Novinky IoT portfolia v roce 2020

Jiří Rott

8.12.2020

Agenda

1. Cisco Industrial Security (Cyber Vision, FW)
2. Industrial switching
3. Industrial routing
4. Application hosting (IOX, Cisco Edge Intelligence)
5. Cisco Industrial Asset Vision

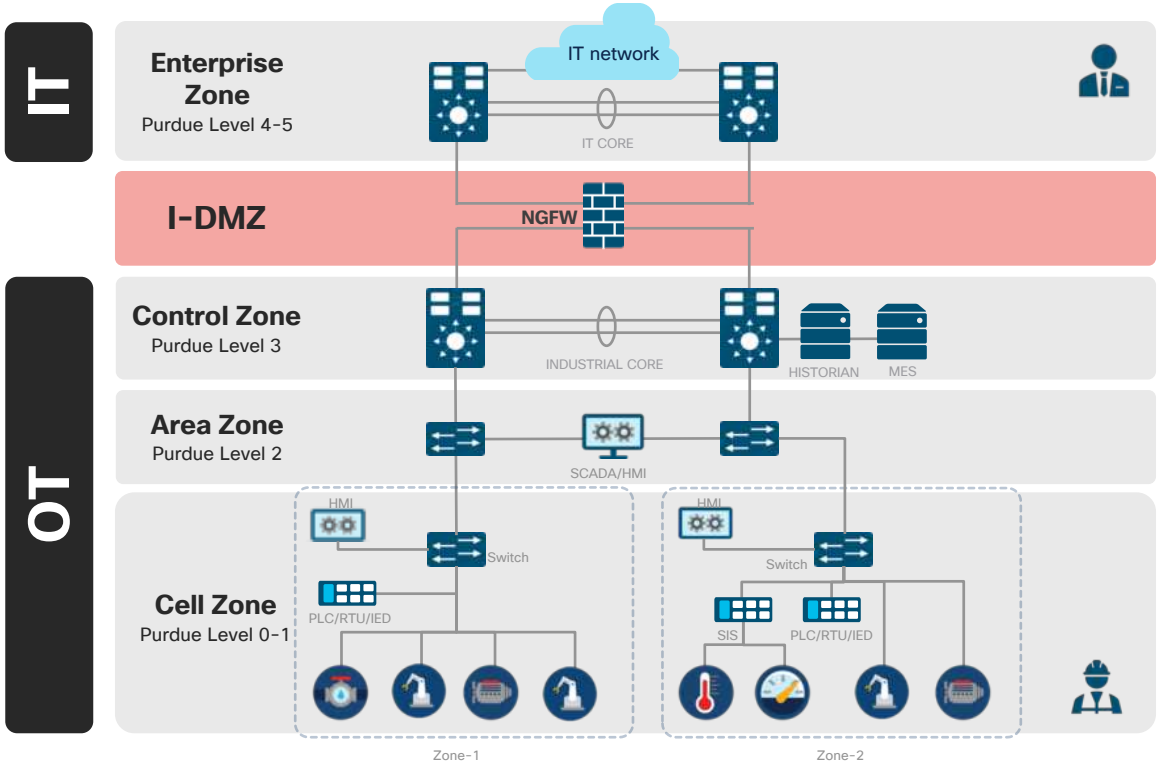
Industrial Security Update

Cyber Vision, ISA3K

Security is a journey

Foundation Security is next level

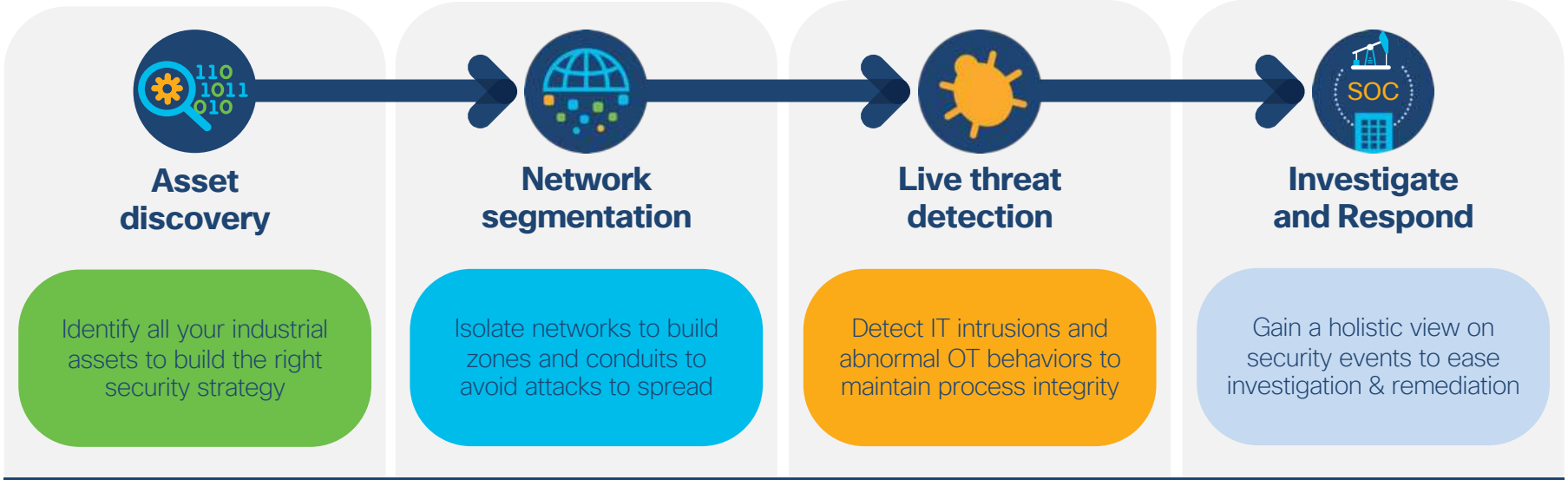
Step 1: Minimal Security



How do we enhance security posture to go from minimal security (IDMZ) to foundation security ?

Foundation Security – **CVD Release March 2021**

New capabilities to secure industrial networks



Gain visibility on your OT to build and enforce the right security policies

The **4-step journey** to secure your industrial network

Asset discovery

- **Cyber Vision** Asset inventory
- **Cyber Vision** Vulnerability detection
- Cisco CX assessment services

Network segmentation

- **ISA3000 Firepower** Zone-segmentation
- TrustSec Micro-segmentation
- ISE - Centralized segmentation policy

Full Spectrum

Live threat detection

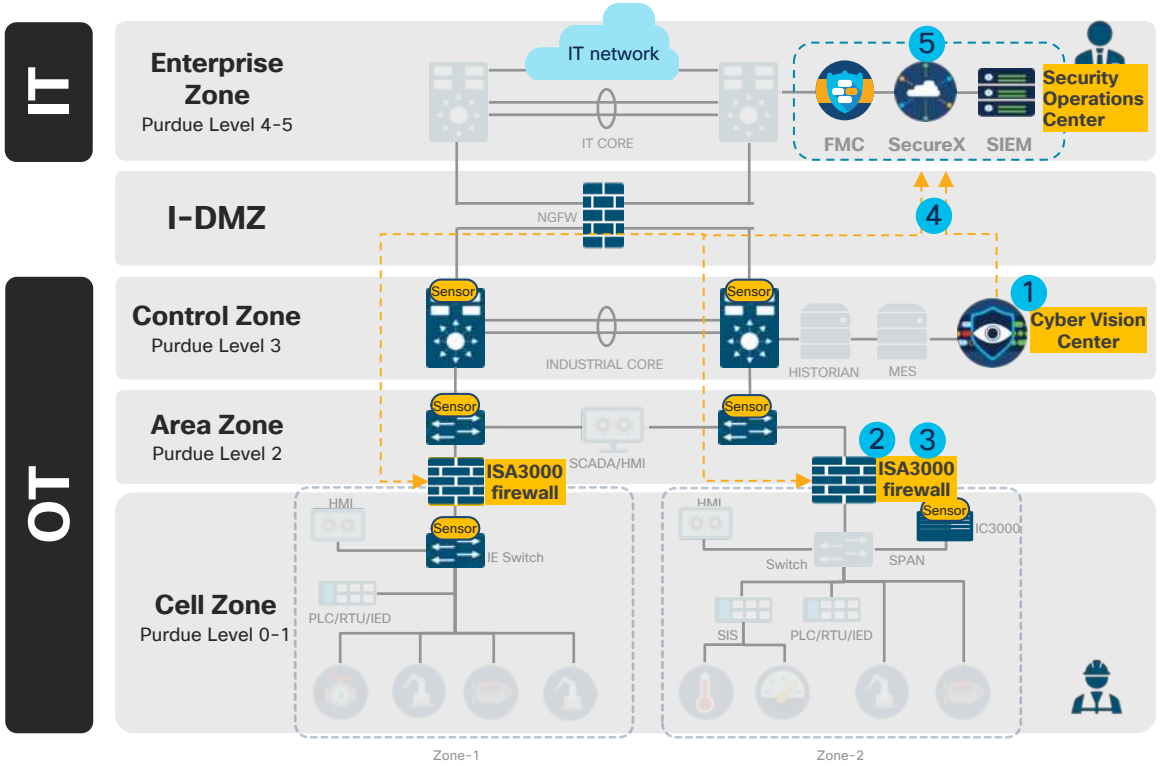
- **Cyber Vision** Anomaly detection
- Firepower/Cyber Vision Intrusion detection
- AMP / Threat Grid Malware detection

Integrated IT/OT SOC

Securing industrial control networks with Cisco

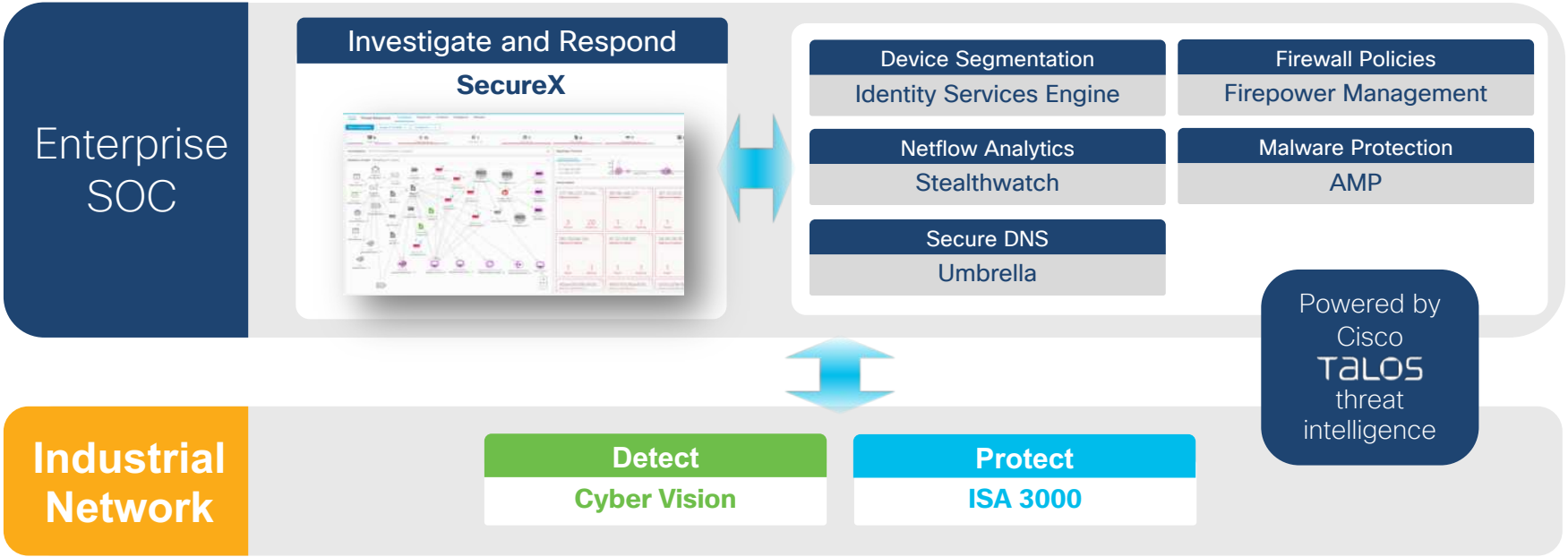
Step 2: Foundation Security

A simple architecture, easy to operate with few products



1. Know your assets with Cisco Cyber Vision
2. Segment networks and secure production cells with Cisco ISA3000
3. Protect against malware and intrusion with Firepower
4. Feed SOC with OT context
5. Investigate and remediate threats with Cisco SecureX

Cisco's fully integrated IT-OT security solution

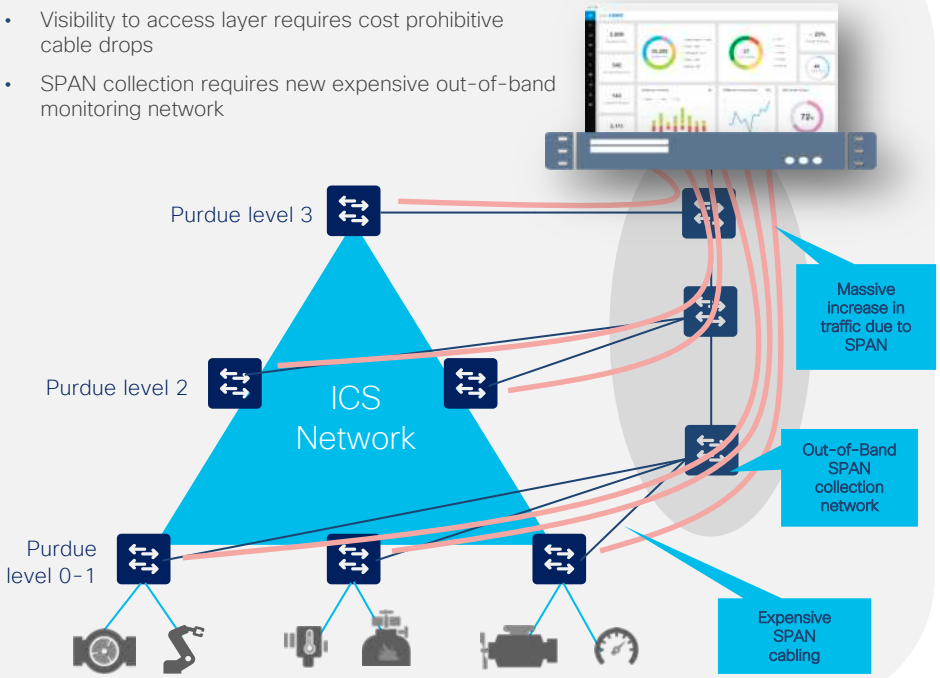


Cyber Vision **scalable** architecture

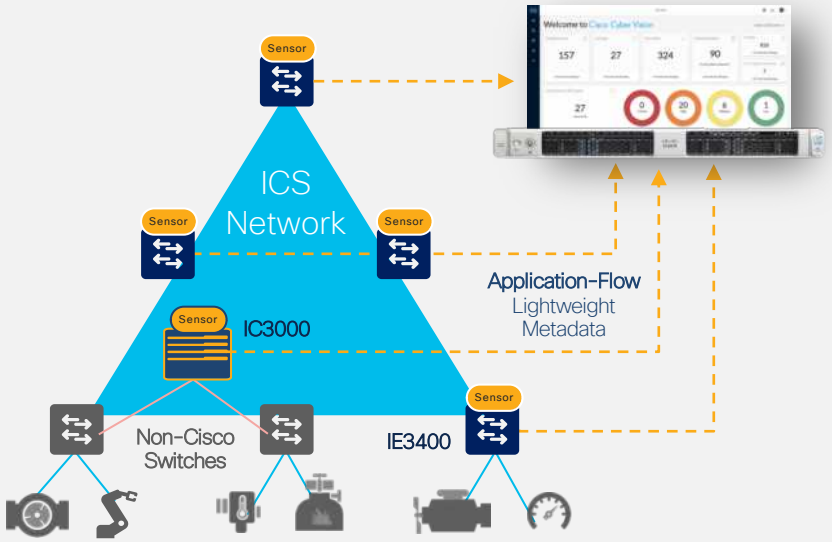
SPAN based solutions incur huge additional hidden-costs during deployment

- Visibility to access layer requires cost prohibitive cable drops
- SPAN collection requires new expensive out-of-band monitoring network

Other solutions



Cyber Vision Center



Network-Sensors eliminate the need for SPAN

- The application-flow is streamed through existing network enabling lowest TCO
- Hardware-sensor to support brownfield only requires one-hop SPAN

Cisco Cyber Vision portfolio

Passive OT – Asset inventory, Protocol discovery, Vulnerability detection, Anomaly detection

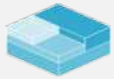
Cyber Vision **Center**

Hardware Appliance
UCS based servers with Hardware RAID

CV-CNTR-M5S5 **CV-CNTR-M5S3 (NEW)**

Software Appliance
Virtual Machines

VMWare ESXi OVA



HyperV VHD

Cyber Vision **Sensors**

IC3000 Industrial Compute

Hardware Sensor
(SPAN based to support brownfield)

Available !!!

