



# Cisco Tech Club Days



## Novinky IoT portfolia v roce 2021

Industrial Gateways, Routing a Cyber Vision 4.0

Jiří Rott

[jirott@cisco.com](mailto:jirott@cisco.com)

14.12.2021

# Agenda

- 1 Portfolio Overview
- 2 IoT Gateway Overview
- 3 IoT Routers IR1101, IR1800, IR8100, IR8300
- 4 IoT OD cloud management (OT)
- 5 Cyber vision 4.0 - update

# Portfolio Overview



# Comprehensive IoT Portfolio

## Industrial Switching

1K, 2K, 3200, 3300, 3400, 3400H, 4K, 5K, CGS



## Industrial Routing

IR8XX, IR1101, CGR1120, CGR1240, CGR2010



## Embedded IoT

ESS, ESR, ESW, Resilient Mesh



## Industrial Wireless

Cisco Ultra Reliable Wireless Backhaul, IW6300, IW3702, IR5XX, IXM Gateway



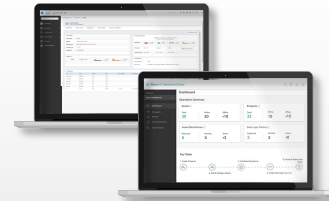
## Industrial Security

ISA 3000, Cyber Vision



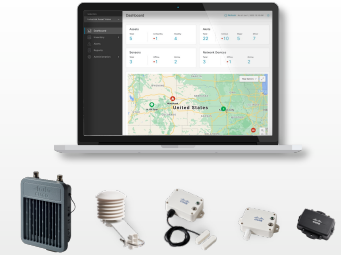
## Edge Intelligence

IOx



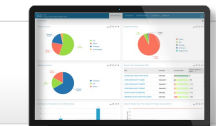
## Full-stack as a Service

Industrial Asset Vision



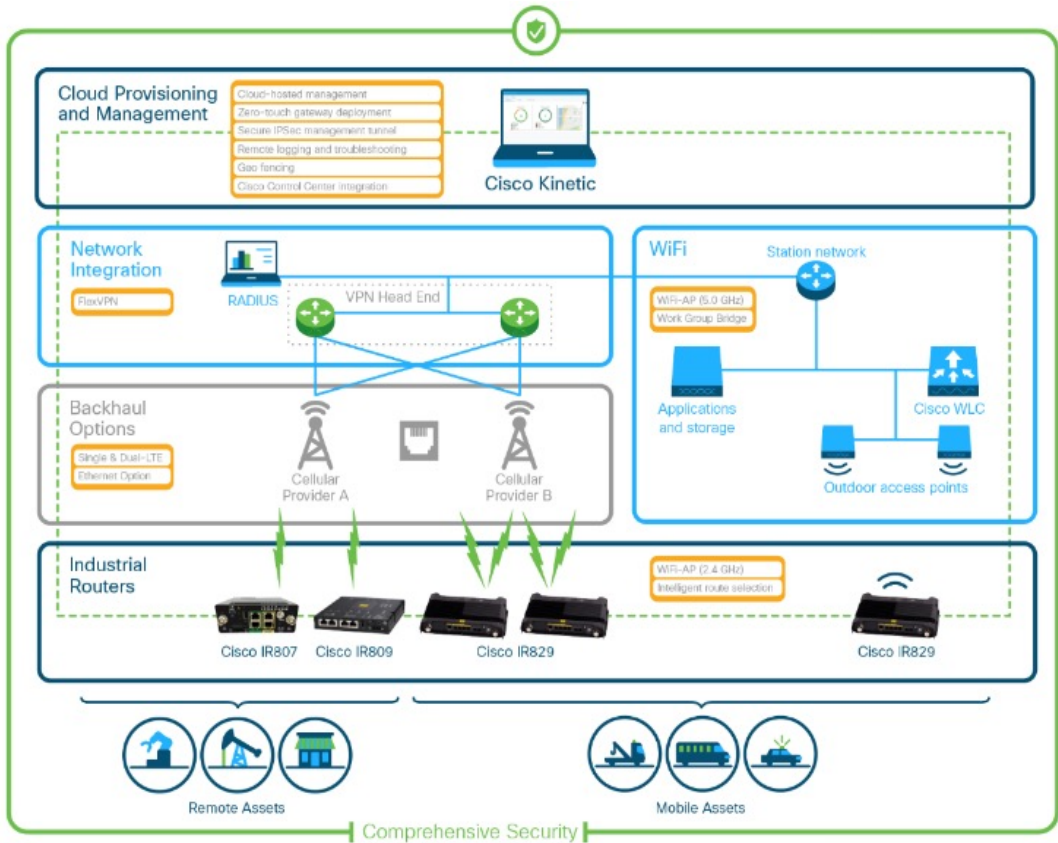
## Management & Automation

Field Network Director, Industrial Network Director, IoT Operations Dashboard



# Cisco Remote and Mobile Assets

RAMA



## Use Case

- Service Fleet
- Buses & Taxis
- Public Safety
- Outdoor Equipment, Remote Sites
- Connected Machines



## Outcomes

- Lower deployment, operating expense
- New business models / new services
- Reduce security threats



## New Features

### Scalability:

- IOX initial partner integration testing

### Simplicity:

- Head end scalability
- High availability
- Automated off/on-line config



# A complete routing portfolio

## Secured and optimized for *every* use case



### Demanding, mission critical deployments

Fleet, first-responders, pipelines



5G

Catalyst  
IR1800

- Wi-Fi 6, LTE/5G
- Gigabit Ethernet & POE
- Automotive Dead Reckoning GNSS
- CAN-Bus
- Transportation certified

Remote monitoring,  
streetlights, intersections



5G

Catalyst  
IR8100

- IP67 rated
- Battery backup
- Ethernet & PoE or PoE+\*
- Modular power supply unit and CPU
- Utility certified

ATMs, low voltage substations,  
roadside equipment



5G

Catalyst  
IR1100

- Compact, for space constrained deployment
- Low power
- LTE/5G/DSL, Ethernet
- Utility certified

Factory, high voltage substations



5G

Catalyst  
IR8300

- Routing & Switching Includes advanced switching powered by Cisco silicon
- U-PoE up to 60 watts
- Precision timing source
- Utility certified

### High volume Simple m2m deployments

Kiosks, vending machines,  
coffee machines

IG21R, IG31R



IG20

Cisco IoT Gateway (IG)

- Cloud-first, cost-effective
- Deployment with no staging required
- Indoor & ruggedized versions

\*roadmap item

# IoT Gateway Overview

# Positioning IoT Gateway

Enterprise Security + Edge Compute + Detailed Configuration



Cisco Industrial IoT Routers

- Advanced IPv4/IPv6 Routing
- 5GLTE, High Bandwidth, Band14, Public & Private LTE
- GE PoE/Wi-Fi6
- Enterprise Security
- SDWAN
- Full Cisco IOS-XE Stack
- Redundancy
- Compute/Storage
- Industrial Temp. grade
- On-prem & Cloud Managed

Simple Secure Connectivity



Cisco IoT Gateways

- ✓ Static IPv4 Routing
- ✓ Simple Connectivity
- ✓ End-to-End Security
- ✓ Cloud Managed
- ✓ Cloud OS
- ✓ Low LTE Bandwidth
- ✗ Compute/Storage
- ✗ Redundancy



# Monitor assets remotely to gain operational insights



## Retail kiosks



**Connect indoor assets**



## Charging stations



**Suitable for outdoor use**

**Ruggedized models**







## Machinery



**Suitable for industrial use**

**Ruggedized models**

# Cisco IoT Gateways Hardware Specifications

				
Region	IoT gateway LTE	IoT gateway LTE + Wi-Fi	IoT rugged gateway LTE	IoT rugged gateway LTE + Wi-Fi
Europe	IG21-EU-K9	IG21-EU-E-K9	IG21R-EU-K9	IG31R-EU-E-K9
Technical specifications				
LTE	CAT1	CAT1	CAT4	CAT4
2 GE LAN/WAN ports	✓	✓	✓	✓
Serial RS-232*	✓	✓	✓	RS-232+485
Internal antennas	✓	✓	External	External
USB	-	✓	✓	✓
Wi-Fi	-	✓	-	✓
IP30 rating	-	-	✓	✓
2 GPIO/1 alarm*	-	-	1 alarm	2 GPIO
Operating temperature	0°C to 40°C	0°C to 40°C	-20°C to 60°C	-20°C to 60°C
Dimensions	160 x 138.5 x 42.6mm	160 x 138.5 x 42.6mm	203.2 x 144.7 x 35.1 mm	203.2 x 144.7 x 35.1 mm
Mounting options	DIN rail, floor, panel, wall	DIN rail, floor, panel, wall	DIN rail, bracket	DIN rail, bracket
Weight	495 grams	506 grams	785 grams	797 grams

\* Post FCS: Enabled by software upgrade

# Cloud Managed: High Level Features

Automated  
SIM  
Provisioning\*

Ethernet,  
& Wi-Fi

IPsec VPN

DHCP / DNS  
/ NAT

MAC  
Filtering

Logging &  
Troubleshooting

IG21



IG21R, IG31R



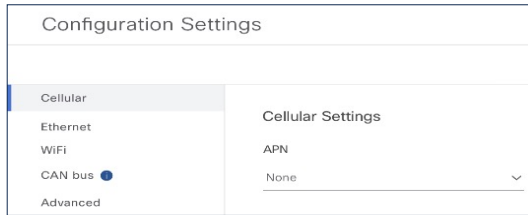
\* For Supported Carriers with Control Center Secure Device Onboarding

Cloud Native Operating system managed with IoT Operations Dashboard

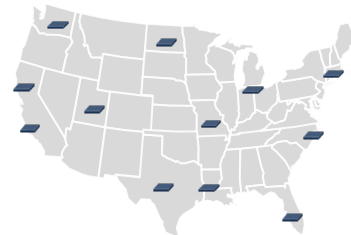
# Fast and simple day-0 setup

No Staging! No manual SIM activation! Yes, it's THAT easy!

