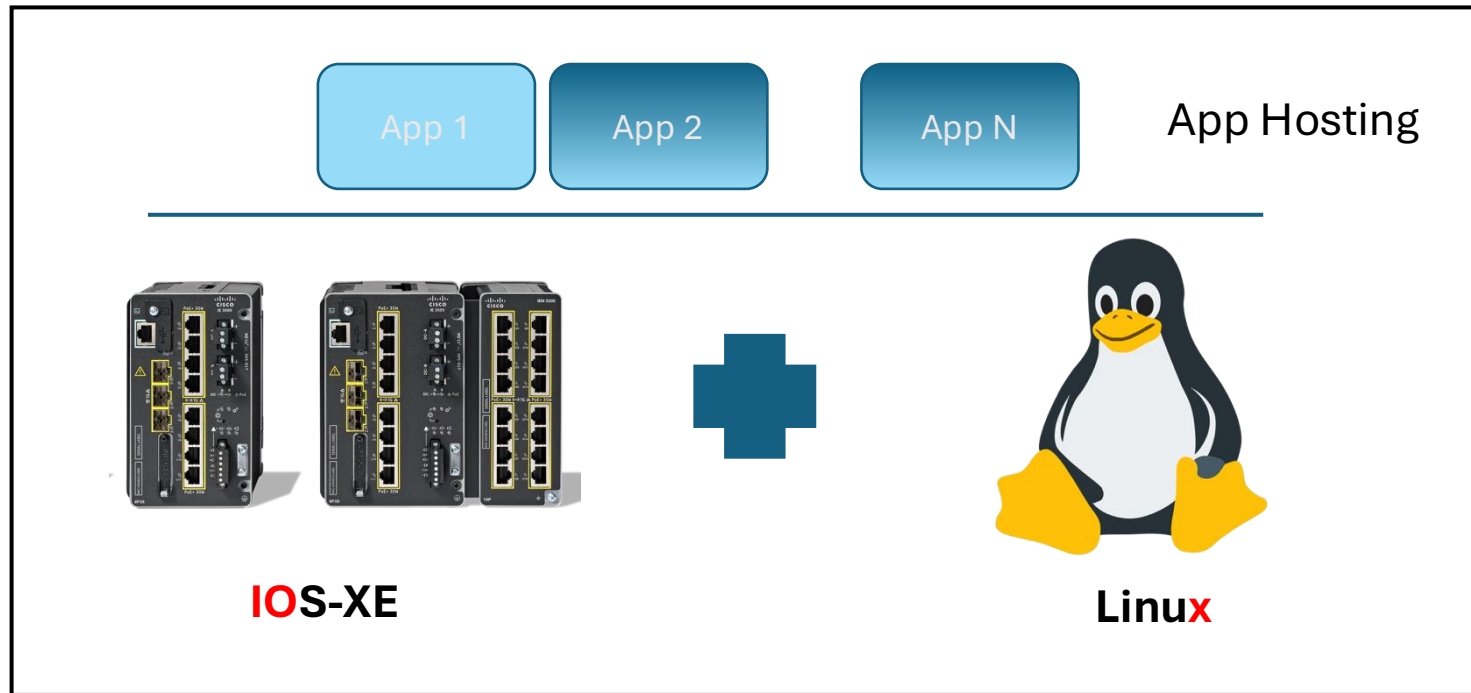
On the right side of the application list, there is a dashed box containing "Add New" and "Refresh" buttons.