IE3400 Switch

IE3400 IP67 Switch

IR1101 Gateway

Catalyst 9000 Series Switch

Network Sensors !!! Major differentiator
(Deep Packet Inspection built into network-elements eliminating the need for SPAN)

Cisco Cyber Vision 3.2

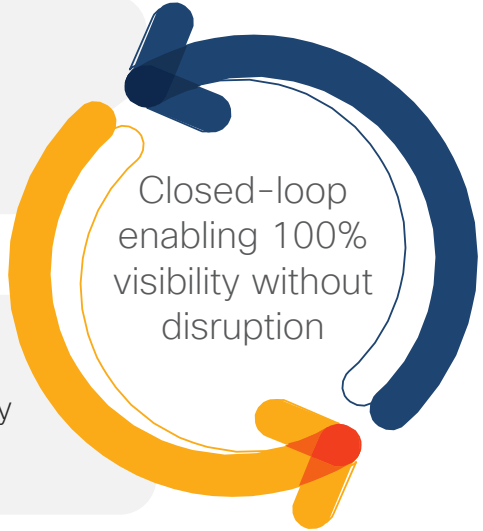
Active vs. Passive asset discovery

Passive Discovery

- Builds visibility by listening to network traffic
- No interaction with industrial assets
- Edge sensors see cell traffic without SPAN networks

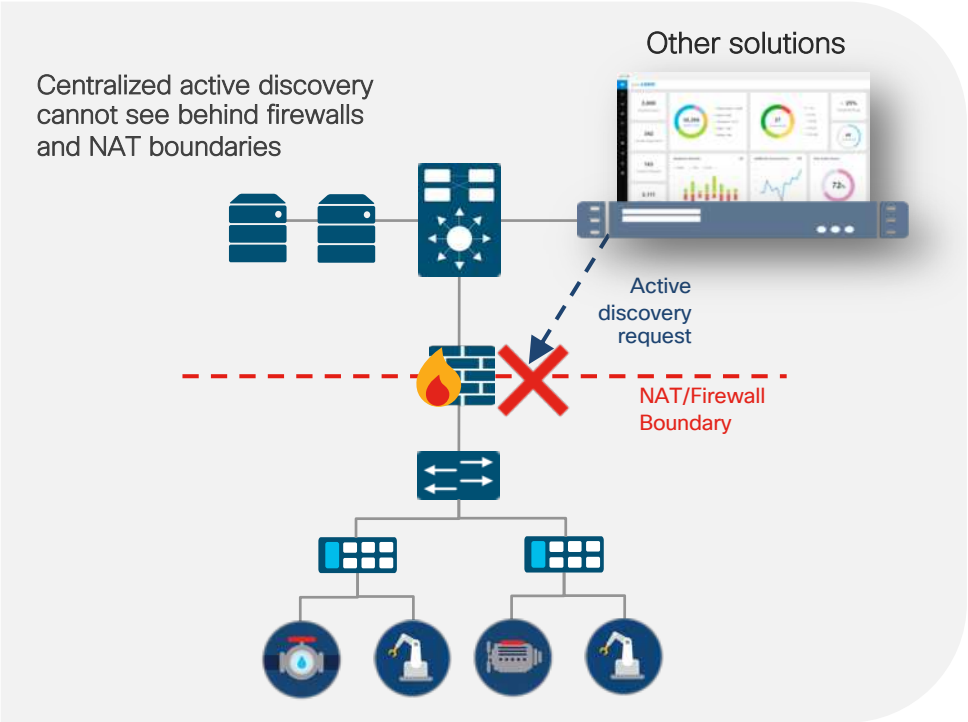
Active Discovery

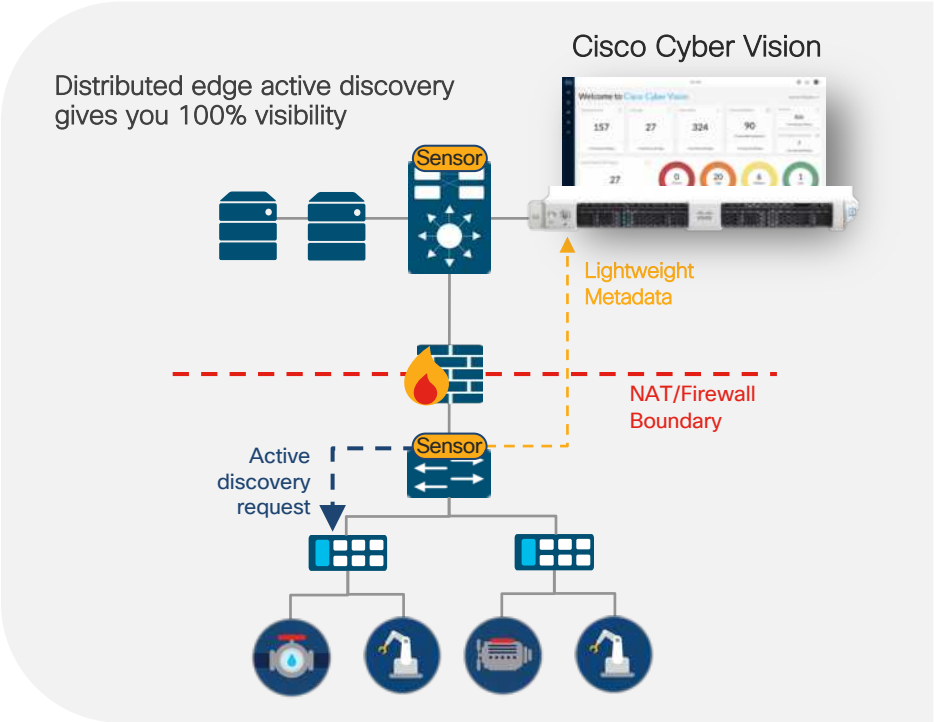
- Learns the ICS protocols at play from passive discovery
- Sensors send hello requests to discover silent devices
- Gets comprehensive details on every asset



Distributed edge discovery sees more

Silent devices, FWs

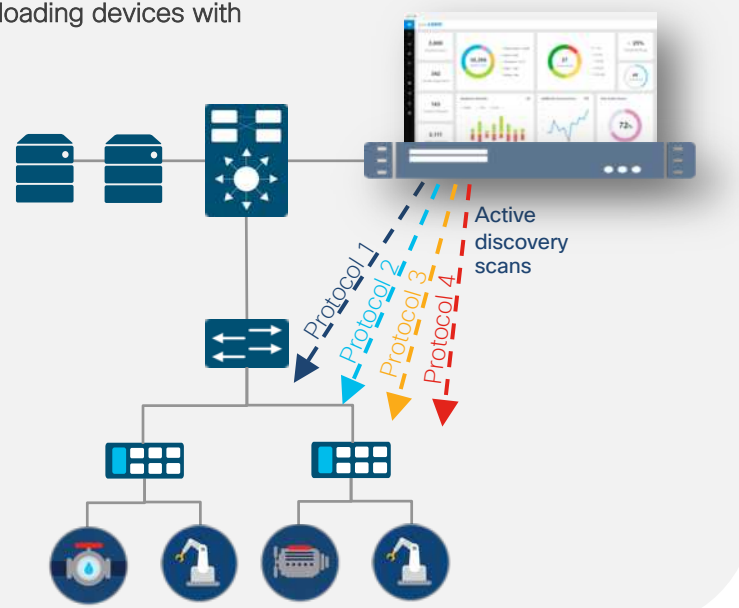




Closed-loop control makes active discovery safe

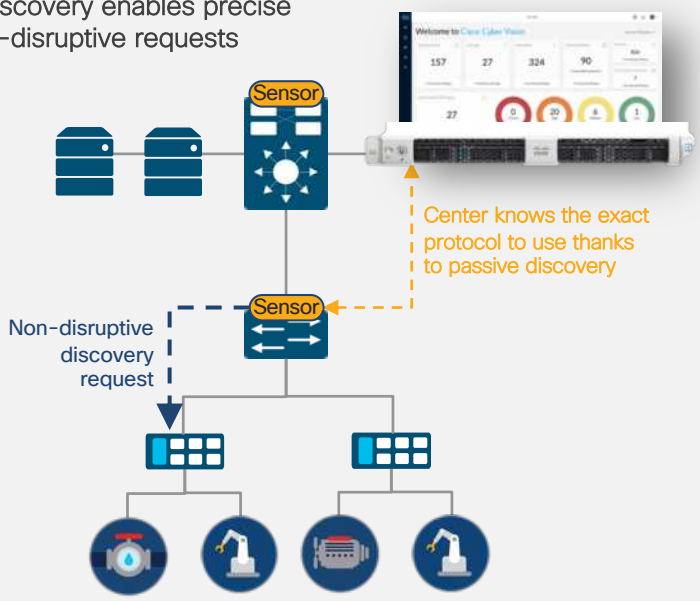
Basic active discovery solutions scan networks overloading devices with ARP requests

Other solutions



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

Cisco Cyber Vision



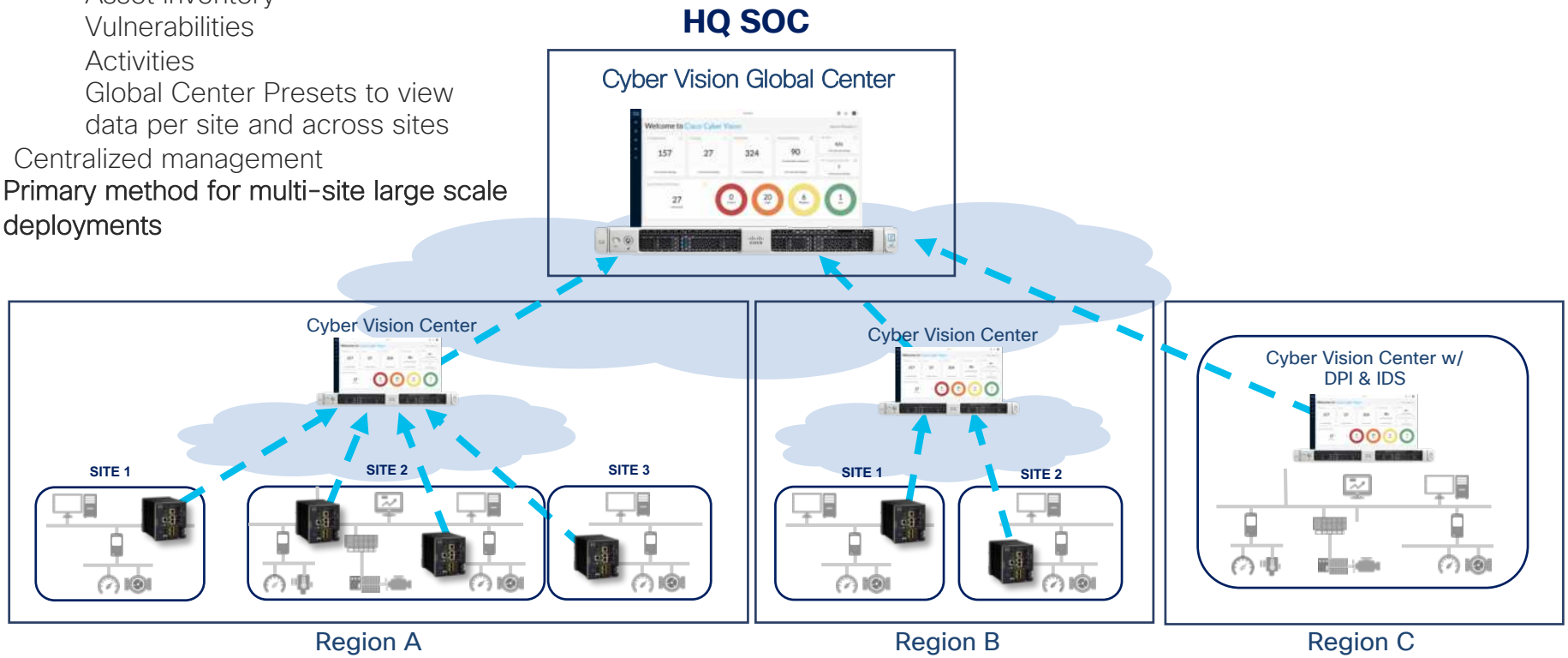
Cyber Vision Global Center

Global visibility

- Asset inventory
- Vulnerabilities
- Activities
- Global Center Presets to view data per site and across sites

Centralized management

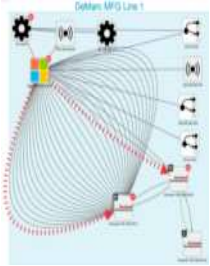
Primary method for multi-site large scale deployments



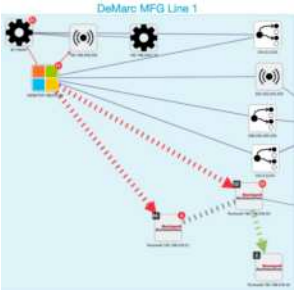
Giving global visibility on all industrial assets and security events across all sites from a central console

Aggregated activities: Simplifying the console

Unaggregated

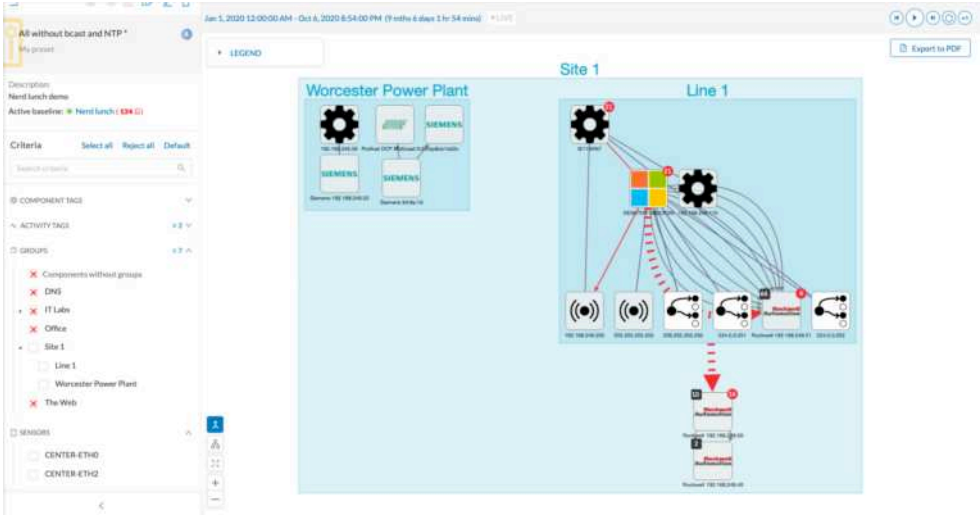


Aggregated



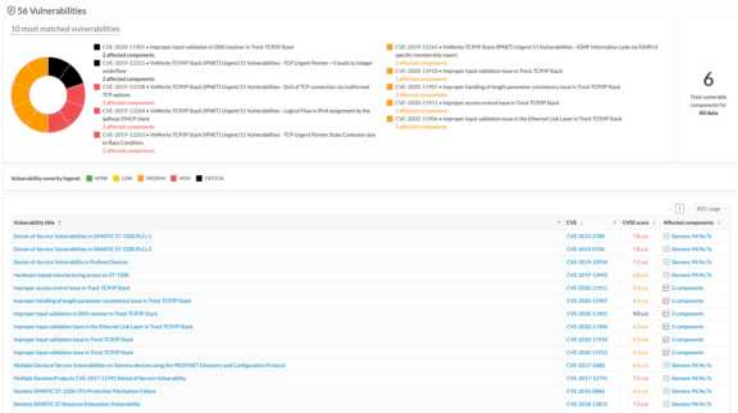
Nested groups

- Flexible organization to match the business and processes
- Multi-faceted views
- Quick drilldown