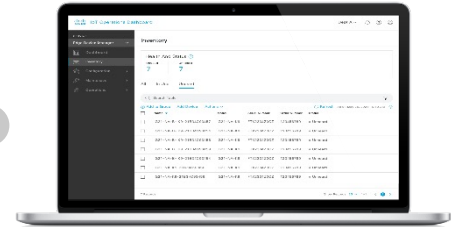
## Gateway Provisioning



Create Configuration on IoT Operations Dashboard



Order and Ship gateway **directly** to install site



Assign Configuration on IoT Operations Dashboard

## Installation Process



Field personnel



Mount the gateway

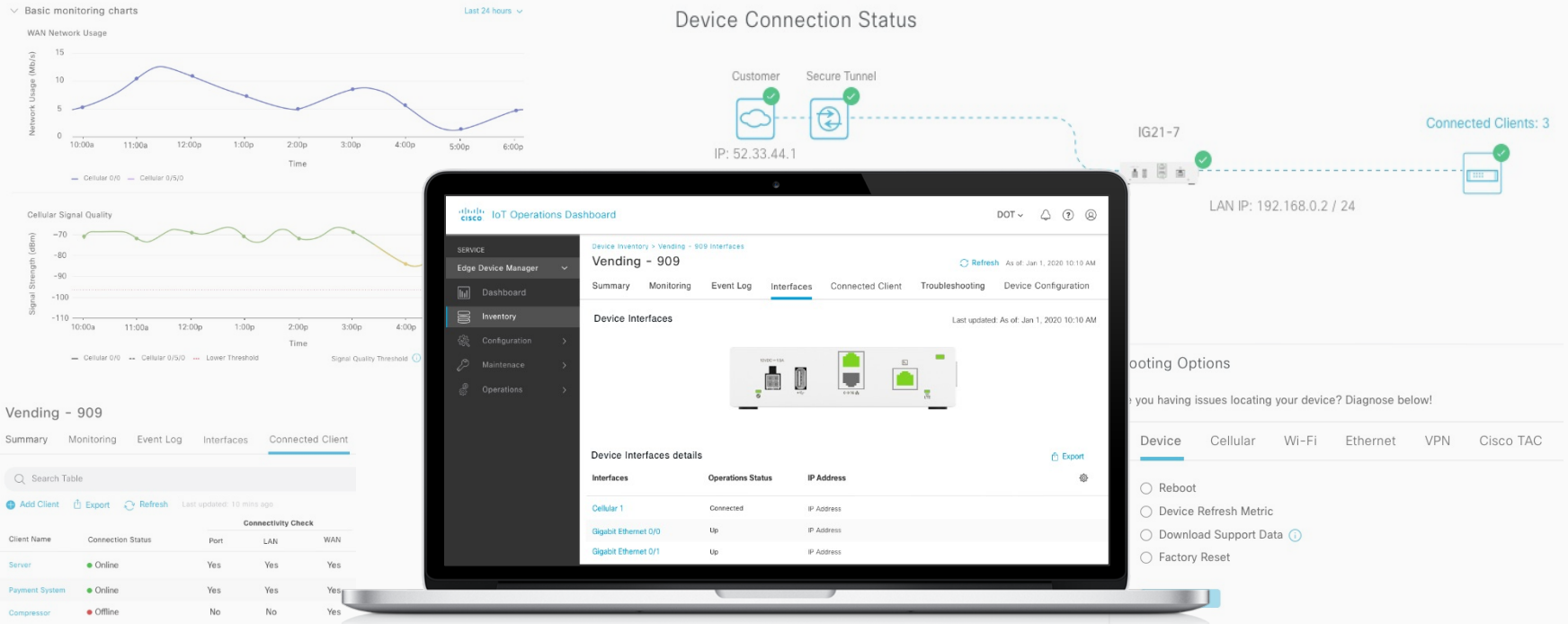


Power ON – Wait for the green light!



Cisco AR Viewer Mobile App

# Remote monitoring of gateways and clients

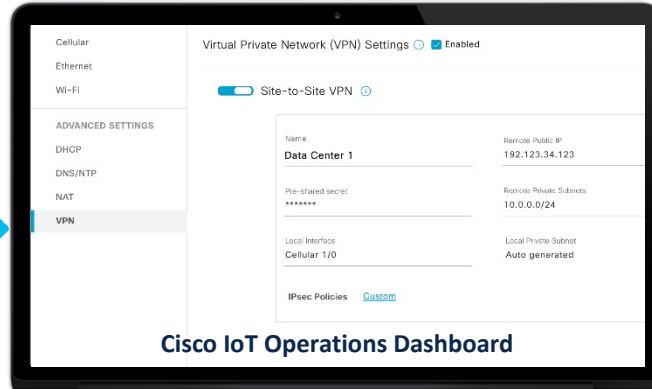


# Securely connect assets

## Asset

Cisco IG21

Cisco



Cisco IoT Operations Dashboard

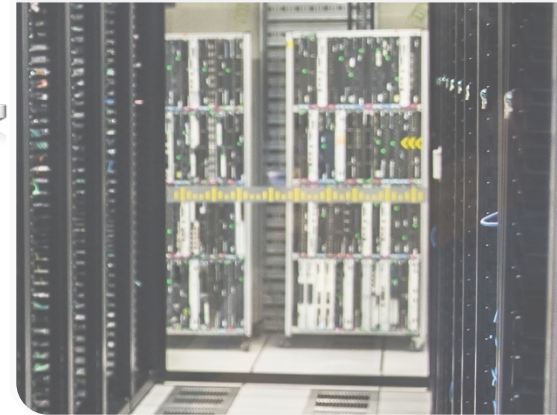
## IPsec tunnel



End-to-end security with Advanced Encryption Standard (AES) encrypted IPsec tunnel

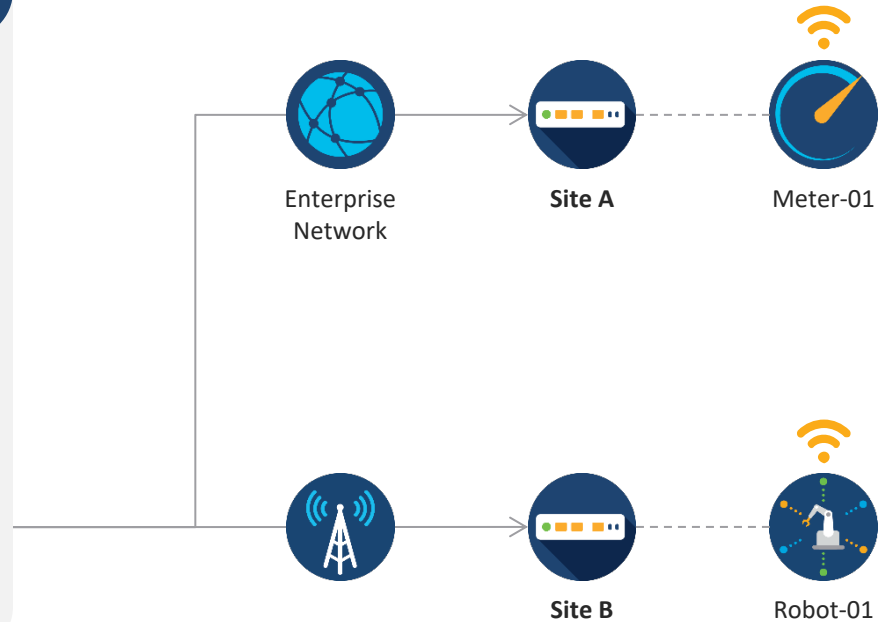
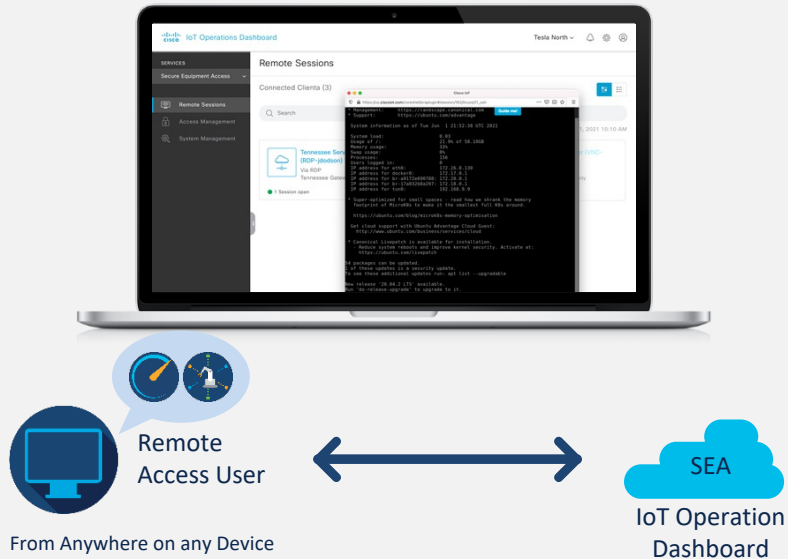
## Data center

Cisco ASR1K / CSR / Catalyst  
8000 Edge



# Troubleshoot Connected Assets with Secure Equipment Access (SEA)

## SEA on IoT Operations Dashboard



IR 1101



# IR1101 - The Next Generation Industrial ISR

First IoT Router with IOS XE  
High-end security Programmability



Top/Bottom Modules  
for additional interfaces



Edge computing enabled  
100G SATA



IOS-XE unified image 17.2.1r  
Classic IOS and SDWAN



Investment protection



Lower TCO



Modular LTE (public/private) & 5G  
Ready\*



Low average Power  
consumption of only 10W



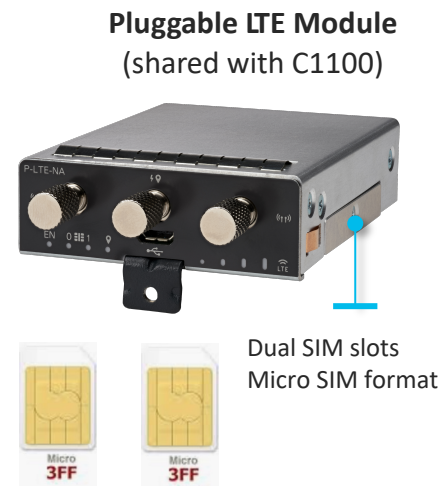
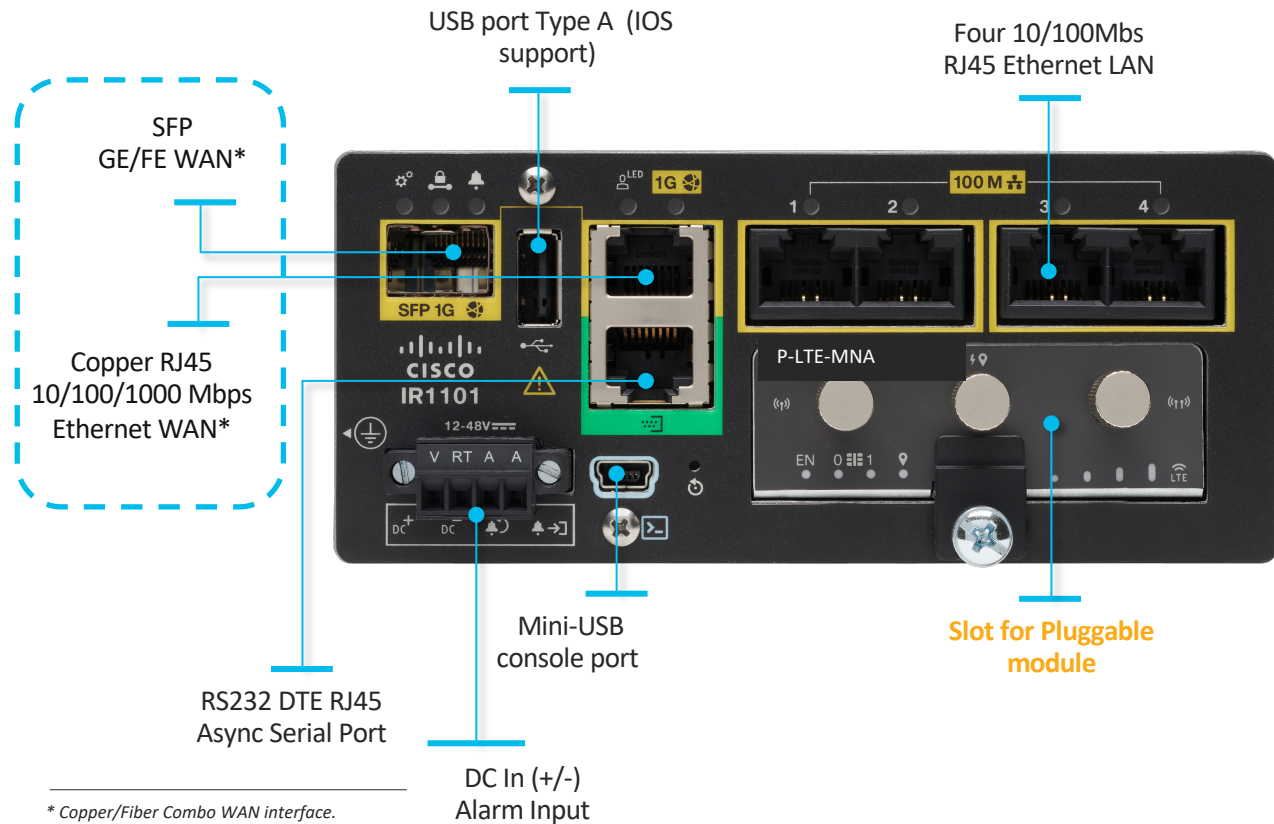
Compact form factor for  
Din-rail installations



Extended product life time



# IR1101 – Base Platform - Compact and Flexible



\* Copper/Fiber Combo WAN interface.