# App Responsiveness Measurement - SLAMonitor App

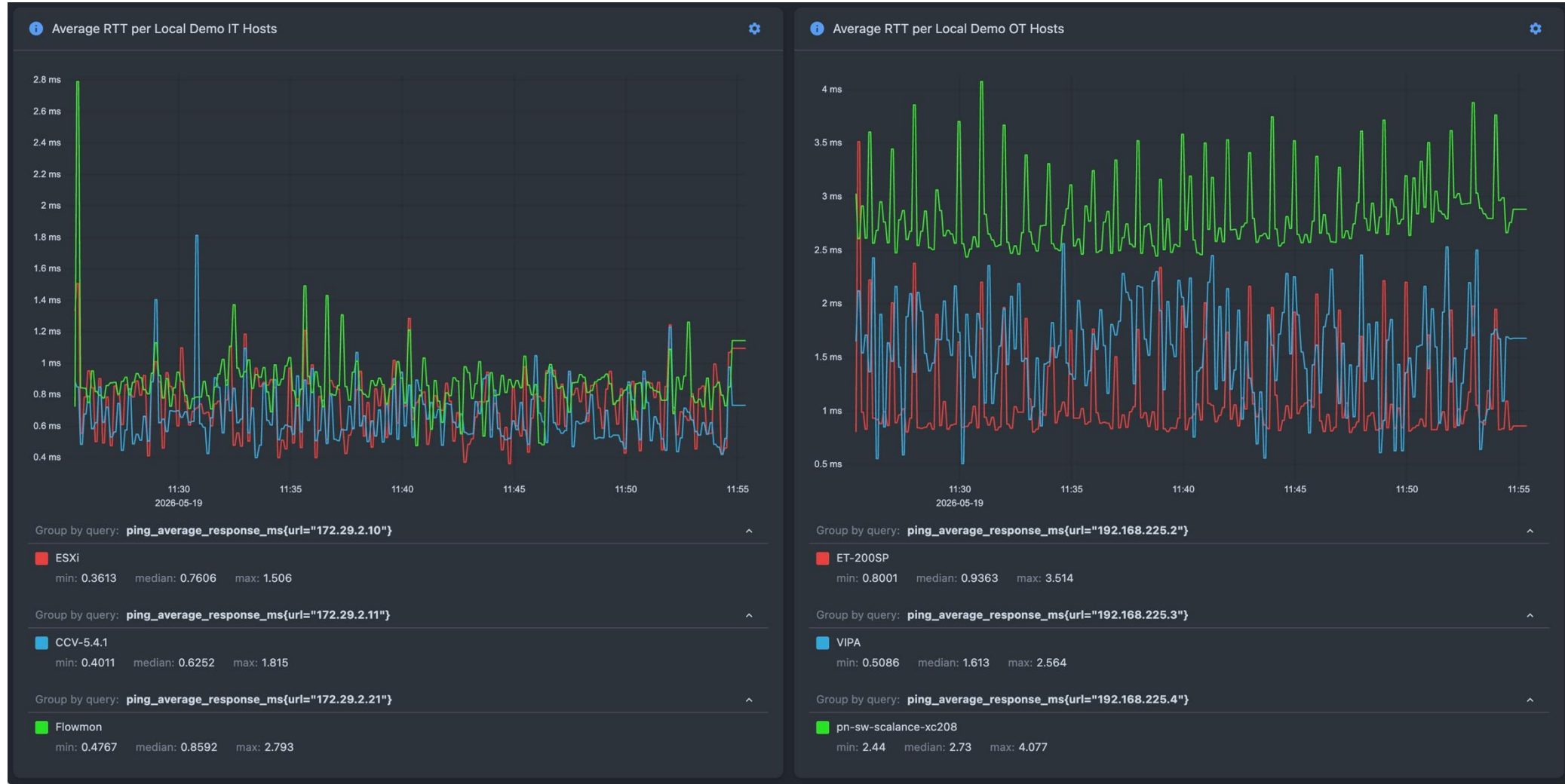
Embedded App for SLA App/Servers Monitoring