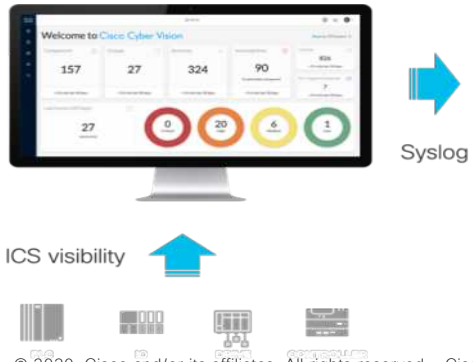
Vulnerability Dashboard

- Top 10 vulnerabilities
- Based on presets
  - Filter by tags, groups and/or sensors
- Links to quickly identify affected components
- Additional context for impact and remediation



IBM QRadar integration

Unified IT/OT security events management in SIEM

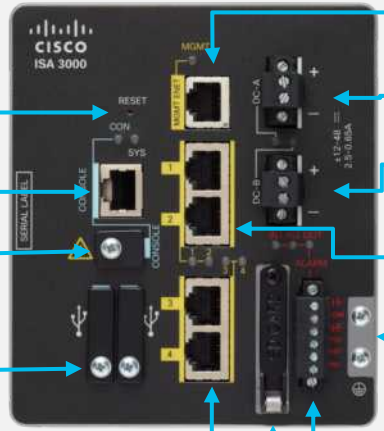


ISA3000
Built for OT

- **Two models:** 4 copper ports or 2 copper + 2 fiber ports
- **DIN-rail** mounting
- **Thermal support:** -40C to +60C
- **Hazloc** with nA protection
- **Environmental hardening** for vibration, shock, surge, and electrical noise immunity
- **Industry compliance** for industrial automation, ITS, and electrical substation environments
- **High availability** features such as hardware bypass, dual-power inputs, Quality of Service policies, and latency detection and mitigation functions ensure traffic continuity to keep operation on track

ISA-3000-4C

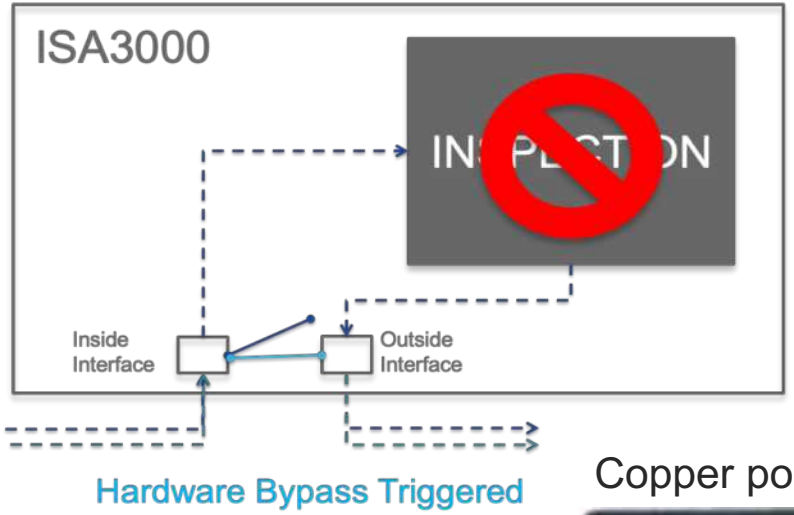
ISA-3000-2C2F



Hardware Bypass

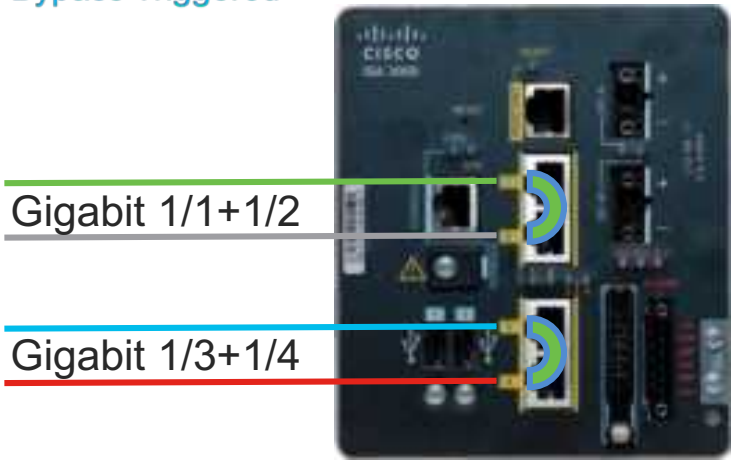
What happens?
- Powered Off
- Power Outage
- Reload

Bypass can also be enabled manually for
- Maintenance
- Software upgrade
- Security updates



- Hardware bypass functionality
  - Gigabit-Eth 1/1-1/2 and 1/3-1/4
  - Only for RJ-45 copper ports
  - Recommended only in FW transparent mode
  - Beware max. cable length (~50m)
- Software controllable options
  - Enable/Disable
  - Event driven (Power-Up/Down/Module-UP SFR)

Copper ports only



ISA3000 Industrial Protocol support

Protocol/Application detectors

BACNet
COSEM
COTP
DNP3
Emission control protocol
Fujitsu device control
GOOSE
GSE
IEC-60870-5-104
ISO MMS
Modbus
OPC-UA
Q931
SRC
TPKT
CIP
Honeywell Control Station/NIF Server
Honeywell Experion DSA Server Monitor

Deep Packet Inspection

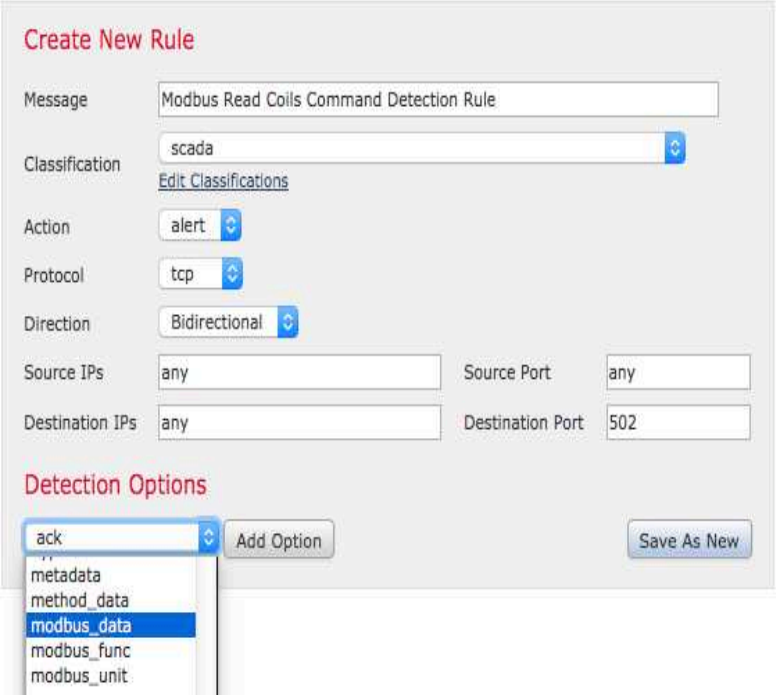
Options to inspect header, payload to filter based on functions, commands and data

Modbus
DNP3
CIP
IEC-60870-5-104
IEC 61850 - MMS

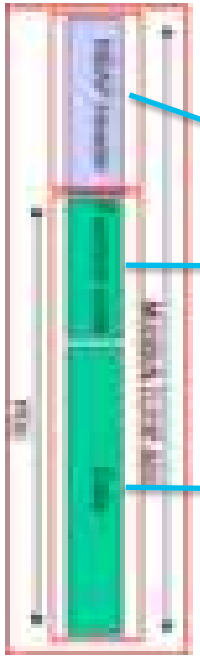
e.g., detect Modbus read coils, write single coil etc

OT Pre-processors – command inspection Modbus

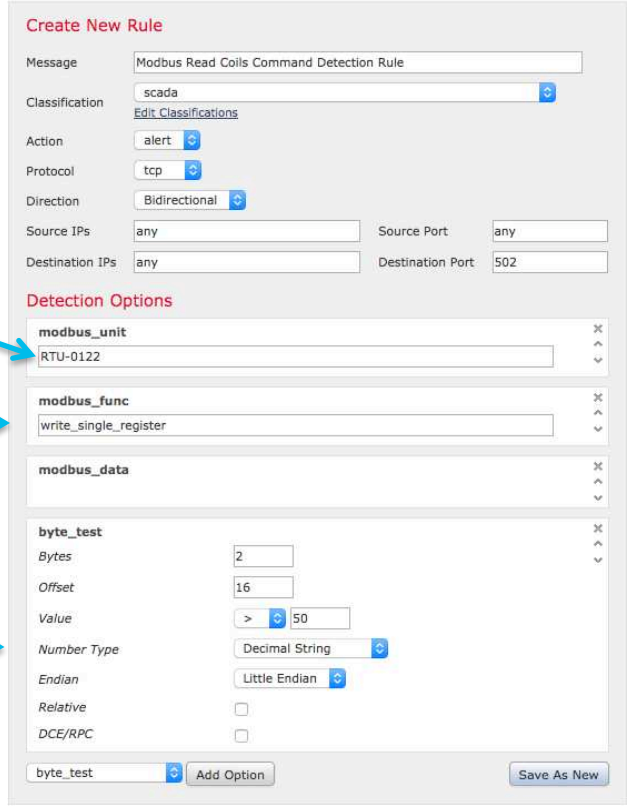
Modbus IPS rule options covers entire Modbus packet



Modbus packet



A Modbus rule to prevent increase the limit > 50 on RTU-0122



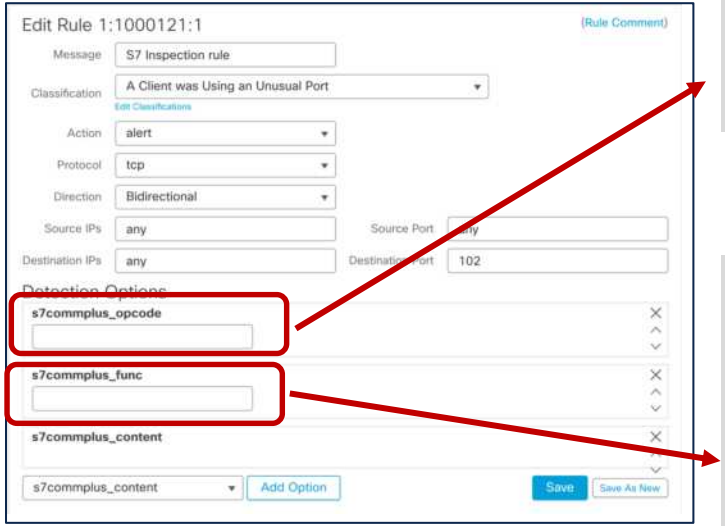
ISA3000 FTD 6.7
What's new?

OT Features	Useability improvements
	FTD Upgrade process improvements
Siemens S7 pre-processor - Customers with Siemens devices, EMEAR	FMC Remote deployment
IEC **60870-5-104** AppID - Support **whitelisting** of applications and commands	Unified device health monitoring
IEC 61850 MMS AppID - Support **whitelisting** of applications and commands	Identity policy improvements (pxGrid 2.0)
Hardware Bypass sticky option	Site-2_Site VPN – VTI support

S7 support

- Communication for **Siemens S7 PLCs (S7 300/400/1200/1500)**
- SCADA/Supervisor (e.g. **Step 7, TIA v13) ⇔ PLC S7**
- S7comm on COTP on TPKT on TCP (port 102)
- Siemens iso-on-tcp RFC1006

Intrusion rule for S7 detection



S7 opcodes:

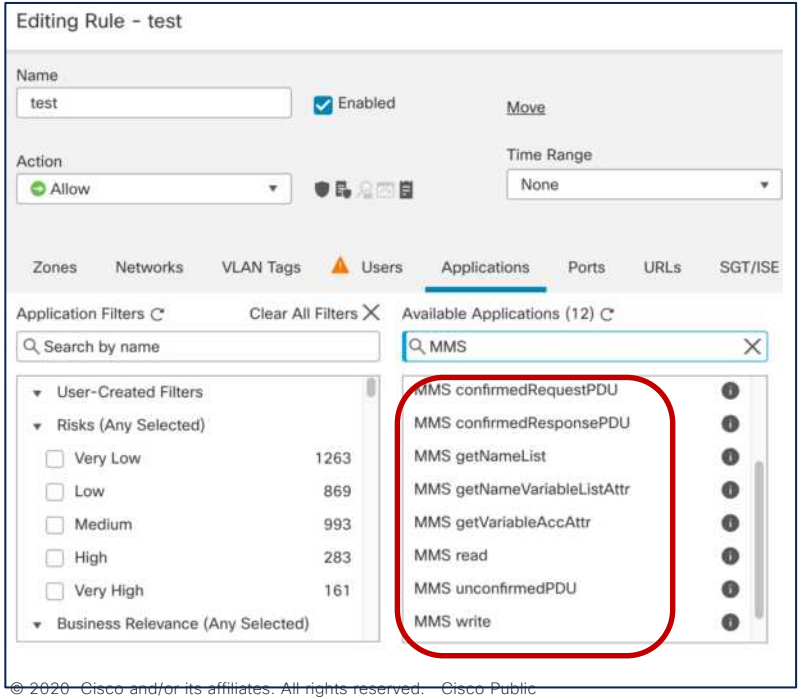
- request
- response
- notification
- response2

S7 Functions:

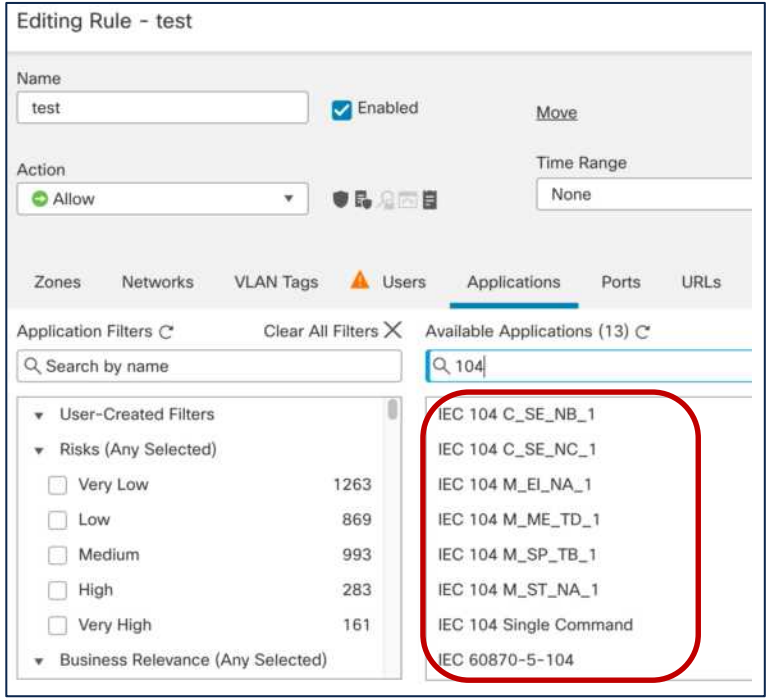
- explore
- createobject
- deleteobject
- setvariable
- getlink
- setmultivar
- getmultivar
- beginsequence endsequence
- invoke
- getvarsubstr