# IRM-1100-4A2T

## IR1101 Serial and Ethernet Expansion Module

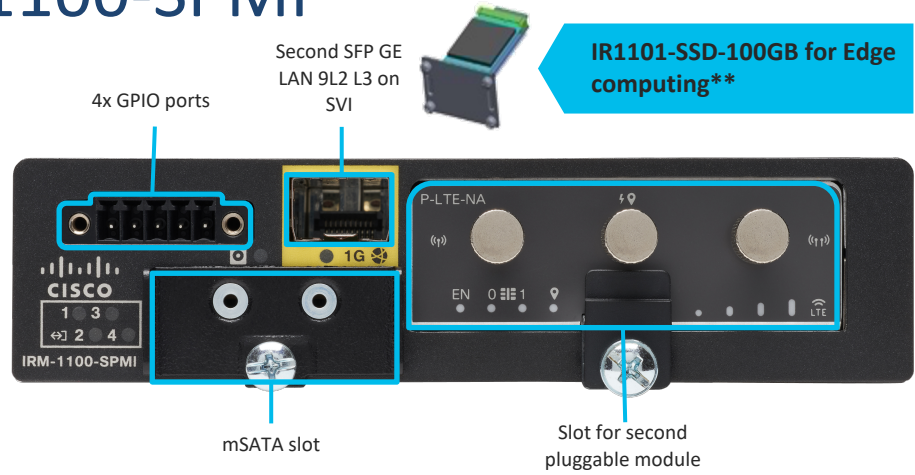
New  
17.7.1  
IOS-XE



Expansion Module	Description
IRM-1100-4A2T	<ul style="list-style-type: none"><li>• 2 x GE RJ45 Layer-2 LAN (Layer-3 done through SVI)</li><li>• 4 x Asynchronous Serial Ports (RS232/RS485/RS422)(DCE)</li></ul>

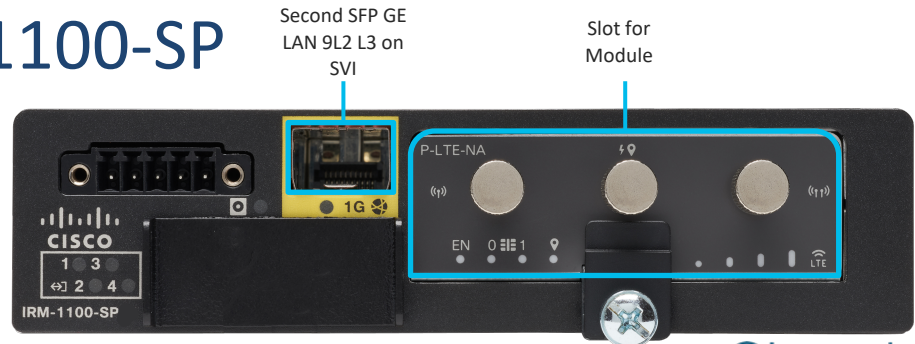
# Expansion module: IRM-1100-SPMI

Expansion Module	Description
IRM-110-SPMI	<ul style="list-style-type: none"> <li>• 4x GPIO ports</li> <li>• SFP GE LAN (L2)</li> <li>• Slot for pluggable module</li> </ul>



# Expansion module: IRM-1100-SP

Expansion Module	Description
IRM-110-SP	<ul style="list-style-type: none"> <li>• SFP GE LAN (L2)</li> <li>• Slot for pluggable module</li> </ul>



# Configurations to be supported by IR1101

## Deployment Scenarios with Serial/Ethernet Expansion Module

### Config 1

IR1101  
Serial Expansion Module



### Config 2

IR1101  
LTE Expansion Module  
Serial Expansion Module



Ethernet Ports on the expansion module will **not** be operational

### Config 3

IR1101  
Serial Expansion Module  
LTE Expansion Module (bottom)



SFP and SATA on the expansion module will **not** be operational

### Config 4

IR1101  
2x Serial Expansion



Ethernet Ports on the expansion module in the bottom will **not** be operational

Ethernet Ports on Expansion Module total throughput limited to 1Gbps

New  
17.4.1

# DSL SFP for IR1101



SFP-VADSL2+-I



Industry-grade  
ADSL2, ADSL2+, VDSL2



-40 to 60° C



EMI Certifications

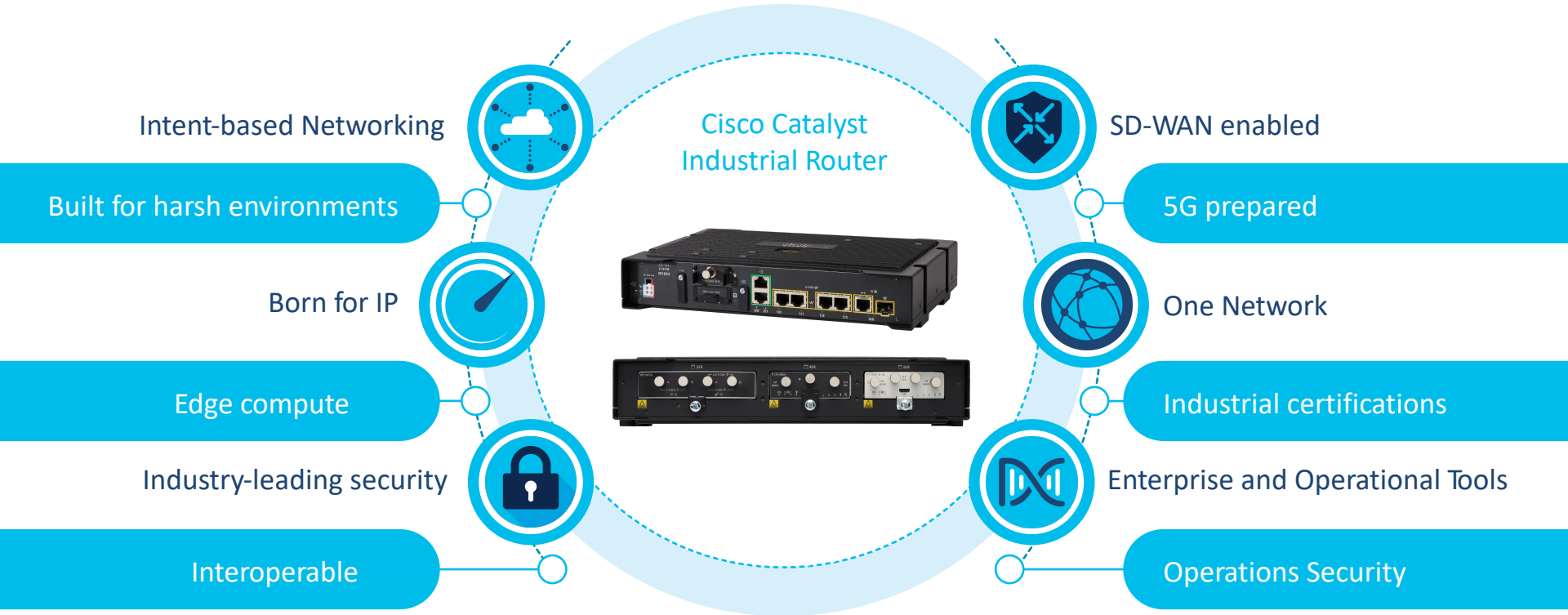


DSL management integrated  
into Cisco IOS-XE CLI

SFP form factor provide additional  
protection investment and flexibility

IR 1800

# Catalyst IR1800 Industrial Router





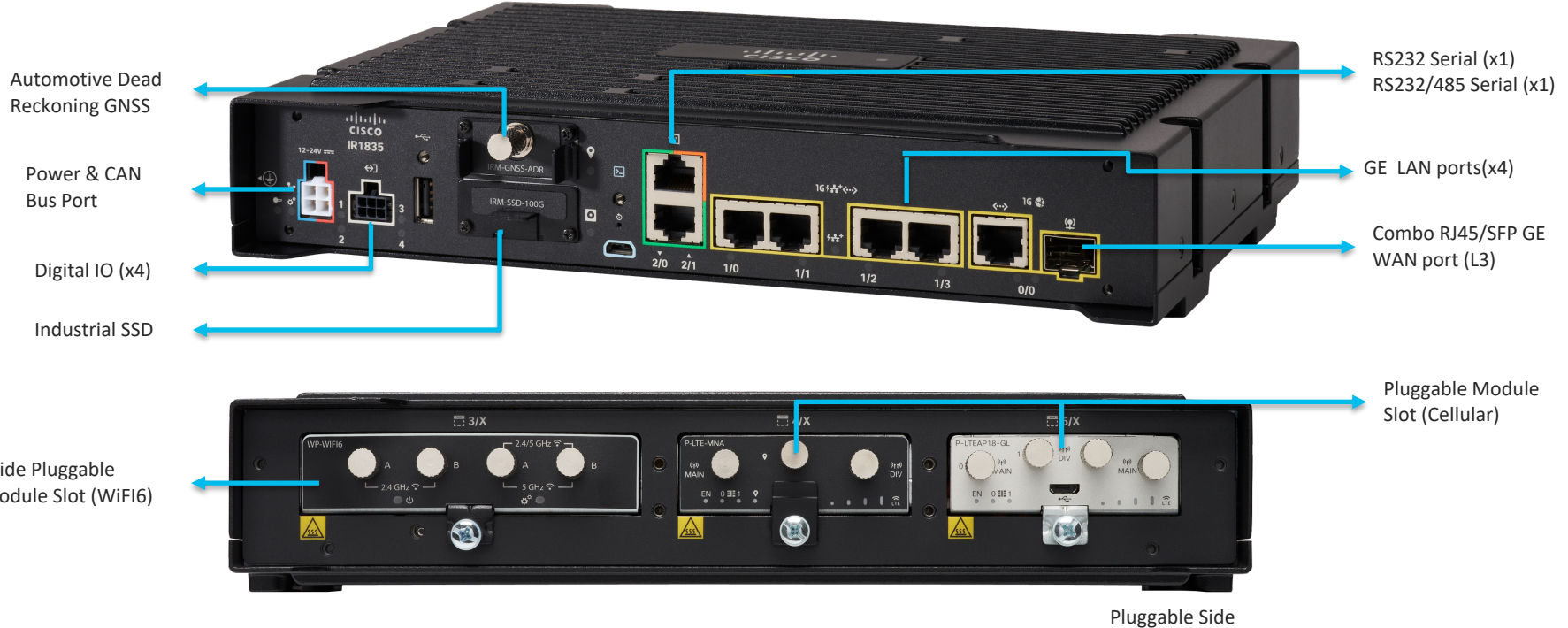
# IR1800 Series Routers



Features	IR1821-K9	IR1831-K9	IR1833-K9	IR1835-K9
Processor	600 MHz	600 MHz	600 MHz	1200MHz
Memory	4GB	4GB	4GB	8GB
LTE Slot	one	two	two	two
Wi-Fi Module	✓	✓	✓	✓
CAN Bus	✓	✓	✓	✓
PoE	✗	✗	✓	✓
mSATA Module	✗	✗	✓	✓
Automotive Dead Reckoning GNSS (Module)	✗	✗	✓	✓
GPIO	✗	✗	✗	✓
Serial Interface	RS232 (1)	RS232 (2)	RS232 (2)	RS232, RS232/485

# Catalyst IR1835-K9

Available in US, Canada,  
and Europe



# P-WIFI-AX-

802.11ax module for IR1800  
Autonomous and Controller mode



Pluggable 802.11ax module  
for IR1800 series



Supports WGB Mode  
(IOS-XE 17.6.1)



EWC Controller Support



Extended Temperature Range



Parity with WNBU's AP 9115

# WiFi6 Deployment Scenarios

## Controller Mode

Extended Enterprise Stationary &  
Mobile Use Cases

Access Point



Controller  
Cisco Catalyst 9800



## EWC Mode

Mass Transit/Transportation Remote  
& Mobile Assets

Access Point + Controller



## WGB Mode

Data Offloading Over Infrastructure  
WiFi

Access Point



Cisco AP



# Software Features

# IR1800 Software Features / Benefits & Licenses

IPv4/IPv6

QoS

Security

Routing

Single/Dual 4G  
or 5G

Wi-fi6

IRM-ADR-GNSS

Manageability

Licenses

**Network Advantage:** MPLS, Mobile IP, BFD, RSVP, TCP optimization, WANMOM, App-aware QoS policies and troubleshooting

**Network Essentials:** Traffic segmentation (VPN, VRF, VLAN), Crypto Tunnels, IPSec, IKEv2, ssl-vpn, DHCP, QoS, ACL, EIGRP, IGMP, HTTP, IP Multicast, Radius, TACACS, OSPF, RIP, HSRP

Foundation Services

## High-end Security



- Security Enhanced Linux (SELinux)
- Next-gen encryption
- Quantum computer resistant crypto algorithm
- Hardware Crypto-acceleration
- Cisco Trust Anchor
- Firewall, Umbrella
- Cybervision

## Edge Computing



- IOx developer tools
- On-prem or cloud managed
- Trusted apps with App signing
- App lifecycle mgmt.