# Cisco IOX Concept for Critical Apps Operation Diagnostics and Monitoring

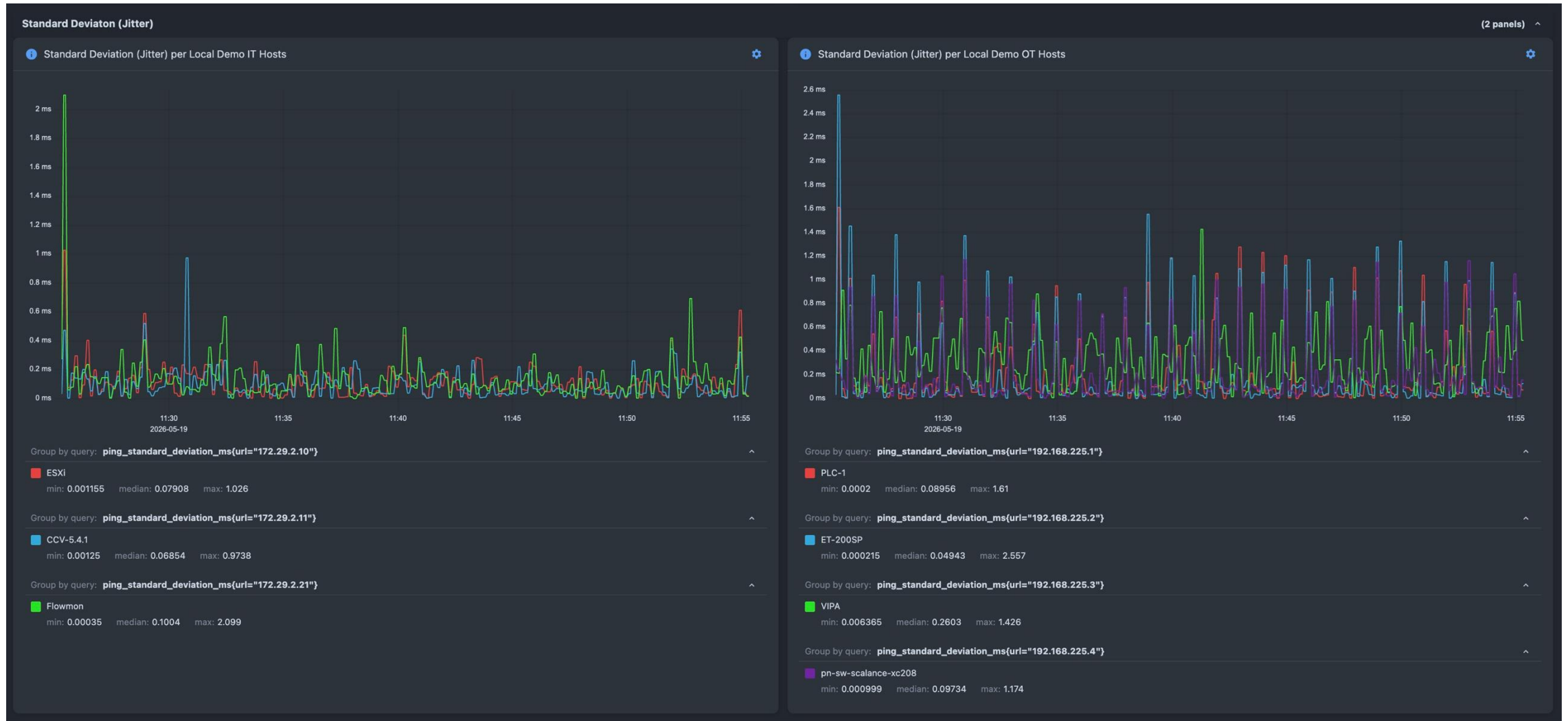


- IE3x00 with Dockerized App
- **Round-trip-Time Measurement** and Visualization App of IT and OT part of the Deployed Remote App Solution

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



# SLAMonitor App – Jitter Per IT/OT Groups



# SLAMonitor App on IE3400 – App Resources

← Cisco 17.12.7a Cisco IE-3400-8T2S Welcome admin | Home | Save | Settings | Help | Refresh | Share

Configuration > Services > IOx Hello, admin | Log Out | About

**Cisco Systems**  
Cisco IOx Local Manager

Applications | Docker Layers | System Info | System Setting | System Troubleshoot

**SLAMonitor** RUNNING

"SLA Monitoring Container"

TYPE	VERSION	PROFILE
docker	"1.0.1"	custom

**Memory \*** 100.0%

**CPU \*** 100.0%

■ Stop    ⚙ Manage

➕ Add New    ↻ Refresh



# 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

The screenshot displays the Cisco IOx Local Manager web interface for a Cisco IE-3400-8T2S switch. The interface is divided into a left sidebar with navigation options (Dashboard, Monitoring, Configuration, Administration, Licensing, Troubleshooting) and a main content area. The main content area shows the 'Applications' tab, which lists two running containers: SLAMonitor and NFSensor. Each container card displays its name, description, type, version, profile, and resource usage (Memory and CPU) with progress bars. Below each card are 'Stop' and 'Manage' buttons. A right-hand panel contains 'Add New' and 'Refresh' buttons.

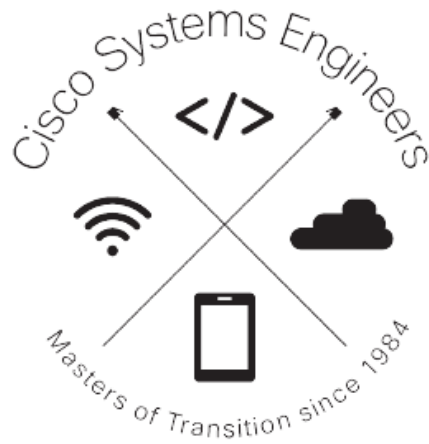
Navigation: Configuration > Services > IOx

Header: Cisco Systems, Cisco IOx Local Manager

Sub-headers: Applications, Docker Layers, System Info, System Setting, System Troubleshoot

Application	Type	Version	Profile	Memory *	CPU *
SLAMonitor "SLA Monitoring Container"	docker	"1.0.1"	custom	48.1%	71.4%
NFSensor "NetFlow Monitoring Container"	docker	"1.1"	custom	48.1%	28.6%





**SOITRON**<sup>⚙️</sup>  
industry

**CONTROL**  
SYSTEM