AppID – IEC-104, 61850 MMS

- IEC-61850 MMS



- IEC-60870-5-104



Industrial Ethernet Switching Update

IoT Industrial Switching portfolio Q1Y21

IOS-XE
IOS - IOS
Non IOS

Feature

IE 1000

- Lightly-managed
- Layer 2 only
- Din rail mount

IE 2000

- L2 or L3 (IP lite
- FastEthernet Downlinks
- Industrial, Enterprise Vertical
- Din rail mount

IE2000U

- L2 or L3 (IP services)
- FastEthernet Downlinks
- Utility Vertical

Din rail mount

IE3200

- Layer 2
- 2 GE uplinks
- 8 GE downlinks
- Din rail mount

IE3300

- Layer 2/Layer3
- 2 GE uplinks
- Up to 24 GE ports
- Modular
- Din rail mount

IE3400

- Layer 2/Layer3
- 2 GE uplinks
- Advanced Features
- Up to 24 GE ports
- Modular
- Din rail mount

IE 4000

- For all industries
- Layer 2 or 3 (IP service)
- 4 GE uplinks
- Up to 20 GE ports
- Din rail mount

IE 4010

- For all industries
- Layer 2 or 3 (IP service)
- 4 GE uplinks
- 28 total GE ports
- 19" rack mount

IE3300-10G

- Layer 2/Layer3
- 2 TenGig uplinks
- Up to 24 GE ports
- Modular
- Din rail mount

IE 5000

- Designed for all industries
- Layer 2 or 3 (IP service)
- 4 10 GE* uplinks
- 24 GE downlinks
- 19" rack mount

FastEthernet downlinks

Gigabit uplink and downlinks

10Gig uplinks

IE3400H has FE Model too

'*' -Selected Models

Catalyst IE3300 10G – new

Faster speeds, More power

PID	**IE-3300-8T2X**	**IE-3300-8U2X**	**IEM-3300-4M**
Base system or expansion module	Base System	Base System	Expansion module
Uplink Speed	**2 x 10Gig**	**2 x 10Gig**	NA
Downlink Speed	8 x 1Gig	8 x 1Gig	**4 x 2.5G (mgig)**
PoE Budget	NO PoE	**480W(Base +Exp)**	**360W**
PoE Ports	NO PoE	8	4
Per Port PoE	No PoE	**60W** (802.3bt type 3)	**90W** (802.3bt type 4)
IOx / CyberVision	**Yes**	**Yes**	NA
FCS	Sept/Oct 2020	Q1 2021	Q1 2021

Systems and modules IE3k2,IE3k3,IE3k4

Highly flexible architecture with a wide array of module choices

IE3200 fixed system

1. IE3200 copper fixed
2. IE3200 PoE+ fixed

Note: No support for Expansion modules

IE3300, IE3400 expandable systems

2x1Gig SFP and 8p Cu

2x10Gig SFP and 8p Cu

1. IE3300 copper basic modular system
2. IE3300 PoE/4PPoE basic modular system
3. IE3400 advanced modular system
4. IE3400 Advanced PoE= modular system

IEM3300, IEM3400 expansion modules

8p Cu

2p Fi + 6p Cu

16p Cu

2p Fi, 14p Cu

8p Fi

8p Fi

4p Cu

1. IEM-3300 8p copper
2. IEM-3300 8p PoE+
3. IEM-3400 Adv copper
4. IEM-3400 8p PoE+
5. IEM-3300 6p copper + 2p fiber mixed
6. IEM-3300 16p copper
7. IEM-3300 16p PoE+
8. IEM-3300 14p copper + 2p fiber mixed
9. IEM-3300 8p fiber
10. IEM-3400 Advanced 8p fiber
11. IEM-3300 4 Mgig (2.5Gbps) with 4PPoE type 4

Note: **IEM-3400 expansion modules only work with IE3400 base**
IEM-3300 expansion modules will work with IE-3400 base

IOS-XE SW Features for IE3x00

Available Now

Mfg installed IOS-XE version is 16.12.x

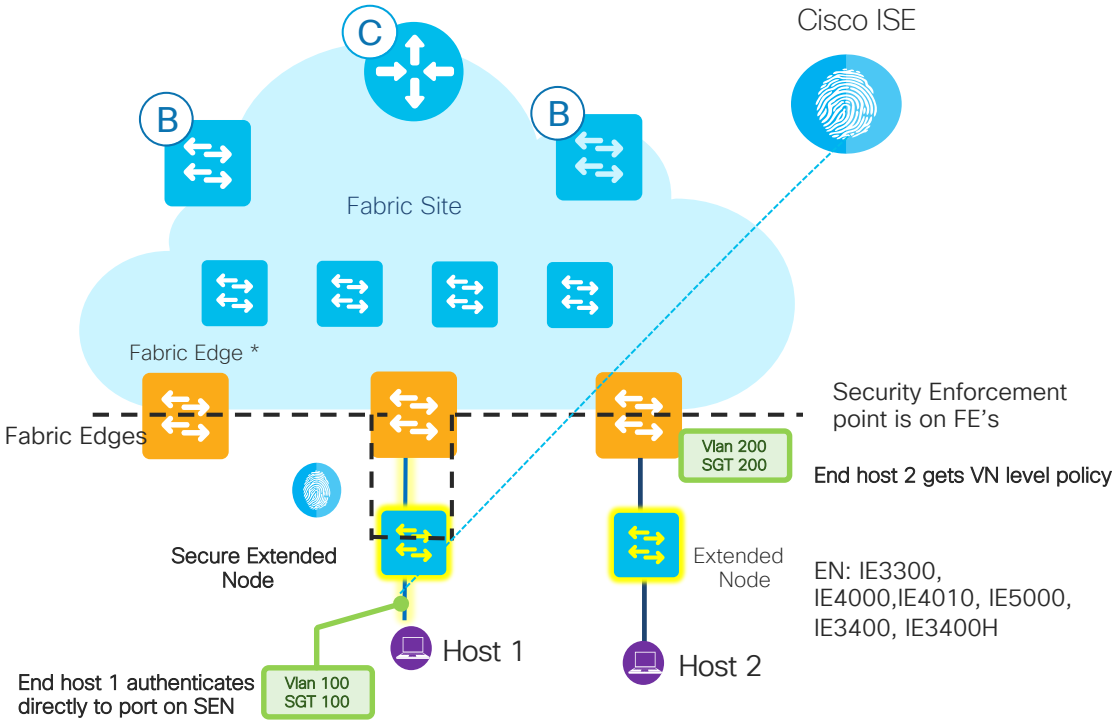
Features introduced 17.1, and 17.2, 17.3.1 (Available for Download now) - summarized

Note: **17.3 is target for "feature parity" with IE3000**

Feature	Release	More Information
EIGRP, ISIS, BGP, RIP	17.1	The remaining L3 dynamic routing protocols
Profinet	17.1	The SW stack is working, certified
IE3400H with Gig ports	17.1	Support for IE3400H Gig starts with 17.1
REP over Port channel	17.1	
HSRP, VRRP (v4, v6) PBR	17.2	Requires Network Adv.
IOx/ Docker, CyberVison Sensor	17.2	IOX and app hosting starts with 17.2
IPv6 FHS Features	17.2	RA Guard, DHCPv6 Guard
MRP (Automanager, 500ms profile), QinQ	17.3	Catchup with IOS Classic MRP support
HSR for SAN	17.3	IE3400 only; no HSR-PRP or HSR-HSR
L3 Mcast routing, (PIM-SSM), IPv6 mcast routing	17.3	Requires the Network Advantage license
IPv6 FHS	17.3	Source guard, Binding Integrity Guard,

Extended Enterprise (CVD)

SDA Security



- The **Policy Extended Node** will have 802.1x/MAB Authentication enabled to talk to ISE and to download the right vlan and Secure Group Tag attributes to the end points
- The **Policy Extended Node** performs security (SGACL) enforcement on egress interface.
  - Micro Segmentation
- End devices connected to **Extended Node** are put in default SGT group for the Virtual Network/VLAN at the FE port. Enforcement for Host 2 on FE egress port.
  - Macro Segmentation

Extended Node, Policy Extended Node & Fabric Edge

	Extended Node	Policy Extended Node	Fabric Edge
Layer	Layer 2 node	Layer 2 node	Layer 3 node
Macro-segmentation	VLAN to VRF mapping	VLAN to VRF mapping	Direct to VRF
Micro-segmentation	Industrial Ethernet IE5000 Catalyst IE3300 Rugged Series	Secure Group Tag (Inline Tagging)	Secure Group Tag (Inline Tagging)
Security Enforcement	Industrial Ethernet IE4010 Industrial Ethernet IE4000	SGACL At IoT Edge Catalyst IE3400 Rugged Series Catalyst IE3400H Heavy Duty Series	SGACL at Fabric Edge
Overlay encap/decap			VxLAN tunneling






Cisco IE Switch Selection for SDA deployment

Product Family	IE1000	IE2000 IP67	IE3200 Series	IE3300 Series (includes 10Gig)	IE3400/IE3400H Series	IE4000	IE4010 Series	IE5000 Series
SDA Support	No	No	No	Extended Node	Policy Extended Node	Extended Node	Extended Node	Extended Node
Cisco DNA Support	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes

2 DNA licenses available (Advantage, Essentials)

- Essentials is for pure networking buyers
- DNA Advantage required for SDA Extended Node or Policy Extended Node

PEN = Policy Extended Node
EN = Extended Node

PEN or EN	Switch License (term or perpetual)	DNAC License (term or perpetual)
EN	Network Essentials (perpetual)	DNA Advantage (term)
PEN	Network Advantage (perpetual)	DNA Advantage (term)
Cisco DNA Support	Network Advantage (perpetual)	DNA Advantage (term)

Redundancy Protocols – Industrial Settings

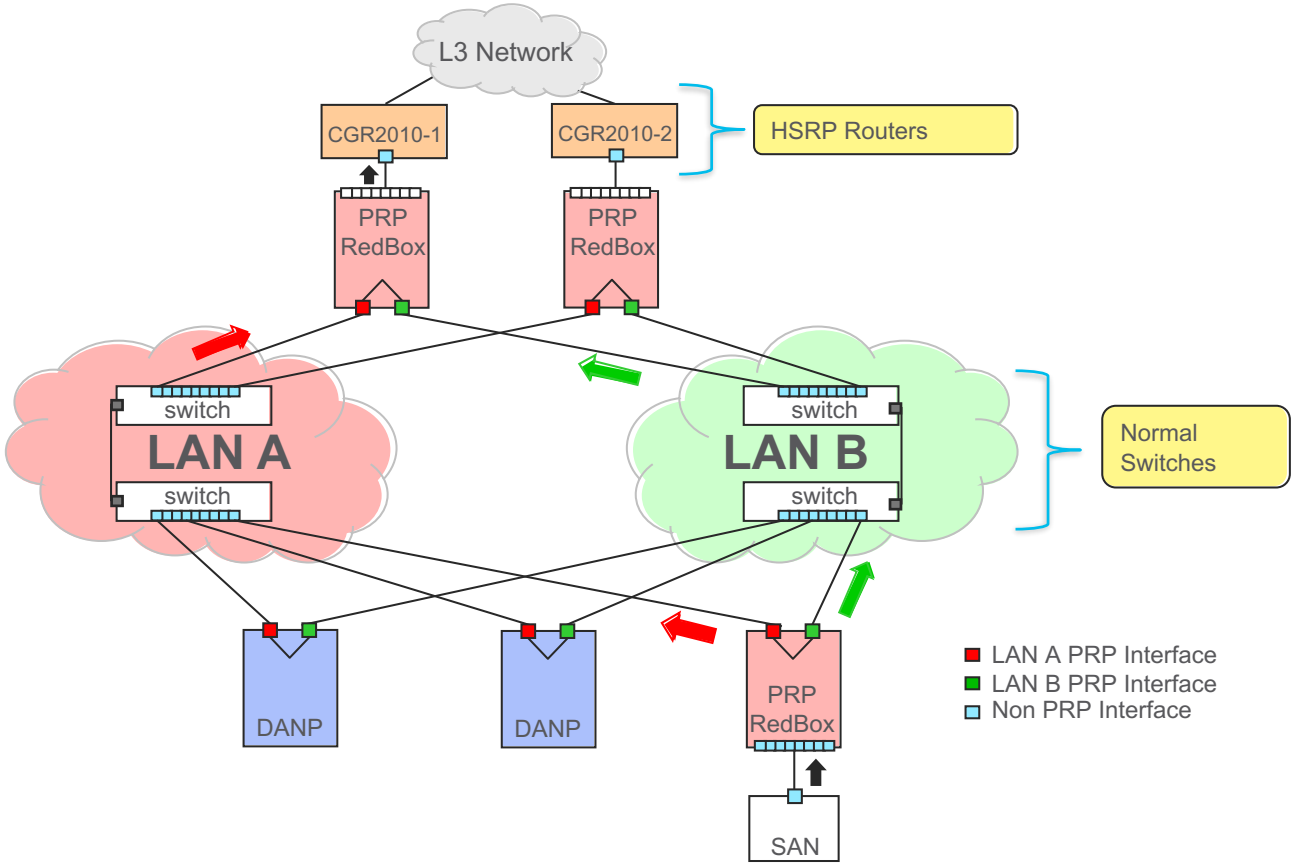
Most prevalent redundancy protocols for industrial uses.

Protocol	
RSTP / MSTP	Rapid Spanning Tree Protocol Multiple Spanning Tree Protocol
MRP	Media Redundancy Protocol
PRP	Parallel Redundancy Protocol
HSR	High-Availability Seamless Redundancy
REP	Resilient Ethernet Protocol
REP Fast	Resilient Ethernet Protocol (Fastmode)

- Fastest recovery
- Areas of expanding support
- Most design support inquiries
- Focus of this section

Parallel Redundancy Protocol (PRP)

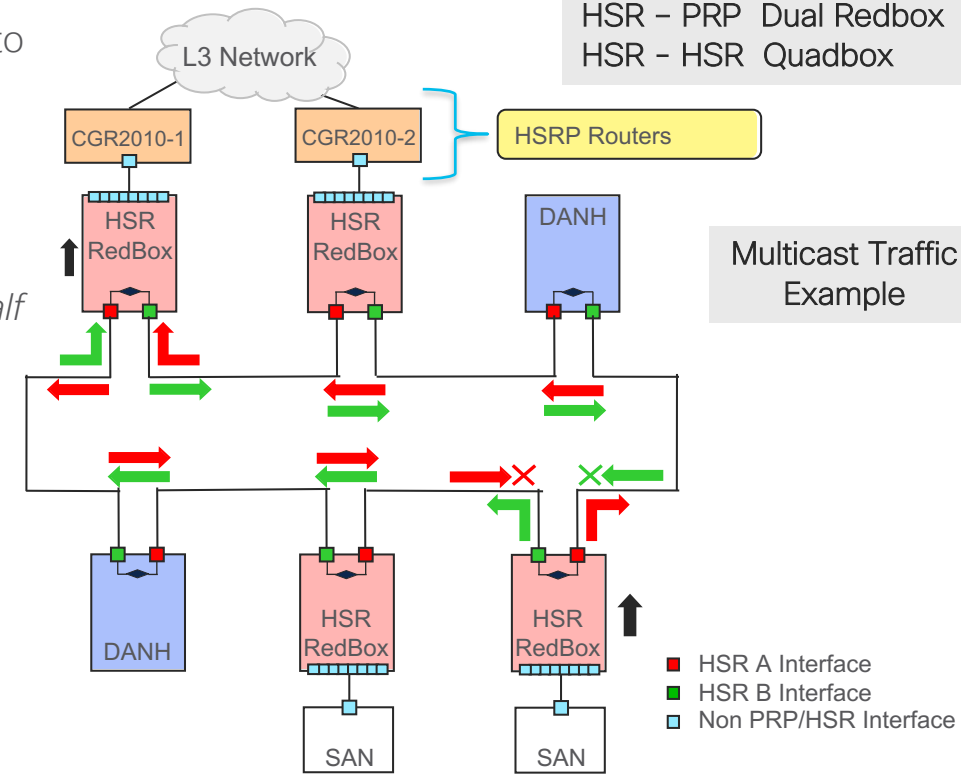
- **Lossless Redundancy** over 2 parallel networks
- LAN A & B Switches **do not have to understand PRP** protocol and **can support any topology**
- Need independent LAN A and LAN B
- **IEC 62439-3 Clause 4 Standard**
- **PRP Redbox** Supported on **IE-3400, IE-4000, IE-4010, and IE-5000, and select IE-2000u SKU(8,16 port)**