## Automation



- Plug and Play
- NETCONF
- RESTCONF
- IETF YANG
- Telemetry
- GNSS (Geo-fencing on management tool)

## Resilient



- Patching for graceful insertion/removal
- Easy maintenance
- Continuous operation

IR 8100

# IR8140H - The Next Generation Industrial Router

The only IoT Heavy Duty Outdoor Router

IoT Router with IOS XE High-end security  
Programmability



Modular LTE (public/private) & 5G  
Ready\*



Edge computing



Modular Battery backup and Power  
Supply



Cisco IOS-XE unified image  
Autonomous IOS and SDWAN



Modular CPU and LTE  
Interfaces



*\*with future 5G module*



Lower TCO



Multi-service/Multi-Access

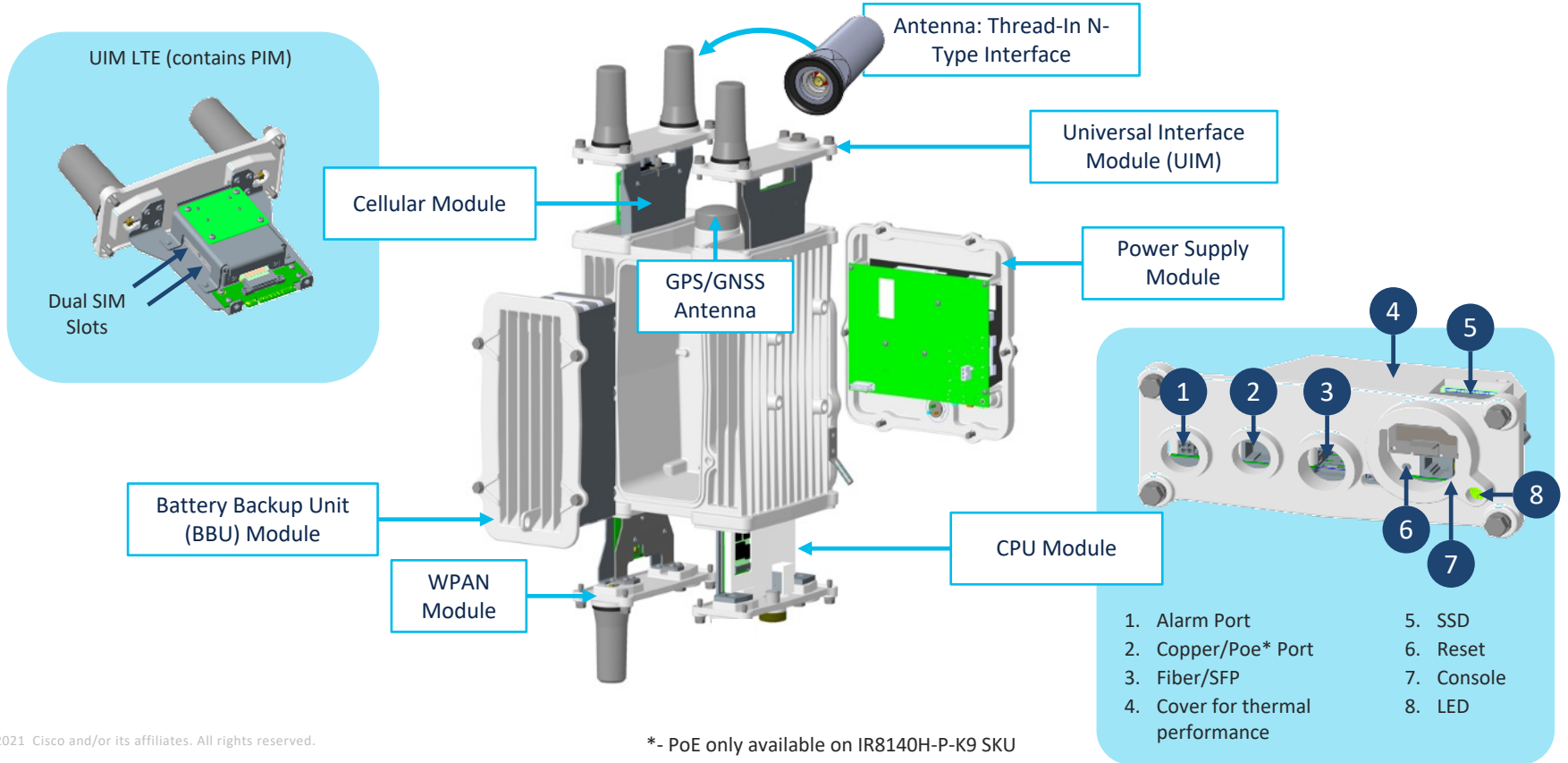


Extended product life-time





# IR8140H –Platform dissected

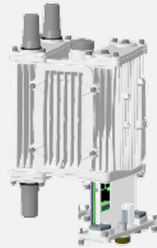


# IR8140H Multiple Backhaul Options

GE Copper



Fiber SFP



Single LTE



Dual LTE



External 12V  
DC/PoE



# Connected cities and lighting

## Making the light pole smarter

### Challenges

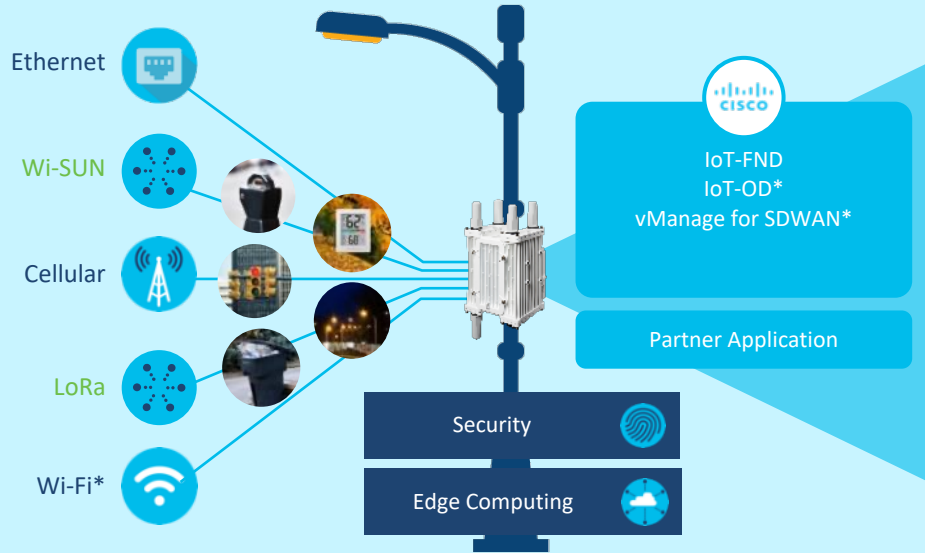
- Legacy lighting infrastructure disconnected
- No Realtime information on City infrastructure
- High maintenance and repair cost
- Multiple solutions to solve a single problem

### Cisco Solution

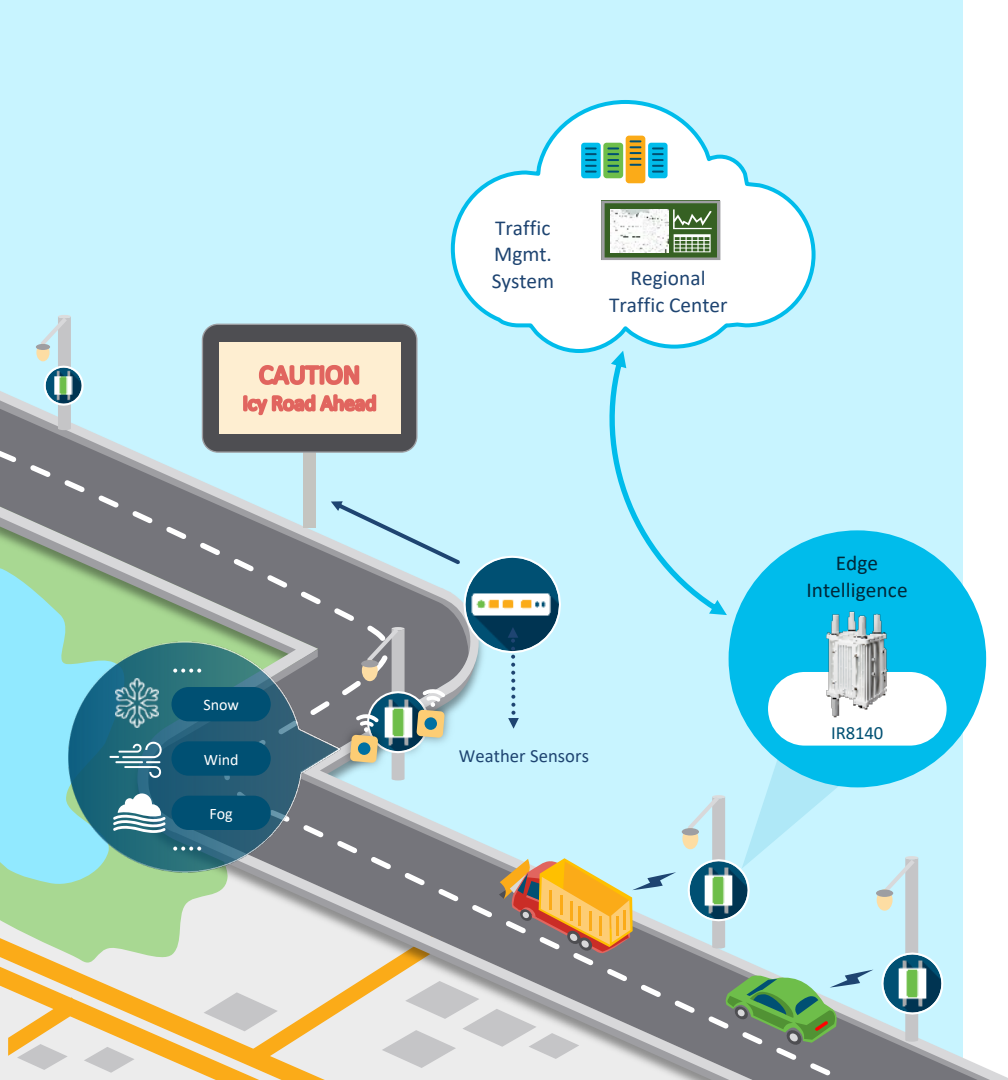
- Wi-SUN / Cisco resilient mesh networked solutions provide connectivity and visibility
- LoRa module on IR8140 aggregates data from LoRa Sensors
- Converged multi-access connectivity provides real-time data on the connected asset