High-Availability Seamless Redundancy (HSR)

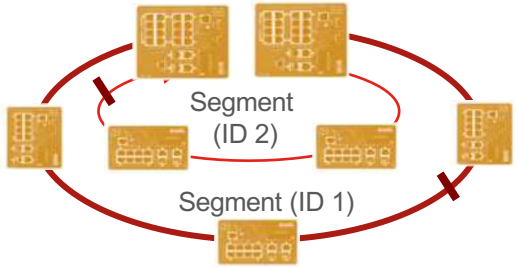
- **Lossless Redundancy** over Ring Topology
- All Nodes in Ring **MUST have special hardware** to support HSR
- **IEC 62439-3 Clause 5 Standard**
- Supported **IE-3400, 4000, 4010, 5000**
- Bandwidth available in ring is *reduced by up to half due* to duplicate packets.
  - Unicast: Receiving Node removes both frames from HSR Ring.
  - Multicast: Source Node ALWAYS removes frames after they both traverse entire ring.
- Vendor Inter-Operability/Implementation Challenges

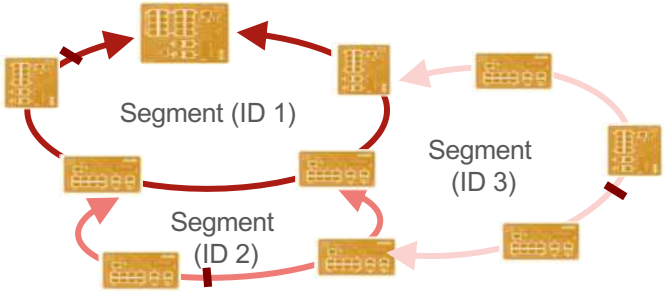
Note:
HSR – SAN Redbox
HSR – PRP Dual Redbox
HSR – HSR Quadbox

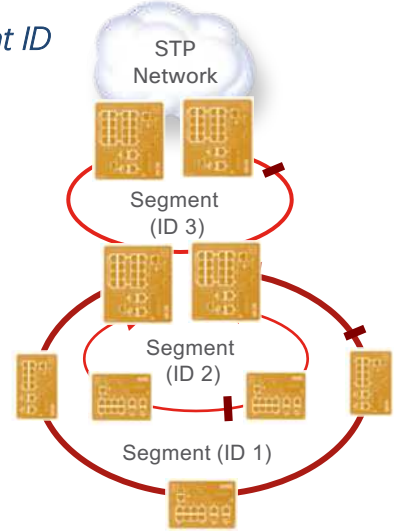


Resilient Ethernet Protocol (REP)

- REP – ring based redundancy solution for fast recovery from single failure
- *REP segment is a chain of ports* connected to each other and configured with the *same segment ID*
- The ports where the segment terminates is called the *Edge Ports*
- An *Alternate port* blocks VLANs to prevent loops and may be any interface in the REP ring





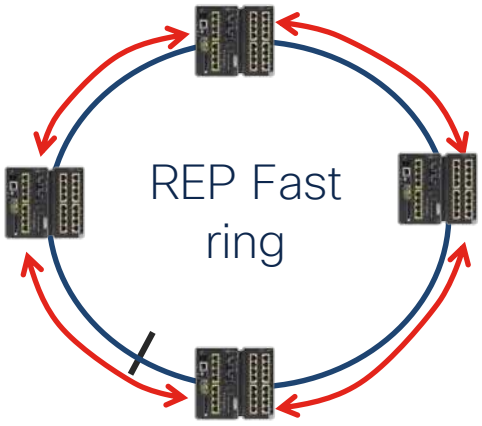


Fast and predictable L2 convergence
  REP → 50ms - 250ms
Easy to configure and troubleshoot
Support across Cisco products:
  REP → IE Switches, CGR2010 ESM, Catalyst, …
Co-existence with STP (TCN from REP to STP)
Optimal bandwidth utilization (VLAN Load balancing)

Does not replace Spanning Tree for complex layer 2 networks (mesh, tree)
Cisco proprietary
Supported on Layer 2 Trunk Ports and EtherChannel only
Does not protect against dual failure in the ring

REP Fast Overview – 25ms (or less) Recovery

- REP Fast is REP, with different link down reporting (beacons)
- **"Beacon based"** – not dependent on Link Down event
- Beacons sent to/from each REP node every **3ms**
  - Link down after 10ms (3 missed beacons)
- Works on Gigabit Copper and Fiber
- 'Edge no neighbor' works same
- REP Fast over EtherChannel supported (IOS-XE 17.1.1)
- **Only supported in the IE-3x00** family of products




```
REPSwitch2# show run
<snip>
interface GigabitEthernet1/1
 switchport mode trunk
 rep segment 1
 rep fastmode
!
interface GigabitEthernet1/2
 switchport mode trunk
 rep segment 1
 rep fastmode
```

Only 1 extra config command per interface

No changes to practical information and troubleshooting

```
REPSwitch2# show rep topology
REP Segment 1
BridgeName                        PortName   Edge Role
--------------------------------- ---------- ---- ----
REPSwitch1                        Gi1/2      Pri  Open
REPSwitch3                        Gi1/1           Open
REPSwitch3                        Gi1/2           Open
REPSwitch4                        Gi1/4           Open
REPSwitch4                        Gi1/3           Alt
REPSwitch2                        Gi1/2           Open
REPSwitch2                        Gi1/1           Open
REPSwitch1                        Gi1/1      Sec  Open
```

Layer 2 Redundancy Protocols Comparison

Protocol	Topology	# of Nodes	# of Max End-Nodes	Typical Convergence	Notes
RSTP/ MSTP	Any	Max nodes 255 Max 16 hops	MAC Address table	50ms-6s	• Not well suited for ring topology
MRP	Ring	50	MAC Address Table	200-500ms	• Interoperable with 3rd party switches that support IEC 62439-2
HSR	Ring	50	512	0ms	• Support on IE-4000, IE-4010 and IE-5000 • IEC 62439-3 Clause 5
PRP	Any	Unlimited	512	0ms	• Duplicate LANs, IEC 62439-3 Clause 4
REP (Cisco pty)	Ring	No limit	MAC Address table	**50-250ms**	• Depends on # of vlans, media, vlan load-balancing • Ring size & # of dynamic MACs impact recovery • Sub 50ms tested to ring size of 25 • **Copper Gigabit > 350ms recovery**
REP Fast (Cisco pty)	Ring	No limit	MAC Address table	**<25ms**	• **IE3x00 only; beacon based** • Ring size & # of dynamic MACs impact recovery • Solves Copper Gigabit for REP

Cisco IoT Routing

Industrial Routing Portfolio

Smart City, Utility (FAN), Transportation, Plant

Plant, WAN,SA

WAN

Features

IR807

- IP30
- 2x serial
- 2x 10/100BaseT
- Security
- 4G,3G,2G uplink
- 2 SIMs
- Low power (6,7W)

IR809

- IP30
- 2x serial
- 2x 10/100/1000BaseT
- Security
- 4G,3G,2G uplink
- 2 SIMs
- Motion detector
- IOX

IR 829

- IP54
- Raw Sockets
- Protocol Translation
- Security
- 4FE Copper
- 1GE Fiber
- WiFi, PoE
- IOX

IR1101

- Modular IP30
- Slots for WAN
- Security
- 1x RS232
- 4FE Copper
- 1x combo GE Fiber/ Metallic
- IOX

CGR 1120

- IP30
- **Modular**
- Raw Sockets
- Protocol Translation
- Security
- 6FE Copper
- 2GE Fiber
- WiFi
- **NAN modules**
- IOX

CGR 1240

- **IP67**
- **Modular**
- Raw Sockets
- Protocol Translation
- Security
- 4FE Copper
- 2GE Fiber
- WiFi, PoE
- **NAN modules**
- IOX

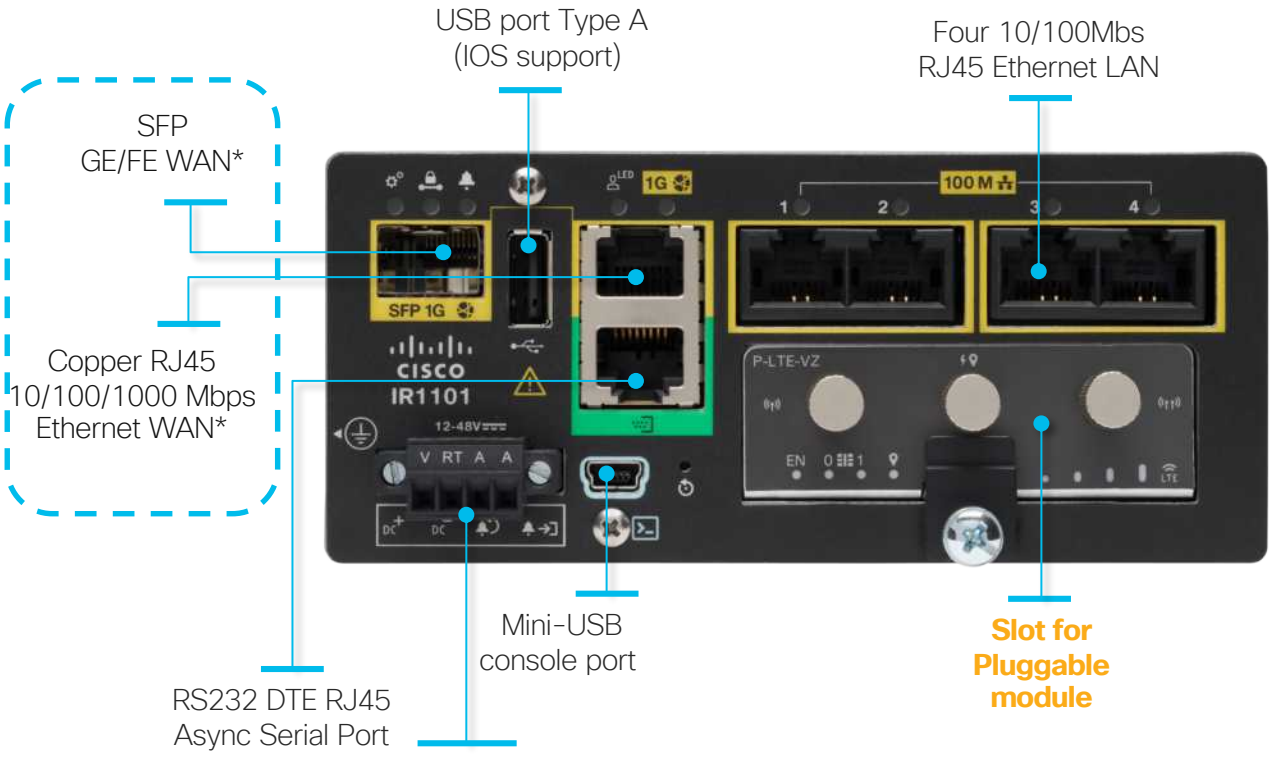
CGR 2010

- **Modular (4 slots)**
- Raw Sockets
- Protocol Translation
- Security
- MPLS L3 VPN
- 2Combo GE
- Ethernet Modules
- Serial
- xDSL

ASR 902/3 ASR920 (IoT cards)

- Modular (6 slots) – 3RU
- Raw Sockets
- ISSU
- **128 Gbps, Low Latency**
- Ethernet, Serial, E&M,
- E1/T1, STM-1
- **MPLS IP, MPLS TP, VPLS**
- PseudoWires
- SyncE, IEEE 1588,

IR1101 – Base Platform – Compact and Flexible



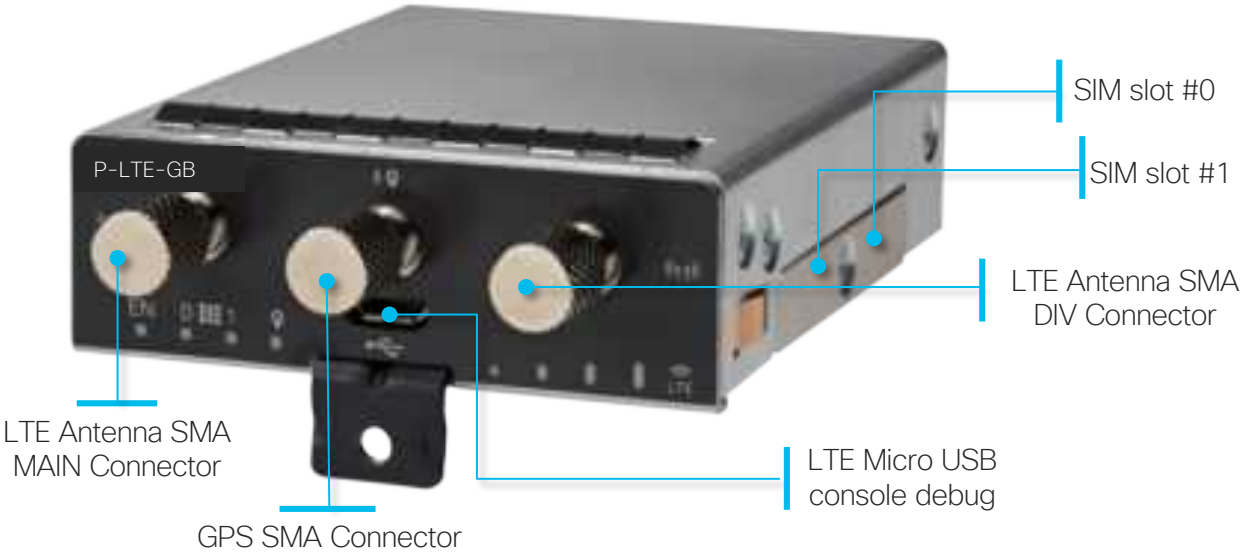
Pluggable LTE Module
(shared with C1100)

Dual SIM slots
Micro SIM format

** Copper/Fiber Combo WAN interface.*

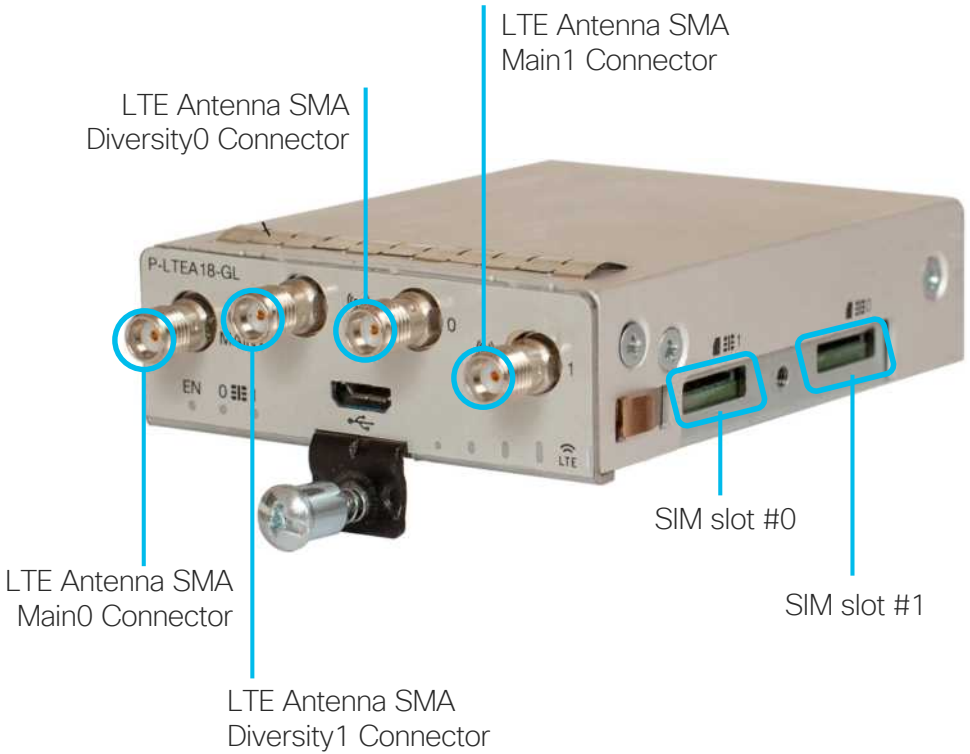
IR1101 Cellular Pluggable Module

- Shared Cellular pluggable modules with Enterprise ISR1100 and other platforms
- Smaller form factor and Cisco Pluggable technology provide additional protection investment and flexibility
- **P-LTEA-EA** - LTE Advanced 3GPP **Category 6** : Bands LTE : 1-5, 7, 8, 12, 13, 20, 25, 26, 29, 30, a 41
- **P-LTE-GB** - LTE **Category 4**: Bands 1,3, 7, 8, 20, 28 and GPRS/EDGE: 900/1800