### Outcomes

- Optimized operations based on alerts and metrics
- Faster response to failures for better safety and efficiency



\*Future roadmap



# Connected transportation

Making the road smarter

## Challenges

- Legacy roadway devices without reliable connectivity
- Slow response to changing road conditions
- New connected vehicles sending overwhelming volumes of data
- Outdoor connectivity in harsh environments

## Cisco Solution

- Edge intelligence on Cisco IoT GWs to provide real-time visibility, custom applications and policy actions
- Secure roadside connectivity with Cisco IoT routers - Ruggedized IP67 platform

## Outcomes

- Vehicles become sensors covering the roadway
- Optimized maintenance operations in varying conditions
- Faster response to road conditions for better safety and efficiency through connected applications

IR 8300

# IR8340 in a Nutshell



Enhanced Security Features



Integrated Switching/Routing,  
Modular Interface Modules



PTP, GNSS, IRIG-B



PoE, AC/DC – High and Low



Investment Protection



Ease of deployment



Multi Service



Integration with  
DNA-C, vManage



SD-WAN Ready  
Edge-computing Enabled



Powered by Cisco IOS XE

# IR8340 Backhaul Options

Dual Copper



Dual Fiber SFP



Single LTE



Dual LTE



- A. Dual Active: Bandwidth aggregation
- B. Fallback: Redundancy

# Catalyst IR8340

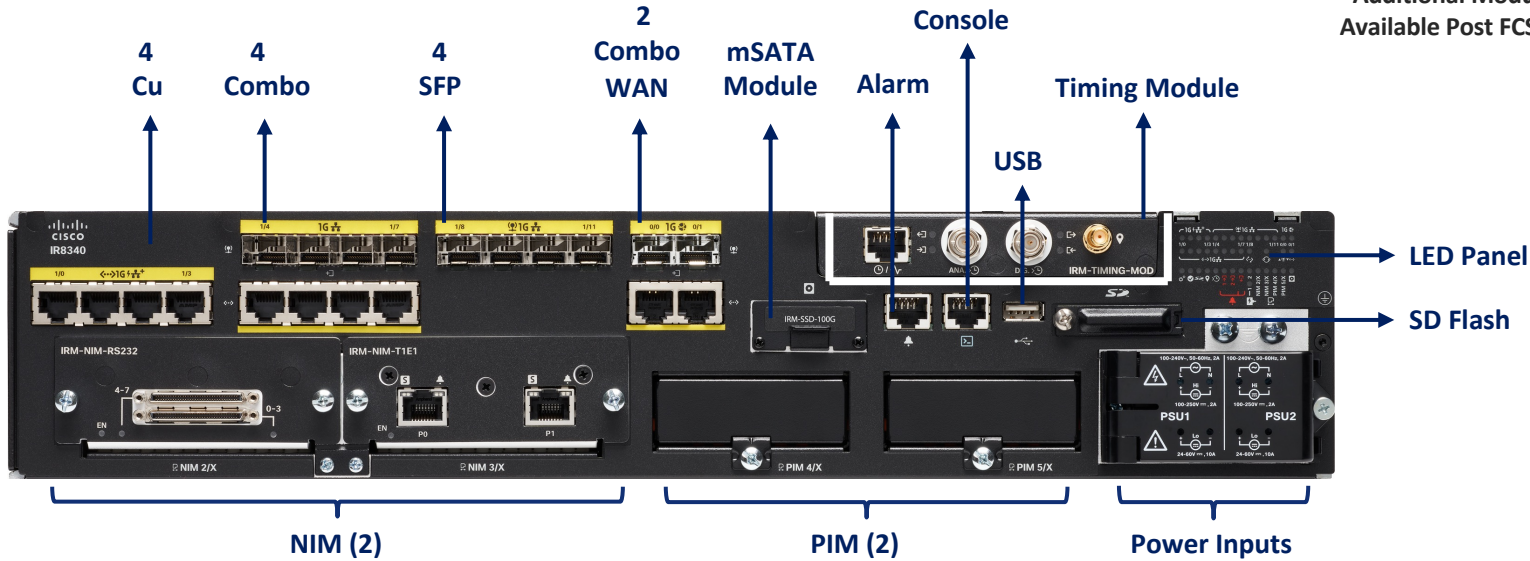


- Operating Temperature Range  $-40^{\circ}$  C to  $+60^{\circ}$  C
- Industrial Grade platform, **IOS-XE software**
  - Single Integrated SW image (*Switching + Routing*)
- 2RU, ~2Gbps throughput with services ON
- IPSEC 1Gbps throughput Aggregate
- 14 GE ports ( 12 – LAN, 2 - WAN),
  - LAN : 4 Cu, 4 Combo, 4 SFP
  - UPOE/POE/POE+ : 60W budget
  - WAN : 2 Combo ports
- Multiple WAN interfaces
  - Dual active 4G-LTE, T1/E1, xDSL (Post FCS)
- Legacy Interface Support
  - T1/E1, Serial : RS232, (RS422, RS485 Post FCS)
- Dual PSU's – AC and DC
  - High/Low Voltage
- **Enhanced Security – IPS/IDS (IOS-XE Applications)**
- **Edge Computing – Cisco IOS-XE Application**
- **SD-WAN support**
- **Timing : IRIG-B in/out, GNSS Receiver, 1588v2**
- **Support for DNA-C, vManage**
- **Adjustable CPU Core Performance Profiles (Post FCS)**



# IR 8340 Chassis – Front View

<u>NIM</u>	<u>PIM</u>
T1/E1 Serial	4G LTE
*Additional Modules Available Post FCS	



NIM – Network Interface Module, PIM – Pluggable Interface Module

\* - Post FCS

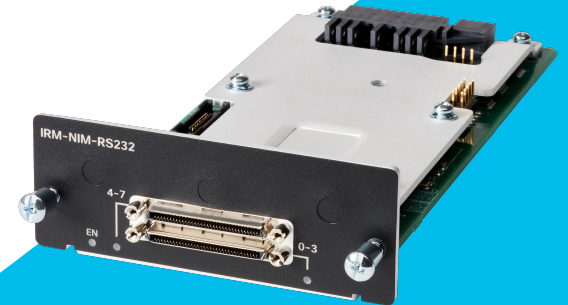
# IR8340 T1/E1 Module

- Operating Temperature Range  $-40^{\circ}\text{C}$  to  $+60^{\circ}\text{C}$
- One and two port SKU's available
- Data only, no voice support
- HDLC, PTP, Frame Relay
- Single wide NIM module



# IR8340 Serial Module

- Operating Temperature Range  $-40^{\circ}\text{C}$  to  $+60^{\circ}\text{C}$
- RS232 support only at FCS
- 256kbps (Synchronous max), 230kbps (Asynchronous max)
- 8 serial interfaces per module
- PPP, HDLS, Bisync support
- Single wide NIM module



# IR8340 Timing Module

- GPS – Input, SMA
  - External Antenna required
  - G.8272 PRTC-A Accuracy within 100ns
- IRIG-B – Input/Output
  - Analog 122/123
  - Digital 002/003
  - IRIG-B to PTP conversion support
- Cisco TOD – RJ45
- SyncE, PTP timing support
- Stratum 1 traceable clock

## Device Types – PTP 1588 v2 PTP Profiles

- Ordinary
- Grandmaster
- Boundary
- Transparent
  - Transparent End-to-End
  - Default Profile
  - Peer to Peer – Power Profile
- Default
  - Best Master Clock Algorithm
    - \*BMCA Applies to all profiles
- Power Profile
  - IEEE C37.238-2011
- Dot1as
  - 802.1AS
- Telecom
  - ITU-T G.8265.1
  - ITU-T G.8275.1

\*WAN only with Timing module.

## Sync E

- ITU-T G.8261
- ITU-T G.8262
- ITU-T G.8264
- ITU-T G.781



## Ethernet Synchronization Message Channel

- ITU-T G.8264

IoT OD

# Network Management Solution



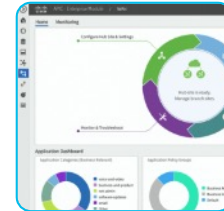
OT Driven



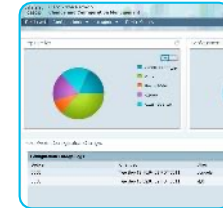
Control Center Support –  
SIM Management



Cisco IoT Field  
Network Director



Cisco DNA Center



Cisco Prime  
Infrastructure



Cisco SDWAN



IT Driven

# Management Tools



## OT Operated

Controls Engineer  
T&D Engineer  
Mass Transit Operator



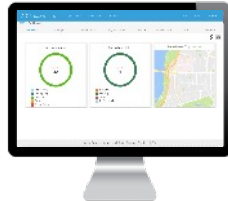
On-Prem



IoT-FND



Cloud



IoT-OD\*



On-Prem



DNAC\*



Cloud

## IT Operated



Network Administrator  
IT Administrator



On-Prem



SD-WAN\*



Cloud

\*Post FCS

	OT Operated - On-Prem	OT Operated - Cloud	IT Operated - On-Prem	IT Operated - Cloud
Config template	CLI Based	GUI Based	CLI Based	GUI Based
NBAPI 3 <sup>rd</sup> party integration	✓	✗	✓	✓
RBAC	Comprehensive	Basic	Basic	Basic
Wi-SUN Mesh	✓	✗	✗	✗
Remote Site (Extended Ent)	✗	✗	✓	✓
Edge Compute	✓	✓	✗	✗
SCADA	✓	✓ Custom template	✓	Future roadmap

**Common features:** ZTD, Gateway Lifecycle Management, GIS Map, Real-Time Asset Tracking/Playback, Geo Location, Geo Fencing Events/Alerts, Multi-tenancy, App Management, Cellular connectivity Metric

# IOT OD

## What is EDM?

EDM is the ***Edge Device Manager***. A core service in Cisco IoT Operations Dashboard to manage industrial network configurations at scale:

- **Zero Touch Deployment (ZTD)**
  - Configuration Management
  - Visibility and Monitoring
  - Alerts and Reports
  - Troubleshooting Tools
  - **Software Upgrades**
  - *SIM Management with Control Center Integration*
  - **Cisco Validated Design Templates**
- 
- IoT OD support of Meraki Camera
  - Secure Equipment Access (SEA) from EDM

# Navigating EDM Dashboard

The screenshot shows the Cisco IoT Operations Center EDM Dashboard. A central callout box lists the key features visible in the dashlets:

- Device Count
- Quick Device Status Summary
- Highest Cellular Data Users
- Weakest Cellular Signal
- Status Over Time
- GIS Map

Navigation callouts include:

- Service Navigation Dropdown (points to the top of the left sidebar)
- Task Navigation Menu (points to the middle of the left sidebar)
- Device Status (points to the 'Current Status' dashlet)
- Gateway GPS Map (points to the map at the bottom of the left sidebar)
- Organization Navigation Dropdown (points to the top right of the dashboard)
- Account Setting (points to the user profile icon)
- Select Time Range (points to the 'Last 24 Hours' dropdown)
- Summary Info (points to the top right of the dashboard)
- Integrated Guide (points to the 'Guide me!' button)
- Expand Map (points to the map area)



# Device Details

Device information can be drilled down in the Device Details page. Some fields can be modified. Select from the many Tabs to see different details.