LTE Category 18 Pluggable Module

- Shared Cellular pluggable modules with Enterprise ISR1K/4K and other platforms
- **No GPS** port available on P-LTEAP18-GL
- P-LTEAP18-GL must be installed on IR1101 base, **not on expansion module**
- P-LTEAP18-GL - LTE Advanced Pro: Bands LTE 1-5, 7, 8, 12-14, 17, 18-20, 25, 26, 28-30, 32, 38-43, 46, 48, 66, a 71.
- Private LTE Bands
  i.e.: B48(CBRS), B42/B43 (pLTE, i.e. Germany), B66, B71
- **4x4 MIMO**
- **LTE Cat 18**
  1.2 Gbps downlink
  150Mbs uplink
- Dying Gasp

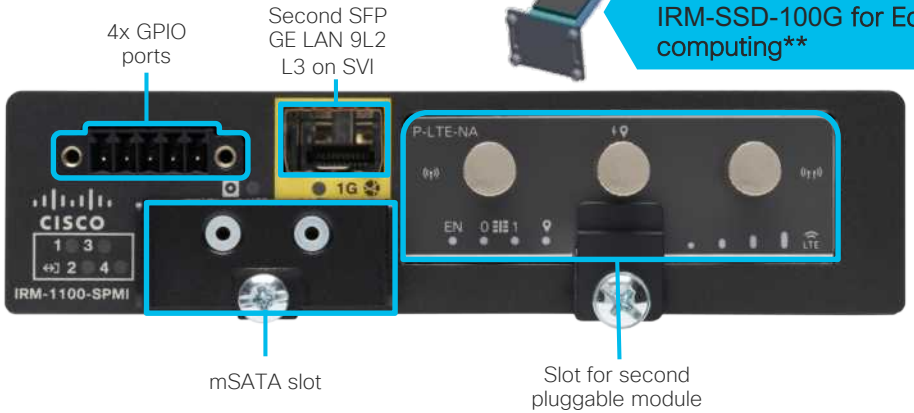


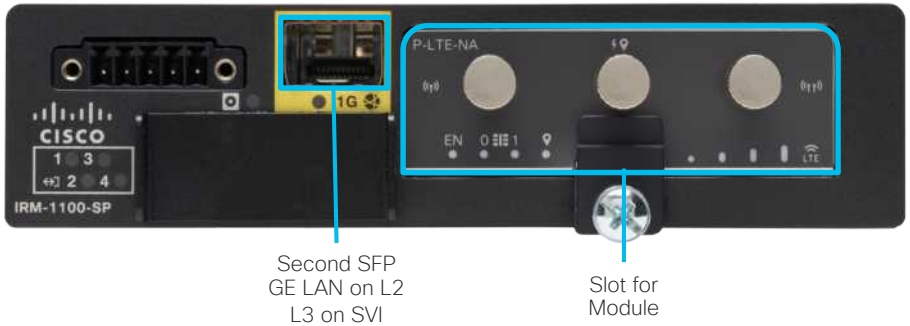
Expansion module: IRM-1100-SPMI,SP

Expansion Module	Description
IRM-1100-SPMI	• 4x GPIO ports mSATA slot • SFP GE LAN (L2) • Slot for pluggable module
IR1101-SSD-100GB IRM-SSD-100G	• 100GB SSD drive (old/new SKU)

Expansion Module	Description
IRM-1100-SP	• SFP GE LAN (L2) • Slot for pluggable module

IR1101-SSD-100GB/
IRM-SSD-100G for Edge computing**





*** SDWAN doesn't support edge compute (future)*

NEW! 17.4.1

DSL SFP for IR1101

Certified for select countries in EMEAR

SFP-VADSL2+-I

Industry-grade

ADSL2, ADSL2+, VDSL2

(Annex A, B, C, M, J, L)

-40° C to 60° C

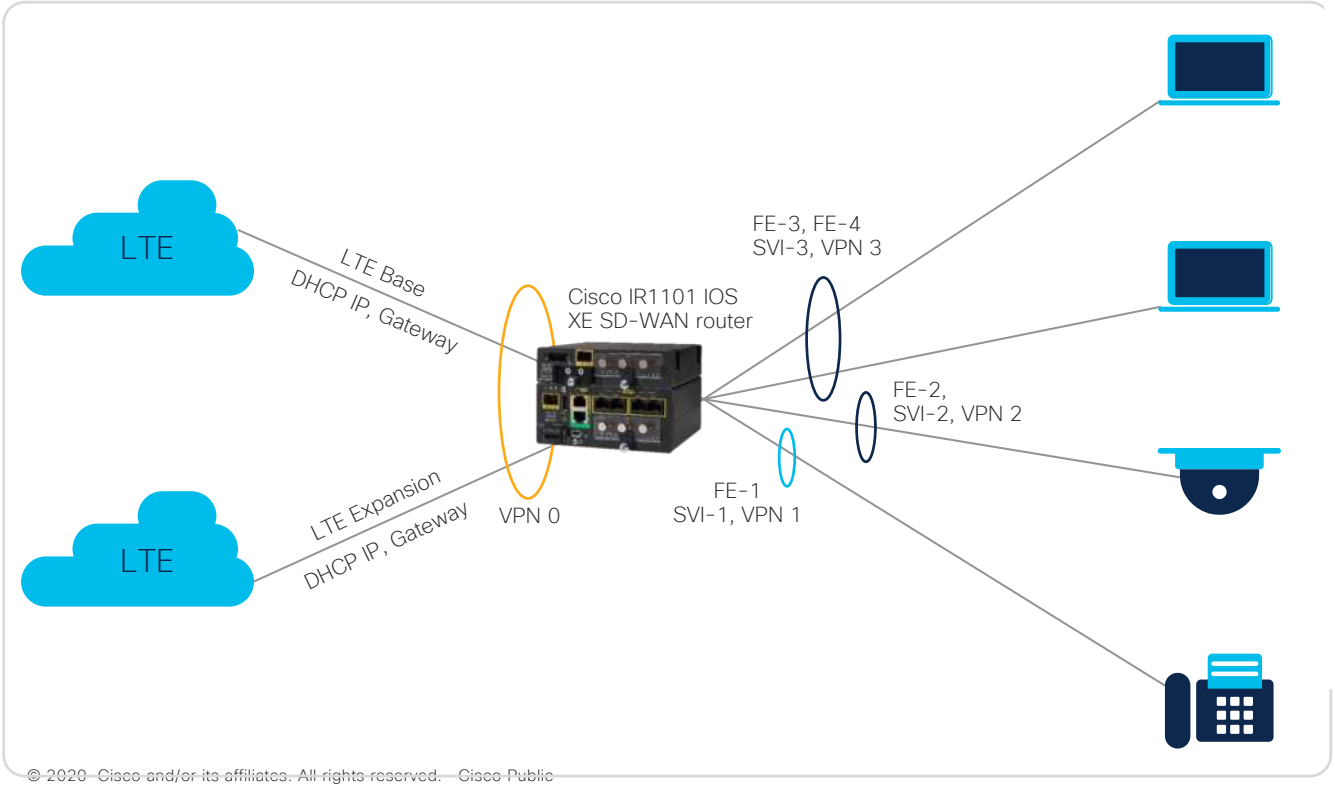
EMI Certifications

DSL management integrated into Cisco software

PID's will be orderable for Europe (selected countries), UK in Jan 2021

IR1101 with SD-WAN

Single WAN router, dual WAN redundancy with dual LTE



Key features

- Up to four endpoints
- High WAN redundancy
- Dual LTE
- Single IR1101 router

Use case examples

- ATM booths
- Unmanned payment centers
- Remote POS

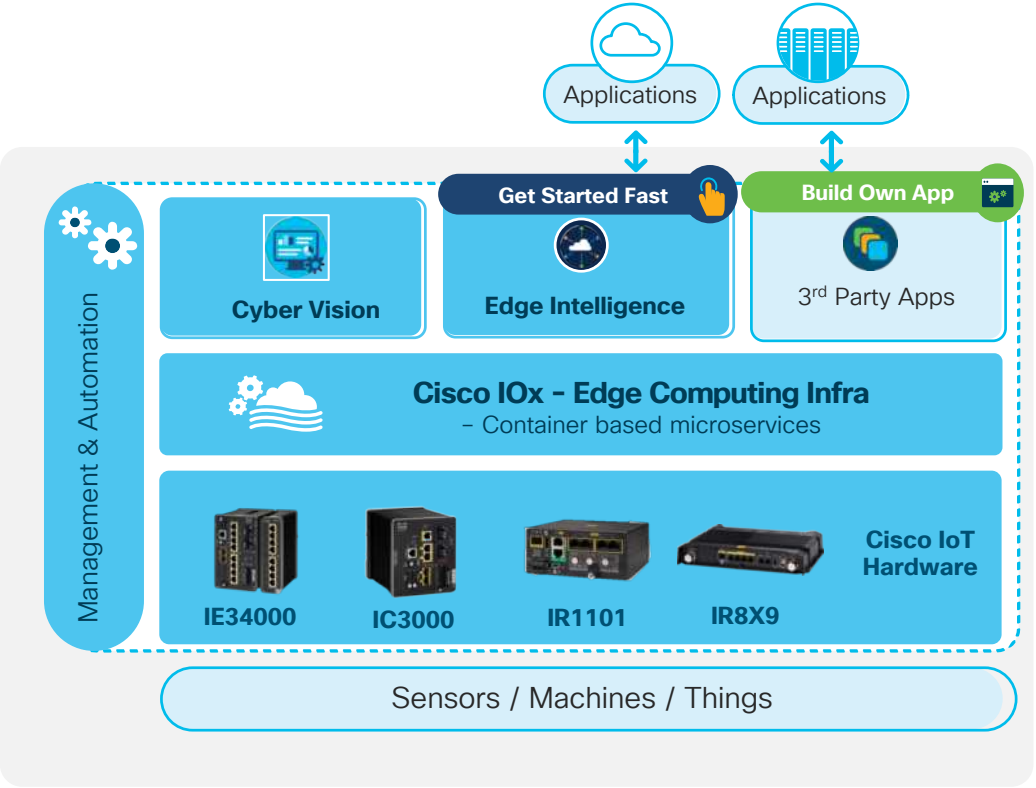
Cisco Edge Compute

IOX, Edge Intelligence

Cisco IOx

(IOS and Linux)

- Cisco IOx is **secured application hosting environment**
- Hosts Virtual Containers
- Supports **docker tooling** for development
- Provisions services like GPS & Secure Storage, for applications
- **Local Manager** for application monitoring and resource usage
- APIs for Application Management (GMM, FND, FD, DNA-C,...)



- IOx Software stack bundled with the IOS/firmware image
- No license Needed to Enable IOx on the Edge Device

HW Resource Comparison

Platform	CPU Architecture	CPU (Units)	Memory (MB)	Storage (MB)	Peripherals	IOx Version(s)
IE3400	ARM 64-bit (aarch64)	1400	2048	3800[1]	-	2.0
IE4000[2]	PPC 32 bit (ppc)	1035	512	256	-	1.7
IR1101	ARM 64-bit (aarch64)	1255	862	512	1 Serial port	1.8, 1.9, 2.0

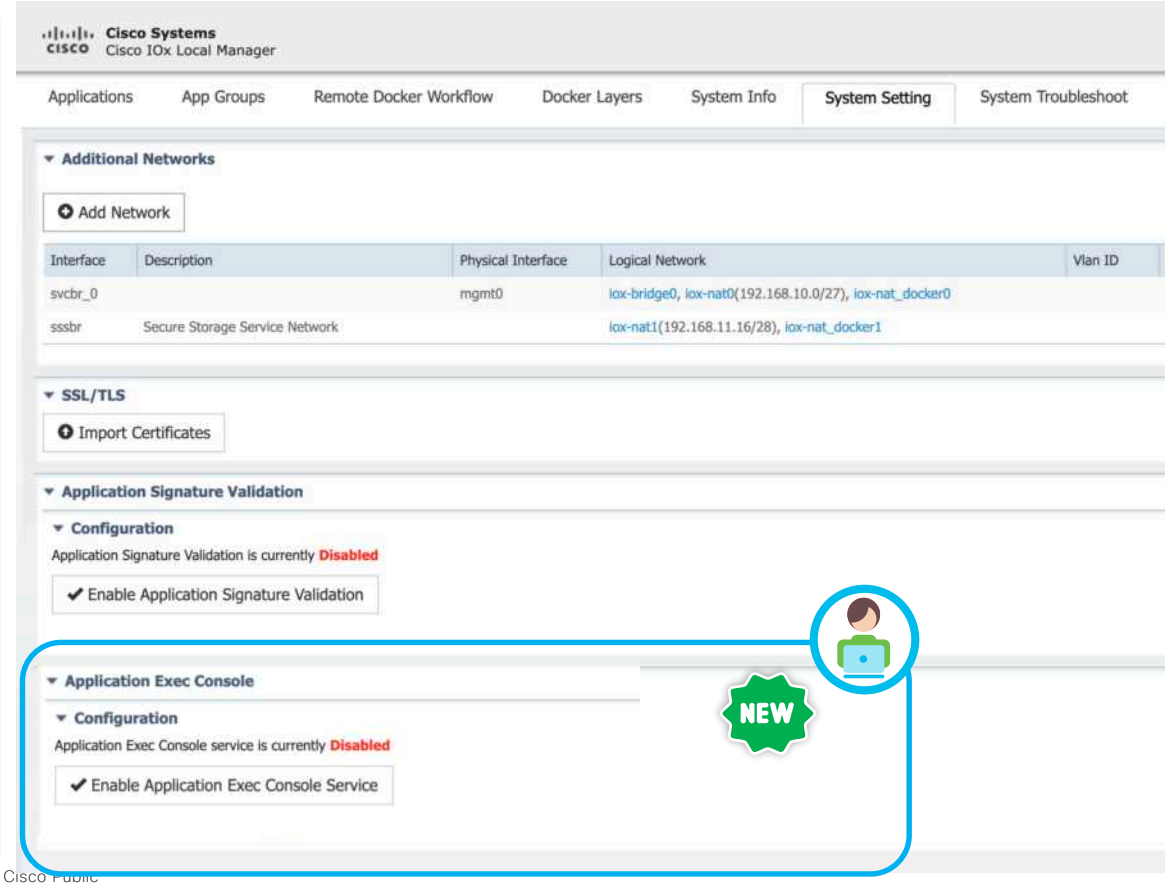
[1]on SD-CARD (mandatory, SD-IE-4GB)
[2]Suport for IOx on **IE4000** has ended with release **15.2.7E0s**

App Console Access (IOx-LM)

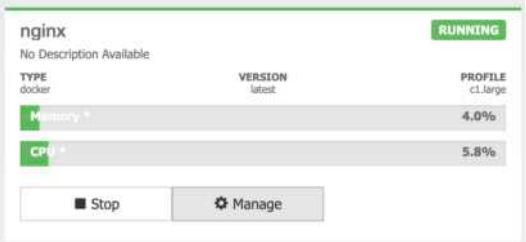
Step 1

Enable “**Application Exec Console**” Service on IOx-LM in System Setting Tab

IC3k, IR8x9, CGR1K-Hokkaido (Native Docker, Docker Type, LXC and VM Apps)

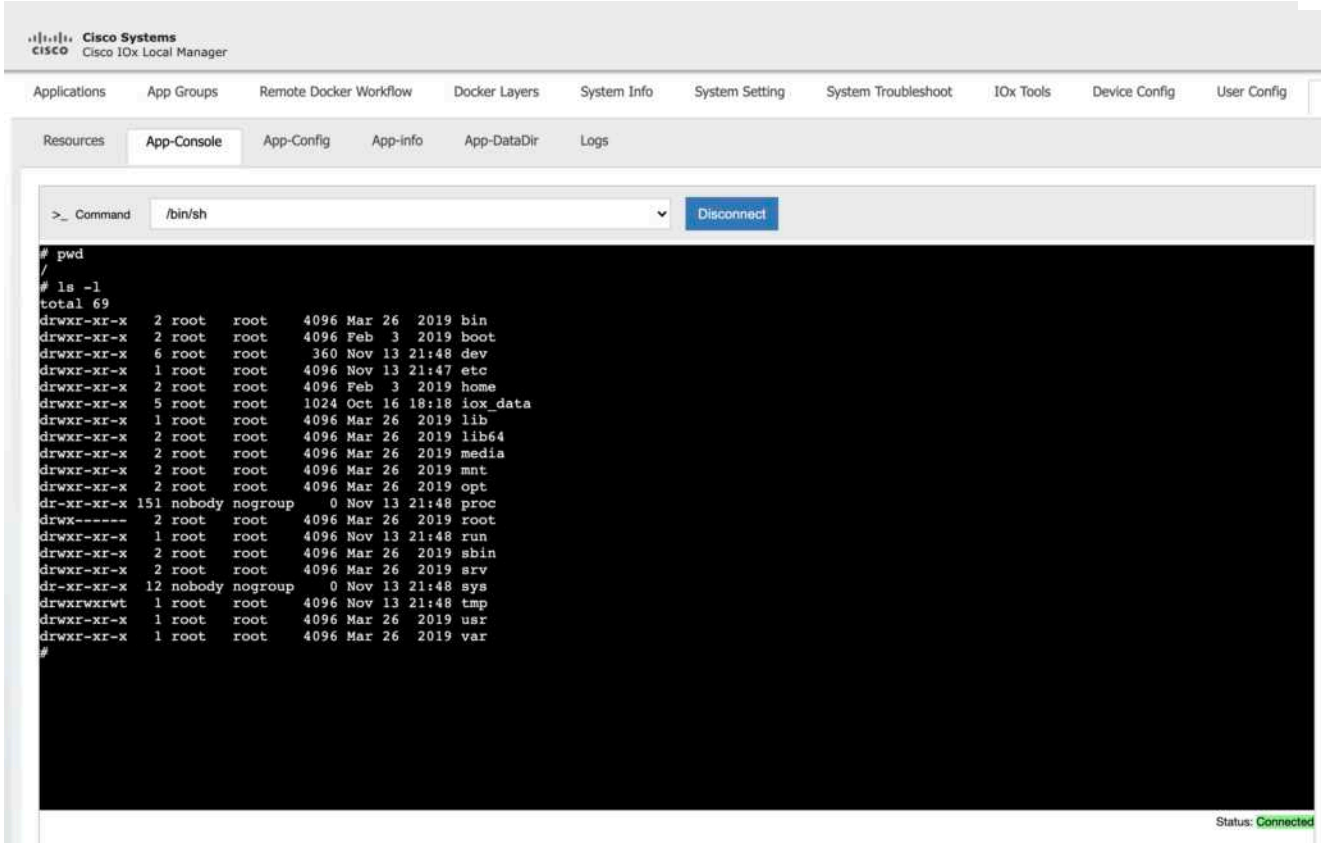


App Console Access (IOx-LM) Cont.



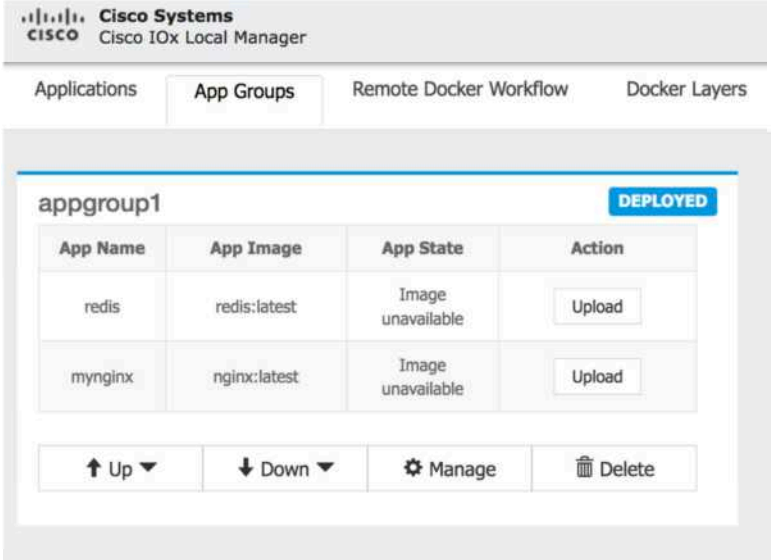
Step 2

Use App “Manage” button to navigate to “App-Console” Tab.



IOx App Groups (IOx-LM)

- IOx App Groups => Multi-Container Application Support
- Uses YAML way to capture - Container Image, network, resource and dependencies Information



[App Groups Documentation on DevNet]

```
version: '3.3'

services:
   redis:
     image: redis:latest
     volumes:
       - db_data:/var/lib/mysql
     restart: on-failure
     environment:
       MYSQL_ROOT_PASSWORD: somewordpress
       MYSQL_DATABASE: wordpress
       MYSQL_USER: wordpress
       MYSQL_PASSWORD: wordpress
     networks:
       - front_end
       - back_end
   mynginx:
     depends_on:
       - redis
     image: nginx:latest
     ports:
       - "9000:80"
     restart: on-failure
     mem_limit: 64m
     environment:
       WORDPRESS_DB_HOST: db:3306
       WORDPRESS_DB_USER: wordpress
       WORDPRESS_DB_PASSWORD: wordpress
       WORDPRESS_DB_NAME: wordpress
     networks:
       - front_end
volumes:
    db_data: {}
networks:

   front_end:
     external:
        name: int1
   back_end:
     external:
        name: iox-nat_docker0
```

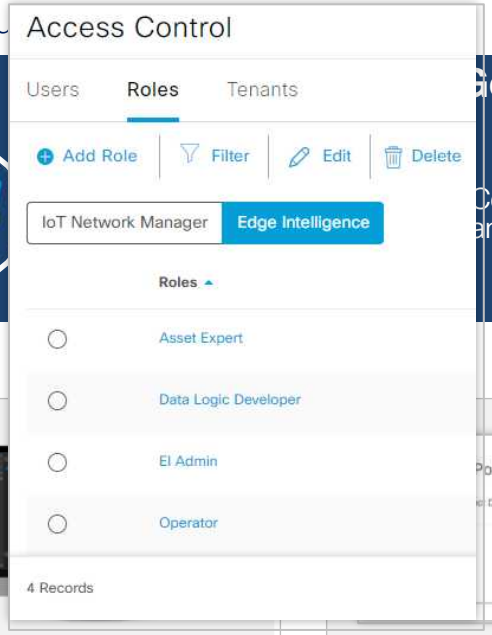
Cisco Edge Intelligence

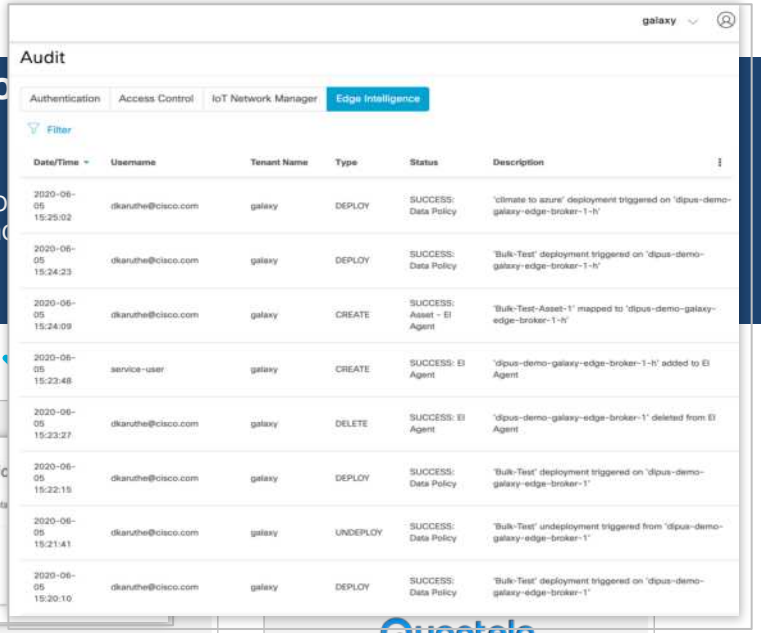
Simplifying the edge to multi-clou

Extract

Seamlessly extract data from disparate sources

Pre-Integrated with Solution





Modbus

OPC UA

MQTT

...

Built on industry's well accepted & developer-friendly tools

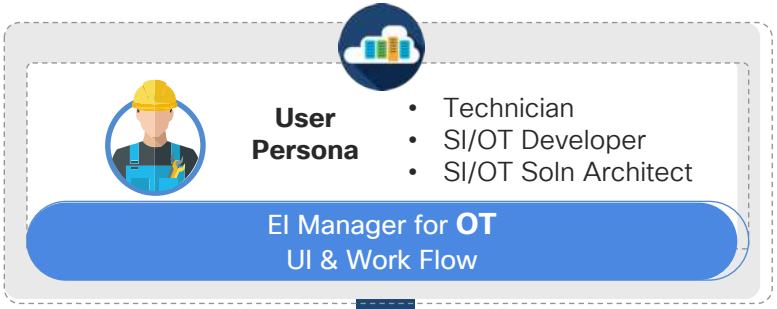
Policy control at device and attribute level on raw or transformed data