The screenshot shows the Cisco IoT Operations Center interface for a device named FTX2103Z035. The page is divided into several sections:

- Navigation:** A sidebar on the left contains 'Onboard/Delete Device', 'Dashboard', 'Inventory', 'Configuration', 'Software', and 'Operations'. A 'Select Device for Details' callout points to the 'Inventory' section.
- Header:** The top header includes 'SERVICES', 'Edge Device Manager', and 'Inventory > FTX2103Z035 Summary'. A 'Demo' dropdown is in the top right. A 'Tabs' callout points to the navigation tabs.
- Tabs:** A row of tabs is highlighted with a red box: 'Summary', 'Monitoring', 'Event Log', 'Running Configuration', 'AP Configuration', 'Troubleshooting', and 'Interface'.
- Status:** A 'Status' section shows 'HEALTH Up' and 'Wi-Fi STATUS Online'. A 'NUMBER OF CLIENTS' is shown as '0'. A 'WiFi Info' callout points to this section.
- Device Details:** A section titled 'Device Details' with an 'Edit' link. A 'Customize Column View' callout points to the 'Customize' button on the right. The data is as follows:

Name	FTX2103Z035	Firmware Version	15.9(3)M2a
IP Address	10.8.2.65	Serial Number	FTX2103Z035
Last Heard	7 seconds ago	Config Group	Basic IR829 eCVD w AP
Open Issues	0	Latitude	0.0
- Cellular Details:** A section titled 'Cellular Details' with a 'View More' link. The data is as follows:

Cellular Status (SIM1)	Active	IMEI (SIM1)	356734060394933
Cellular Connection Type (SIM1)	LTE	APN (SIM1)	CiscoKinetic.com.attz
Cellular Connection (SIM1)	AT&T	MSISDN (SIM1)	N/A
- Cellular Plan Details:** A section titled 'Cellular Plan Details' with a 'View More' link. The data is as follows:

Status	ACTIVATED	Data Usage	4955384832
Rate Plan	Cisco - Kinetic - 5GB Plan	SMS Usage	0
Communication Plan	Cisco - Kinetic - AT&T-GPRS/LTE SMS/MO/MT INT	Voice Usage	0
- Actions:** An 'Edit Device Config' callout points to the 'Actions' dropdown in the top right.

Cyber Vision 4.0

# Cisco Cyber Vision

Asset Inventory & Security Platform for the Industrial IoT



## ICS Visibility

Asset Inventory  
Communication Patterns  
Device Vulnerability



## Operational Insights

Identify configuration changes  
Record control system events  
relevant to the integrity of the system

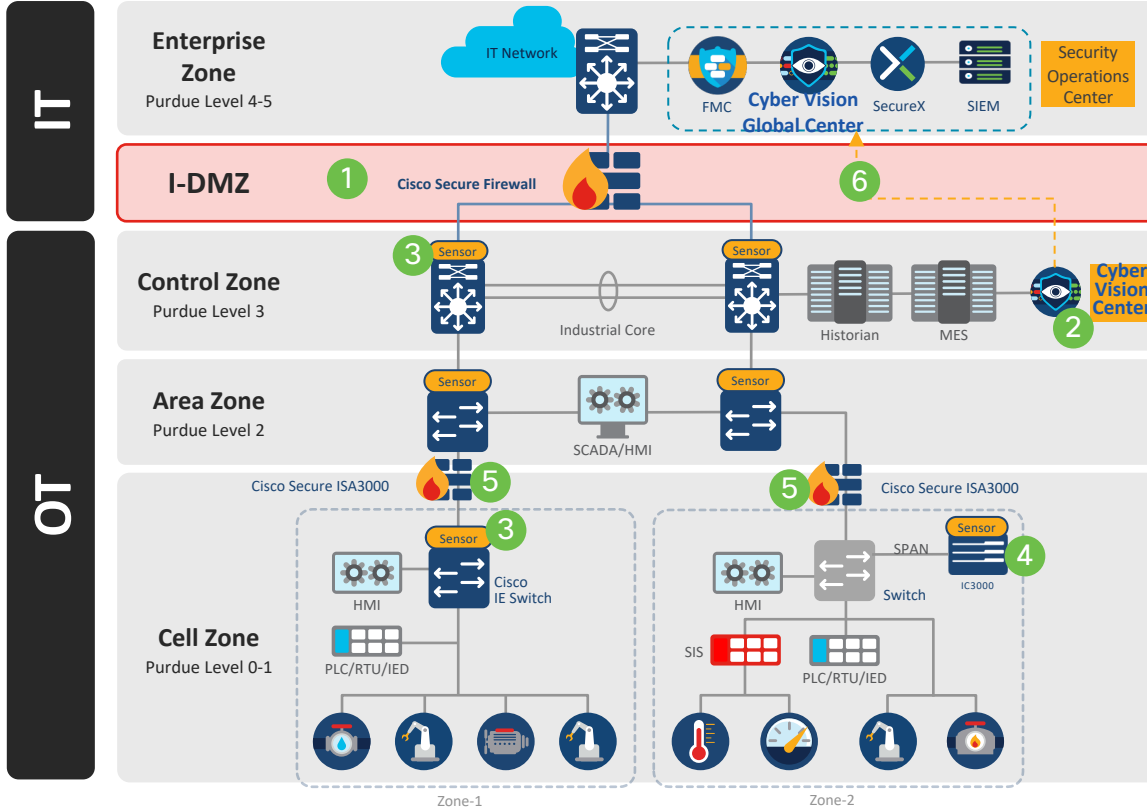


## Threat Detection

Behavioral Anomaly Detection  
Signature based IDS  
Real-time alerting

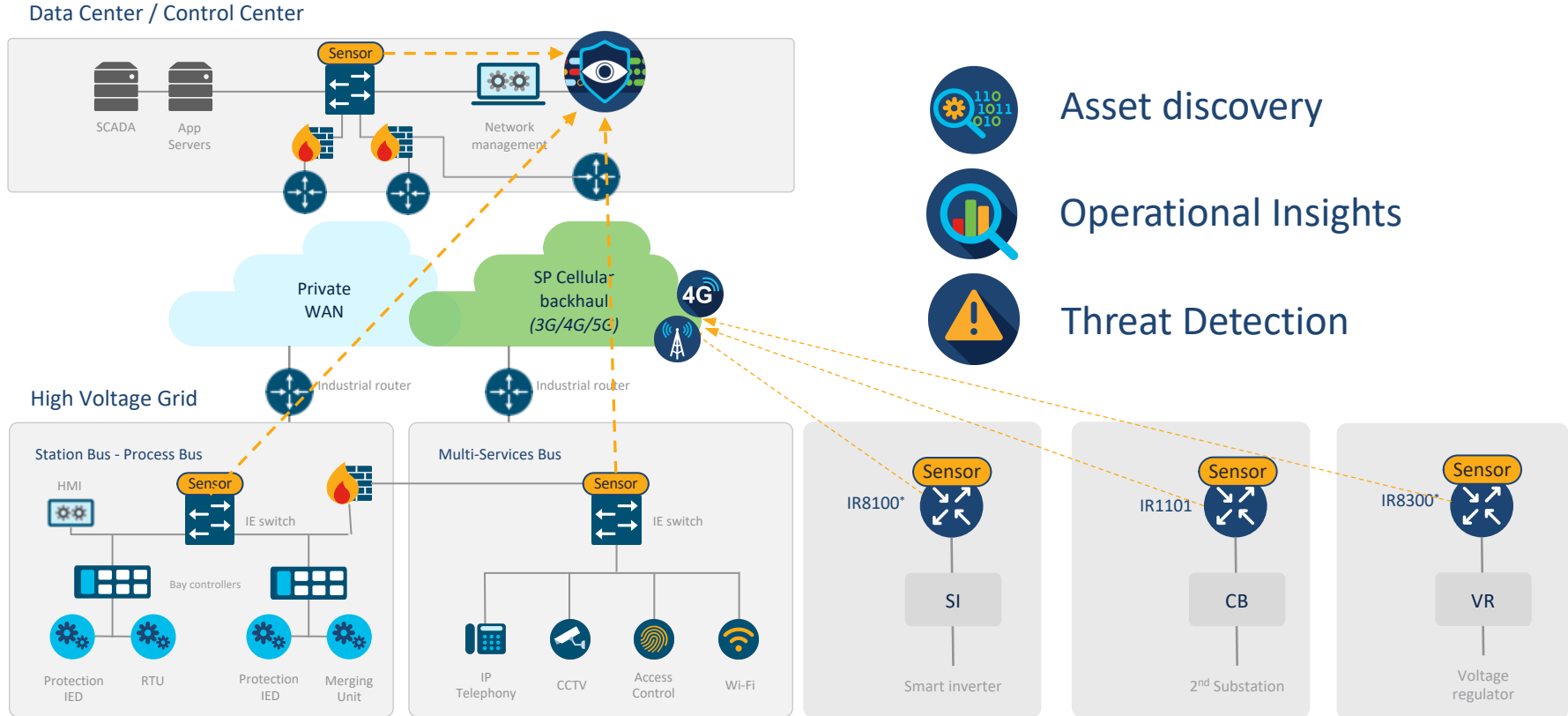
Cisco Cyber Vision helps companies protect  
their industrial control systems against cyber risks

# Cisco Cyber Vision in Manufacturing



- 1 Isolate IT and OT by installing an industrial DMZ with Cisco Secure FW
- 2 Install Cyber Vision Sensors and Center to gain visibility on OT
- 3 Cyber Vision Sensors embedded on IE3400 and Catalyst 9300 switches
- 4 Cyber Vision hardware-sensors deployed via one-hop SPAN to gain visibility on non-Cisco switches
- 5 Deploy Cisco Secure ISA3000 to isolate production zones
- 6 Cyber Vision shares details on OT devices and events with SOC to build informed security policies and investigate threats across domains

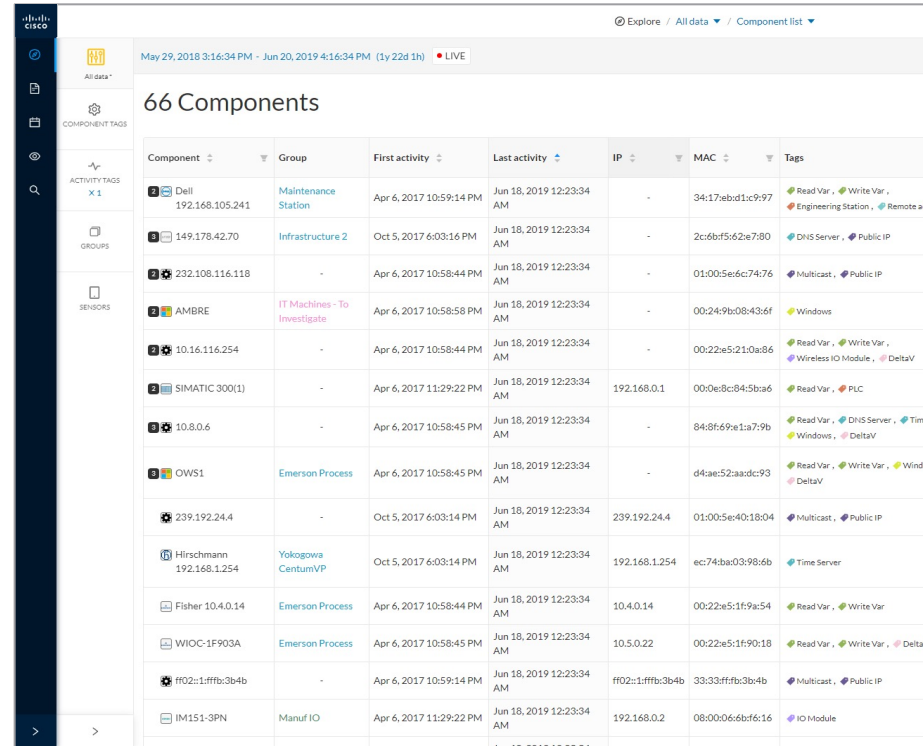
# Visibility in electric utilities architecture



# Visibility: Comprehensive asset inventory

- Automatically maintain a detailed list of all OT & IT equipment
- Immediate access to software & hardware characteristics
- Track rack-slot components
- Tags make it easy to understand asset functions and properties

Track the industrial assets to protect throughout their life cycles



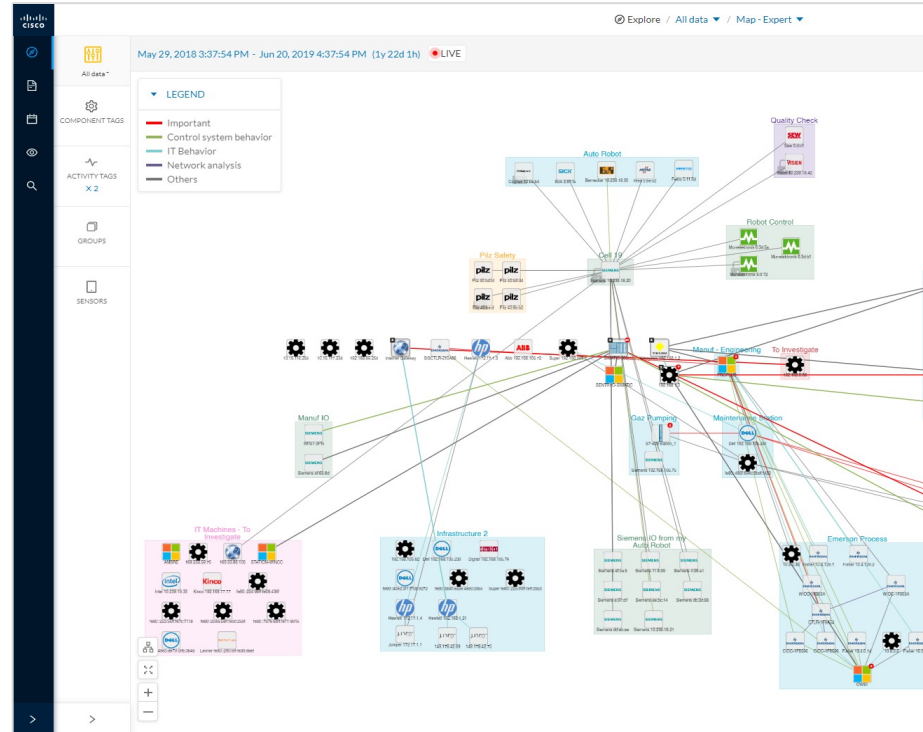
The screenshot displays the Cisco Alltags+ interface, showing a table of 66 components. The table includes columns for Component, Group, First activity, Last activity, IP, MAC, and Tags. The components listed include Dell, Hirschmann, Fisher, WIIOC, and IM151-3PN, among others, with their respective groups and activity dates.

Component	Group	First activity	Last activity	IP	MAC	Tags
Dell 192.168.105.241	Maintenance Station	Apr 6, 2017 10:59:14 PM	Jun 18, 2019 12:23:34 AM	-	34:17:ebd1c9:97	Read Var., Write Var., Engineering Station, Remote
149.178.42.70	Infrastructure 2	Oct 5, 2017 6:03:16 PM	Jun 18, 2019 12:23:34 AM	-	2c:6bf5:62e7:80	DNS Server, Public IP
232.108.116.118	-	Apr 6, 2017 10:58:44 PM	Jun 18, 2019 12:23:34 AM	-	01:00:5e:6c74:76	Multicast, Public IP
AMBRE	IT Machines - To Investigate	Apr 6, 2017 10:58:58 PM	Jun 18, 2019 12:23:34 AM	-	00:24:9b:08:43:6f	Windows
10.16.116.254	-	Apr 6, 2017 10:58:44 PM	Jun 18, 2019 12:23:34 AM	-	00:22:e5:21:0a:86	Read Var., Write Var., Wireless IO Module, DeltaV
SIMATIC 300(1)	-	Apr 6, 2017 11:29:22 PM	Jun 18, 2019 12:23:34 AM	192.168.0.1	00:0e:8c:84:5b:a6	Read Var., PLC
10.8.0.6	-	Apr 6, 2017 10:58:45 PM	Jun 18, 2019 12:23:34 AM	-	84:8f:69e1:1a:79:b	Read Var., DNS Server, Windows, DeltaV
OWS1	Emerson Process	Apr 6, 2017 10:58:45 PM	Jun 18, 2019 12:23:34 AM	-	d4ae:52aa:dc9:3	Read Var., Write Var., DeltaV
239.192.24.4	-	Oct 5, 2017 6:03:14 PM	Jun 18, 2019 12:23:34 AM	239.192.24.4	01:00:5e:40:18:04	Multicast, Public IP
Hirschmann 192.168.1.254	Yokogawa CentumVP	Oct 5, 2017 6:03:14 PM	Jun 18, 2019 12:23:34 AM	192.168.1.254	ec:74:ba:03:98:6b	Time Server
Fisher 10.4.0.14	Emerson Process	Apr 6, 2017 10:58:44 PM	Jun 18, 2019 12:23:34 AM	10.4.0.14	00:22:e5:1f:9a:54	Read Var., Write Var.
WIIOC-1F903A	Emerson Process	Apr 6, 2017 10:58:45 PM	Jun 18, 2019 12:23:34 AM	10.5.0.22	00:22:e5:1f:90:18	Read Var., Write Var., Delta
ff02::1:fff:b:3b:4b	-	Apr 6, 2017 10:59:14 PM	Jun 18, 2019 12:23:34 AM	ff02::1:fff:b:3b:4b	33:33:fff:b:3b:4b	Multicast, Public IP
IM151-3PN	Manuf IO	Apr 6, 2017 11:29:22 PM	Jun 18, 2019 12:23:34 AM	192.168.0.2	08:00:06:60:f6:16	IO Module

# Visibility: Track application flows

- Identify all relations between assets including application flows
- Spot unwanted communications & noisy assets
- Tags make it easily to understand the content of each communication flow
- View live information or go back in time

Drive network segmentation and fine-tune configurations



# Visibility: Instantaneous vulnerability identification

- Automatically spot software & hardware vulnerabilities across all your industrial assets
- Access comprehensive information on vulnerability severities and solutions
- Built-in vulnerability database curated by Cisco Research Teams always up to date

Enforce cyber best practices

The screenshot displays the Cisco ICSA Security Center interface. At the top, it shows the date range from Jan 1, 2019, to Apr 29, 2019, and indicates 234 vulnerabilities. A donut chart shows the distribution of vulnerabilities across different categories. A table lists the top 10 vulnerabilities, including CVE-2017-12741, CVE-2014-0791, and CVE-2014-3888. Below the table, a detailed view of a component (SIMATIC 300(1)) is shown, including its IP address (192.168.0.1) and MAC address (000e8c8452a6). The interface also displays various metrics such as 24 flows, 51 events, and 13 variables. A section titled 'Vulnerabilities' lists two specific vulnerabilities: CVE-2017-12741 (Multiple Siemens Products CVE-2017-12741 Denial of Service Vulnerability) and CVE-2016-9158 (SIMATIC S7-300 and S7-400 CPUs Denial of Service and Information Disclosure Vulnerabilities). Each vulnerability entry includes a severity score of 7.8 (CVSS), a detailed description, a solution, and a link to the Siemens Security Advisory.



# Operational insights: Views for OT teams

- Asset details
- Communication maps
- PLC program changes
- Variable accesses

Monitor the integrity of your industrial process

**Component**  
SIMATIC 300(1)  
IP: 192.168.0.1  
MAC: 00:0e:8c:84:5ba6  
First activity: Apr 6, 2017 11:29:22 PM  
Last activity: May 26, 2019 12:21:13 AM  
24 Flows, 51 Events, 5 Vulnerabilities, 13 Variables

**Minimap**  
LEGEND: Important, Control system behavior, IT Behavior, Network analysis, Others  
Machines - To Investigate: STATION WINCC, SIEMENS M151-3PN, Siemens ef 65 8d, SENTRYO-XP-1, SIEMENS Siemens 192.168.0.10  
Manuf - IO, Manuf - Scada & HMI  
SIMATIC 300(1), SENTRYO-SIMATICProfinet DCP Multicast 0.0.0, 10.45.1.255

**Variables accesses**  
13 / 20 / page

Variable	Types	Accessed by	First access	Last access
> M.2.0	READ	2 components (2 accesses)	Apr 6, 2017 11:29:22 PM	May 26, 2019 12:21:23 AM
▼ M.2.1	READ	2 components (2 accesses)	Apr 6, 2017 11:29:22 PM	May 26, 2019 12:21:23 AM
	READ	Siemens 192.168.0.10	Apr 6, 2017 11:29:22 PM	May 26, 2019 12:21:23 AM
	READ	SENTRYO-XP-1	Apr 6, 2017 11:29:22 PM	May 26, 2019 12:21:23 AM
> M.8.0	READ	2 components (2 accesses)	Apr 6, 2017 11:29:22 PM	May 26, 2019 12:21:23 AM
> M.8.1	READ	2 components (2 accesses)	Apr 6, 2017 11:29:22 PM	May 26, 2019 12:21:23 AM
> M.8.2	READ	2 components (2 accesses)	Apr 6, 2017 11:29:22 PM	May 26, 2019 12:21:23 AM

# Tracking security events in 4.0



8x faster data ingestion



Speedy UI even with large datasets



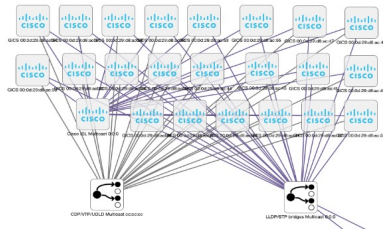
Smarter data retention to avoid disk saturation

- Components vs. Devices
- Risk scoring
- Network boundaries
- New vulnerability detection – switches
- New protocol support
- New activity tags
- Splunk integration

# Understanding Components vs. Devices

## Cyber Vision 3.x was listing **Components**

- Hardware identified by a MAC or IP addresses or Slot IDs
- Can be directly related to the network logic of the OT process



Catalyst switch in 3.0



## Cyber Vision 4.0 now lists **Devices**

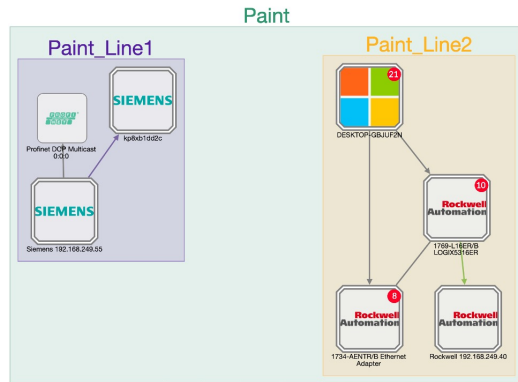
- Physical devices made of several components
- Can be directly related to the device performing a certain task in the industrial process



Catalyst switch in 4.0

# Enhanced device aggregation - Changes to Licensing

## Map view



New double-border icons indicate a device

## ID Cards

Controller Rack

1769-L16ER/B LOGIX53...  
Paint\_Line2 ▲ high  
IP: 192.168.249.50  
MAC: f4:54:33:91:cb:ee

First activity: Apr 28, 2021 11:48:40 AM  
Last activity: Apr 28, 2021 11:48:46 AM

Sensor: -

Tags: Controller, Rockwell Automation

Activity tags: Read Var, Write Var, Low Volume, CIP-IO, EthernetIP

Risk score: 80% See details

Modules:  
Rockwell 192.168.249.50  
Rockwell 192.168.249.50  
Rockwell 192.168.249.50  
Rockwell 192.168.249.50  
24VDC 16PT INPUT & 16PT OUTPUT (Port1-Link01)  
Rockwell 192.168.249.50  
1769-L16ER/B LOGIX5316ER  
SecDemo\_LinePLC | 1769-L16ER/B LOGIX5316ER  
Rockwell 192.168.249.50

Properties:  
fw-version: 31.011  
ip: 192.168.249.50  
mac: f4:54:33:91:cb:ee  
model-ref: 24VDC 16PT INPUT & 16PT OUTPUT, 1769-L16ER/B LOGIX5316ER  
name: Rockwell 192.168.249.50, 24VDC 16PT INPUT & 16PT OUTPUT (Port1-Link01), 1769-L16ER/B LOGIX5316ER...  
[...show more](#)

## Technical Sheets

8 Components

Component	First activity	Last activity	IP	MAC	Tags	Vulnerabilities	Flows	VLAN ID	Sensor
1754-L551A 1754-M12/A LOGIX5555 (Port1-Link00)	Oct 11, 2019 11:12:58 AM	May 24, 2021 12:32:15 PM	192.168.0.200	00:00:bc:5f:8c:ce	Controller	2	-10	-	
1754-OB16/A DCOU/ISOL (Port1-Link04)	Oct 11, 2019 11:12:58 AM	May 24, 2021 12:32:15 PM	192.168.0.200	00:00:bc:5f:8c:ce	No tags	0	-10	-	
1756-IB16/A DCIN/ISOL (Port1-Link03)	Oct 11, 2019 11:12:58 AM	May 24, 2021 12:32:15 PM	192.168.0.200	00:00:bc:5f:8c:ce	No tags	0	-10	-	
1756-IB16/A DCIN/ISOL (Port1-Link02)	Oct 11, 2019 11:12:58 AM	May 24, 2021 12:32:15 PM	192.168.0.200	00:00:bc:5f:8c:ce	No tags	0	-10	-	
1756-OB16/A DCOU/ISOL (Port1-Link05)	Oct 11, 2019 11:12:58 AM	May 24, 2021 12:32:15 PM	192.168.0.200	00:00:bc:5f:8c:ce	No tags	0	-10	-	
SUBSTATION-119-PLC01	Oct 11, 2019 11:12:58 AM	May 24, 2021 12:32:15 PM	192.168.0.200	00:00:bc:5f:8c:ce	No tags	9	-10	-	
1754-ENBT/A (Port1-Link01)	Oct 11, 2019 11:12:58 AM	May 24, 2021 12:32:15 PM	192.168.0.200	00:00:bc:5f:8c:ce	No tags	9	-10	-	
Rockwell 192.168.0.200	Oct 11, 2019 11:12:58 AM	May 24, 2021 12:32:15 PM	192.168.0.200	00:00:bc:5f:8c:ce	No tags	0	-10	-	

Easily list the components of a device. Click on a component to view more details

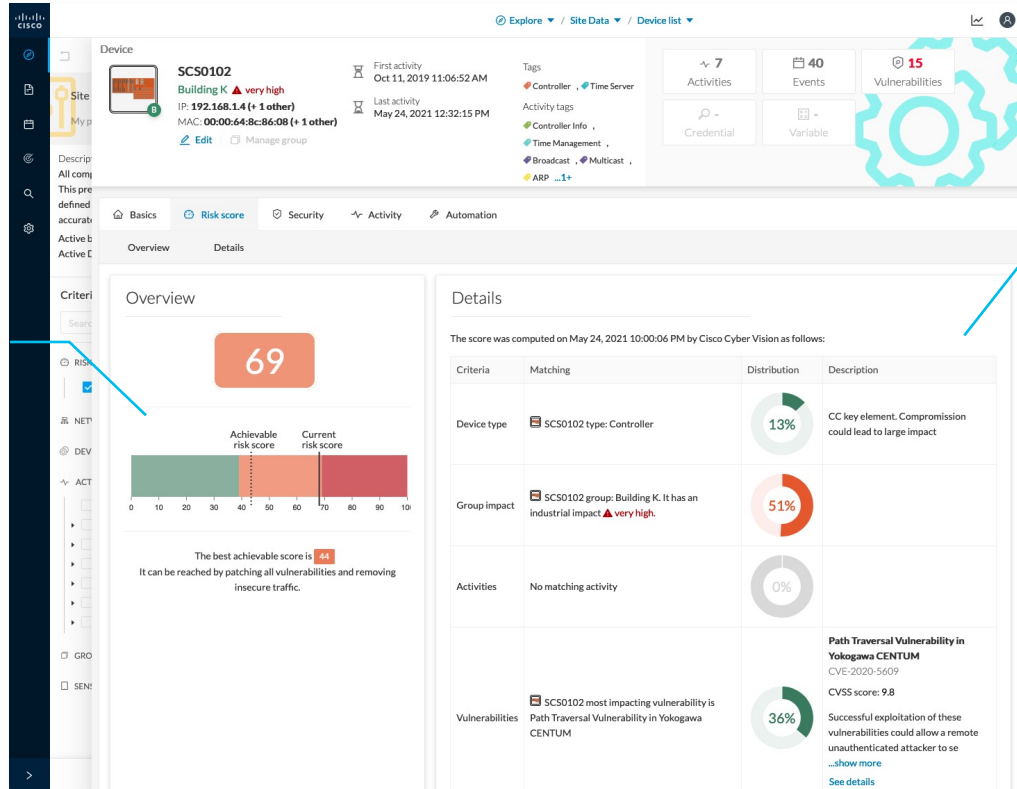
# Defining the Cyber Vision risk scores

- Risk = Likelihood x Impact
- Likelihood
  - Activity tags (some communications create more risks)
  - Exposure to external IP addresses
  - Discovered vulnerabilities
- Impact
  - Device tags (some devices can create more damages)
  - User-defined industrial impact for groups

Impact	Critical	High	High	High	High
	high	negligible	Significant	High	High
	limited	negligible	negligible	Significant	Significant
	No impact	negligible	negligible	negligible	negligible
		Minimal	Significant	High	Maximal
		Likelihood			

Source: EBIOS

# Understanding a device risk score



Understanding how to lower risk

Understanding what impacts the risk score



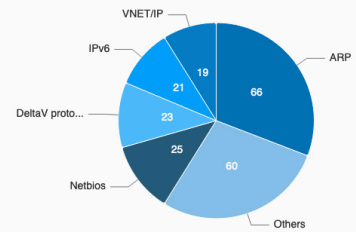
# Welcome to Cisco Cyber Vision

Last 30 days overview

Operational overview | Security overview

All  Protocol distribution  Most critical events  Presets highlight

### Protocol distribution



### Most critical events

Jun 17, 2021 9:36:54 AM	Critical	System has been updated	Cisco Cyber Vision A...
Jun 17, 2021 9:36:54 AM	Critical	System has been updated	Cisco Cyber Vision A...
Jun 17, 2021 9:36:54 AM	Critical	Snort TCP alert id 42340 with signature *OS-WIN...	
Jun 17, 2021 9:37:33 AM	Critical	Center has been shut down	Cisco Cyber Vision ...
Jun 17, 2021 9:36:54 AM	Critical	System has been updated	Cisco Cyber Vision A...
Jun 17, 2021 9:36:54 AM	High	New component detected	Inventory Events
Jun 17, 2021 9:36:54 AM	High	Program Upload	Control Systems Events
Jun 17, 2021 9:36:54 AM	High	New component detected	Inventory Events
Jun 17, 2021 9:36:54 AM	High	New component detected	Inventory Events
Jun 17, 2021 9:36:54 AM	High	New component detected	Inventory Events

### Presets highlights

Edit favorite presets

Preset	Risk score	Last precomputation	Devices	Vulnerabilities	Events
All Controllers	26.5	Jun 17, 2021 9:46:41 AM	14	94	2098
Broadcast traffic only	12	Jun 17, 2021 9:46:47 AM	30	158	2289
IT Activities	16	Jun 17, 2021 9:46:47 AM	36	169	5343
IT Devices	25	Jun 17, 2021 9:46:49 AM	23	94	5242
Internet Activities	12	Jun 17, 2021 9:46:45 AM	0	0	1779
OT Devices	28	Jun 17, 2021 9:46:46 AM	21	128	1000

Focus on OT or security insights

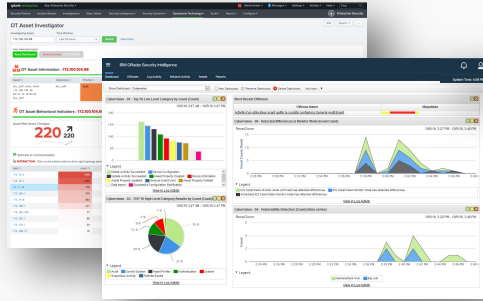
Pin specific presets to home dashboard

Quickly identify "Riskiest" presets

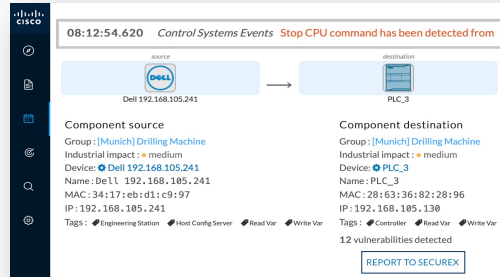
Counters per preset

# Investigate industrial events in your IT SOC

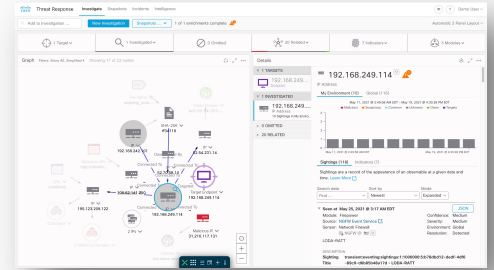
Cyber Vision Apps for Splunk & QRadar



Cyber Vision



SecureX



1

Get alerted to incidents in the industrial network in your SIEM through syslog and API integration with Cyber Vision

2

Pivot to the corresponding instance of Cyber Vision to get more details on the event that generated the alert

3

Promote the event to SecureX incident manager and investigate with enrichment from Cisco and 3<sup>rd</sup> party security products



# Závěr

- Nové cloudově spravované GW (včetně zodolněných verzí)
  - IG21, IG21R, IG31R
- Kompletní obměna IR portfolia
  - IR 1101, IR1800, IR8100, IR8300
  - Postupná dostupnost, rozšíření
  - loX, modularita
- IoT Operational Dashboard
  - Evoluce Kinetic GMM
  - Nástroj pro správu a ZTP
- CyberVision 4.0
  - Components x Devices
  - Risk scoring





# Literatura

## **Industrial routers and Gateways:**

<https://www.cisco.com/c/en/us/products/routers/industrial-routers-gateways/index.html#~benefits>

## **IoT OD:**

<https://www.cisco.com/c/en/us/products/cloud-systems-management/iot-operations-dashboard/index.html>

## **Cisco Cyber Vision:**

<https://www.cisco.com/c/en/us/products/security/cyber-vision/index.html>

## **Cisco Cyber Vision Datasheet:**

<https://www.cisco.com/c/en/us/products/collateral/se/internet-of-things/datasheet-c78-743222.html>

## **Cisco Cyber Vision Center Hardware Appliance Data Sheet:**

<https://www.cisco.com/c/en/us/products/collateral/security/cyber-vision/datasheet-c78-743481.html>