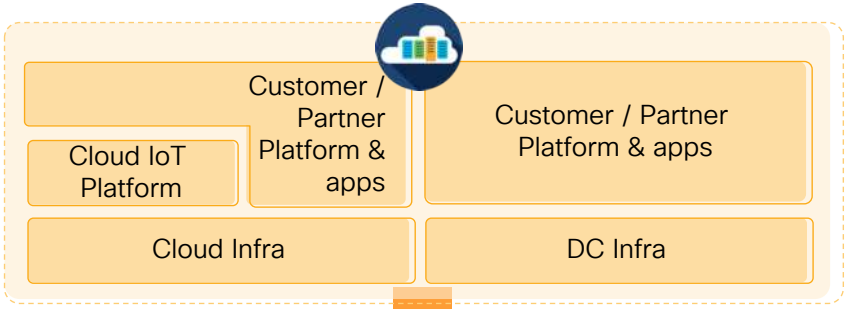
Quantela

MQTT

... more to come

Cisco Edge Intelligence

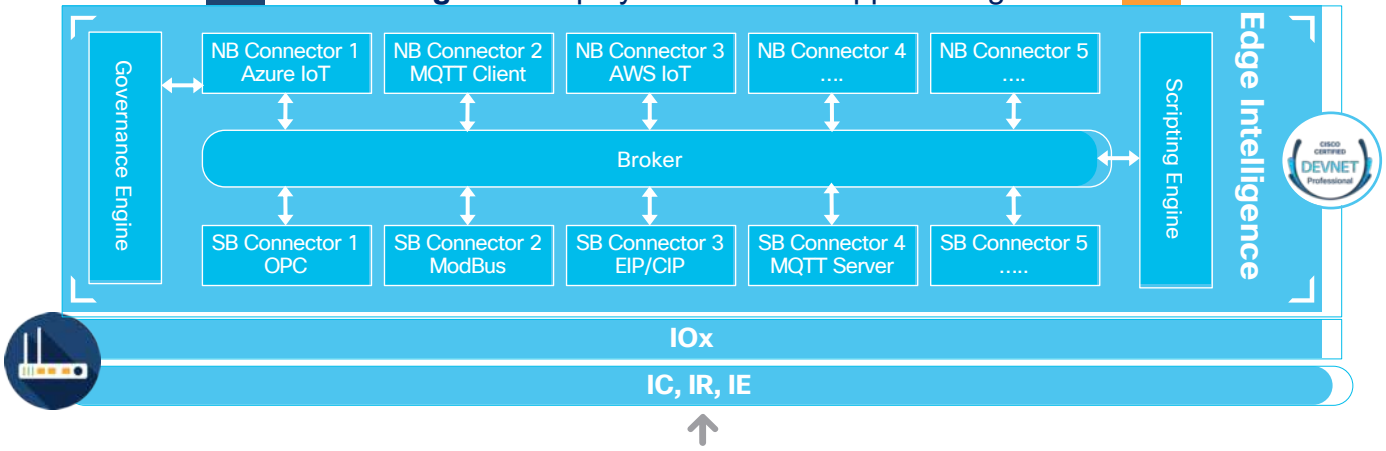


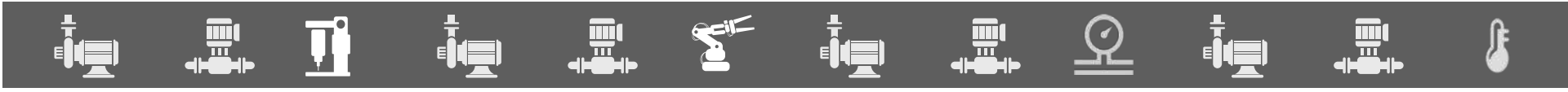


Control Path

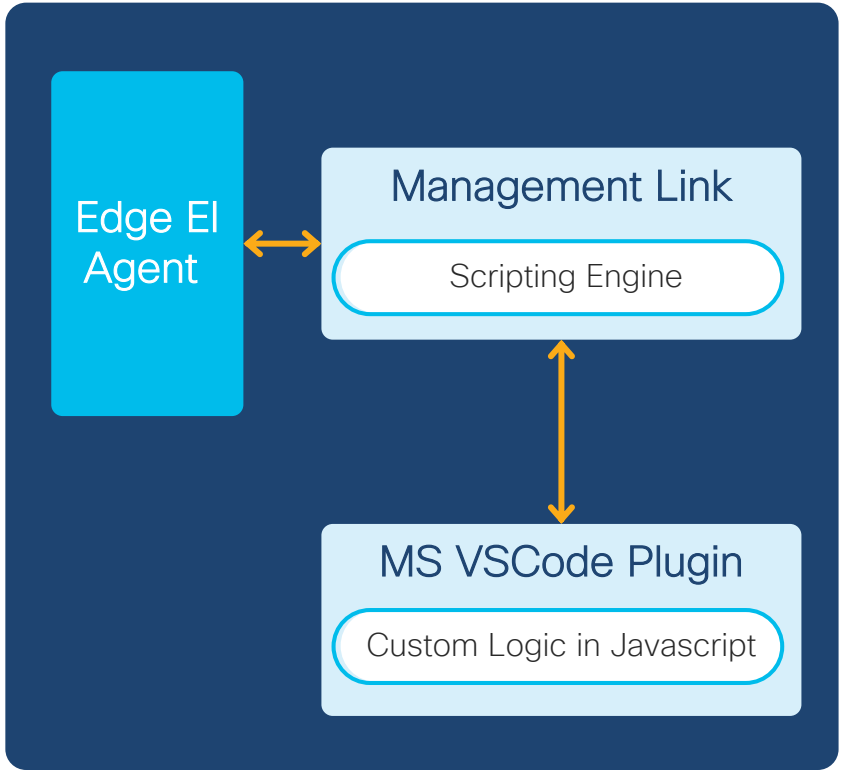
Data Path

EI Agent is deployed as an IOX-App-Package

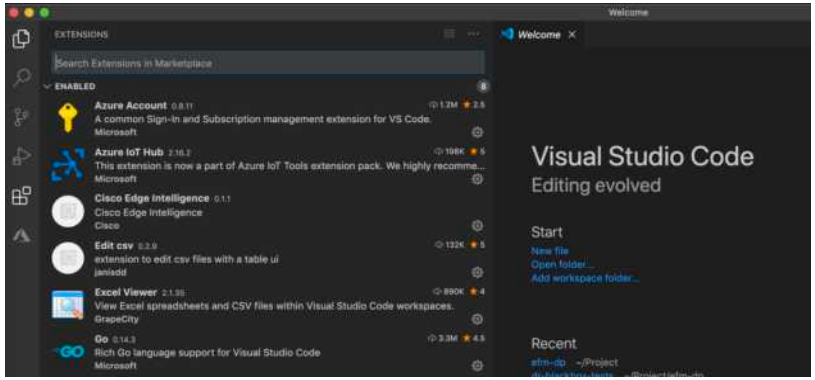




Data Transformation

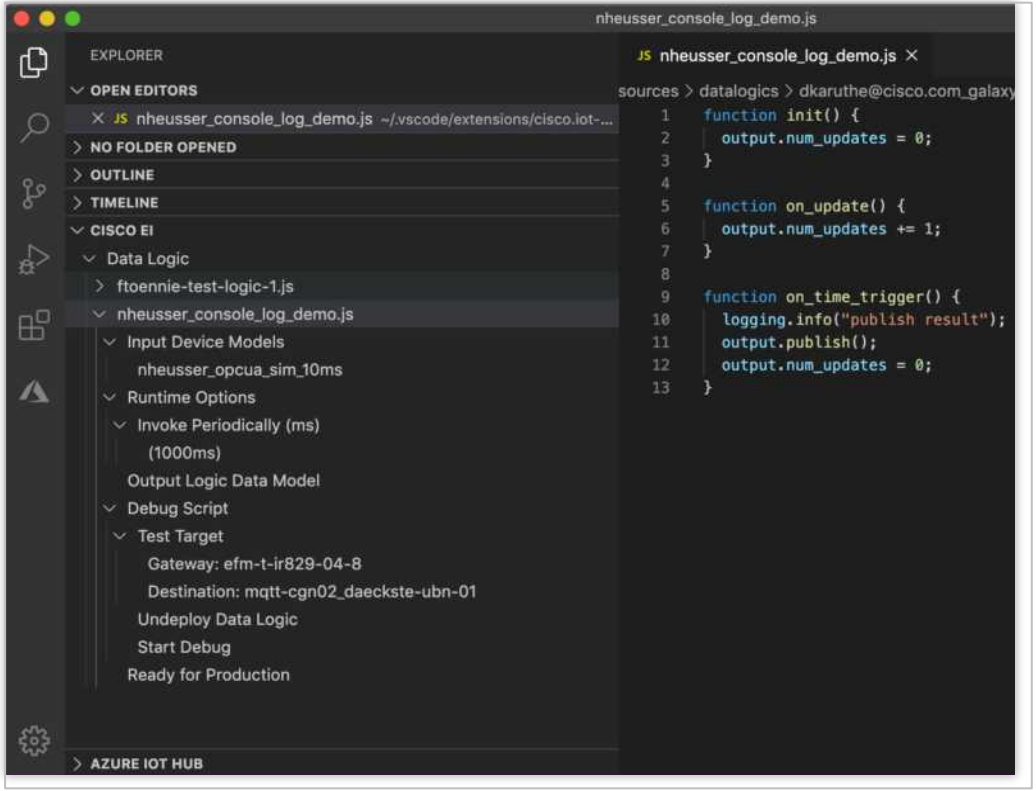


1. Development Tool – Microsoft Visual Studio Code
2. Plugin available in marketplace – "Cisco Edge Intelligence"
3. EI user should have "Data Logic Developer" role



Script Development

- Create a new Data Logic
  - Input Asset model
  - Runtime options
  - Output model
- Test and debug the script
- Upload to EI Cloud.

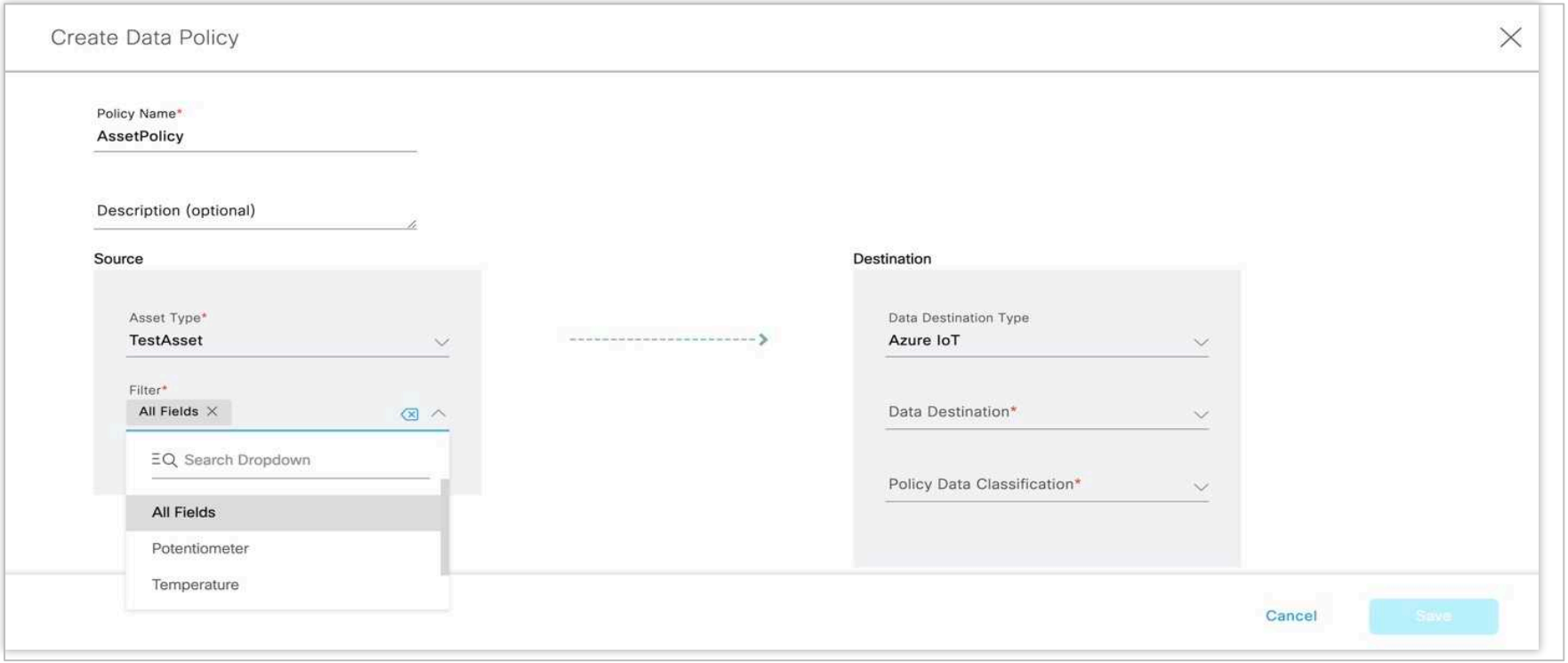


Governance via Data Policy – Overview

- End-to-end data flow definition
- Select the source and destination
- Two types
  - Asset based – send data from device without transformation
  - Data Logic based – send data after transformation via logic script
- Granular control over data policy deployment

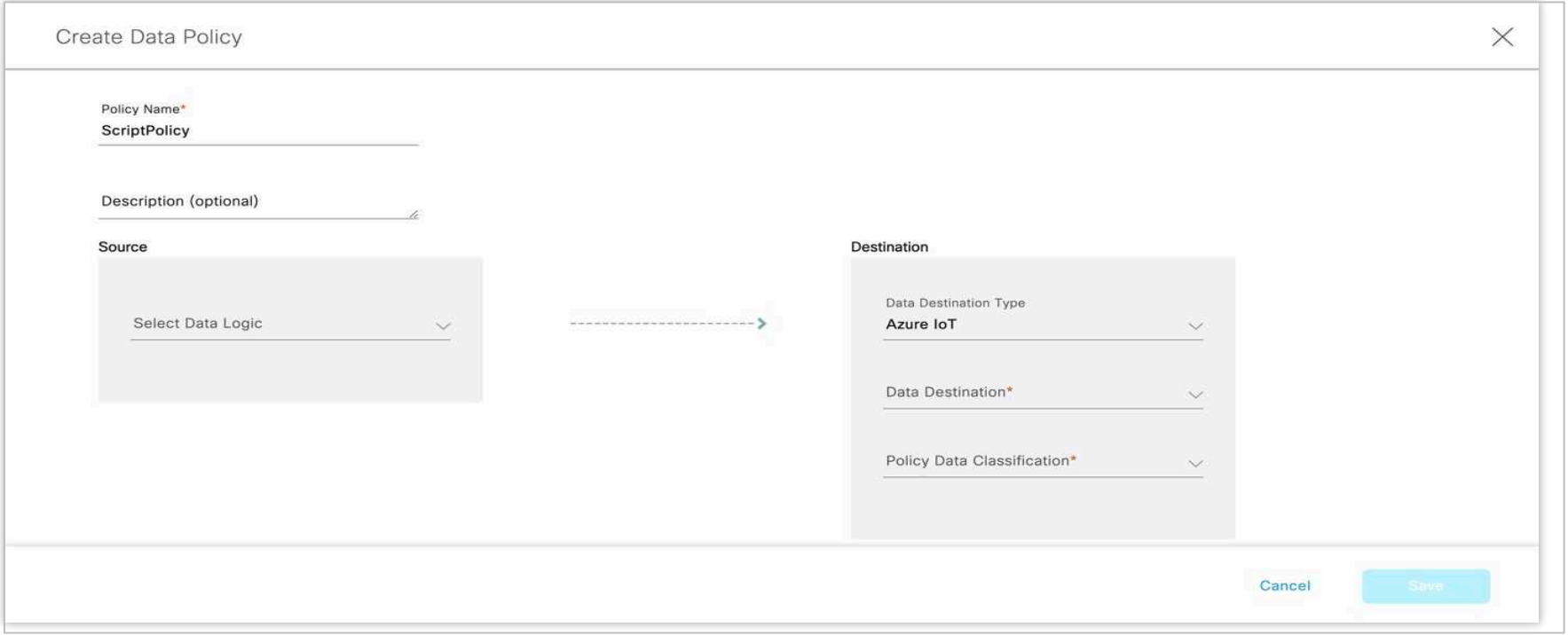
Asset based Data Policy

- Data Policy connecting Asset to Destination
- Ability to filter individual data attributes from Asset



Data Logic based Data Policy

- Very similar to Asset-based Data Policy
- Data Logic connects previously configured Data Logic to



Data Policy – Deployment

Select 1 or many EI Agents for policy deployment

Monitor Deployment and Runtime status

Guide me!

Deploy - 'WaterAverageDemo' Data Flow

Data Policy

Data Policy Requires at least **1 Asset of model WaterSensor** which is connected to EI Agent(s).

Select EI Agent(s) and start deployment.

IR829_FTX2020805U

Deploy

Search Gateway Agent

IR829_FGL21112612

IR829_FTX2020805U

Find

EI Agent	Deployment Status	Policy Status	Error Message
This policy has not been deployed on any EI Agent(s).			

IR829_FTX19438012-SJC

Cold Storage All Variables

Running

WaterAverageDemo

Running

Source

Number of Device(s) Operational	1 | View Operational Device(s)
Number of Device(s) Not Operational	0 |

Destination

Destination Connection Status	Operational
Last Time Data Sent To Destination	-

Data Logic

Data Logic Status	Active
Last Time Data Received from Data Logic	-

Industrial Asset Vision

LoRaWAN

What is **LoRaWAN?**

Unlicensed Spectrum

- Global ISM band, 868/915MHz, 2.4GHz

Long Distance Coverage

- Up to 15 kms in rural areas

Low Data Rate

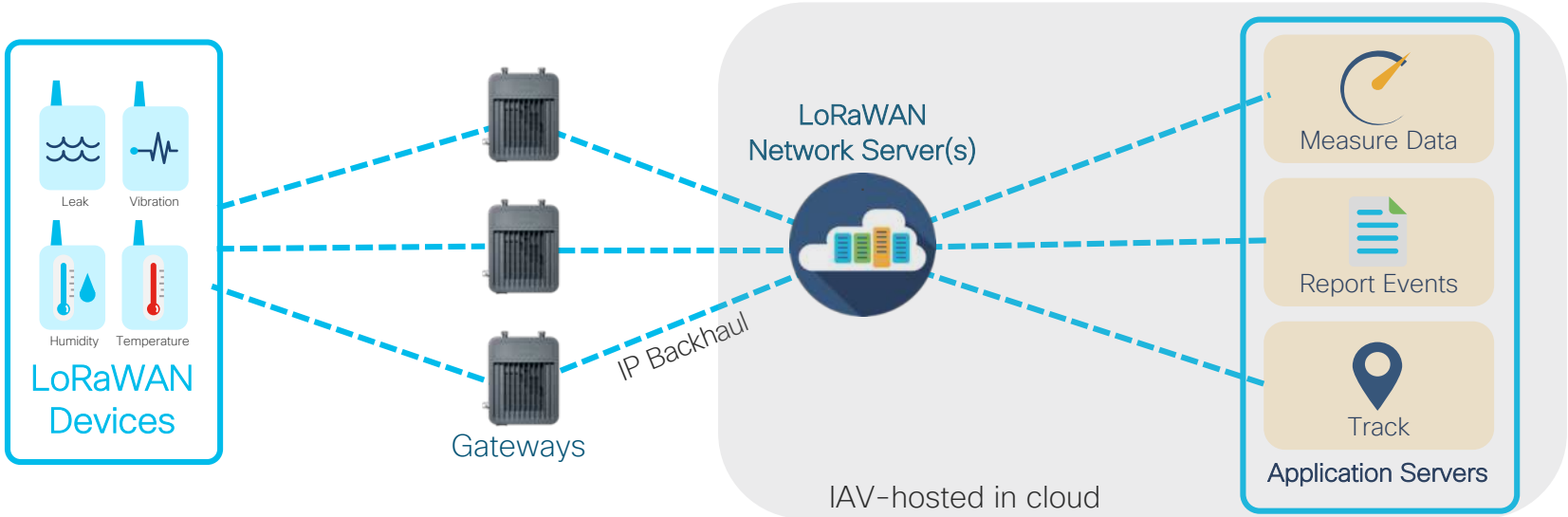
- 300 bps to 5.5 kbps
- Adaptive per distance

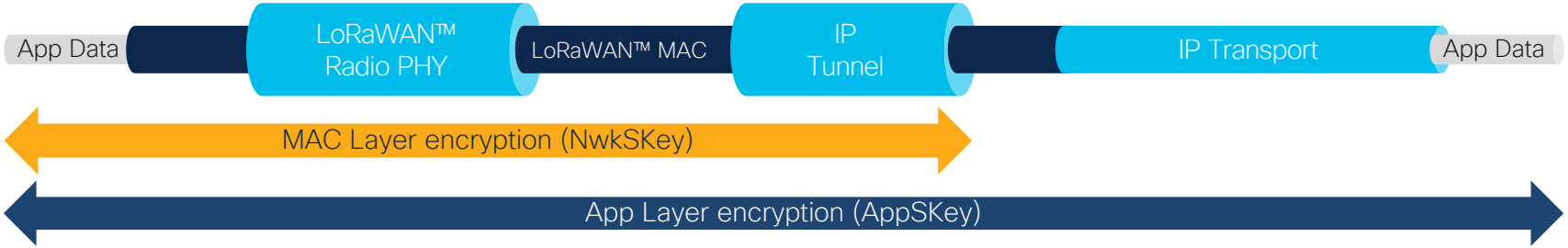
Low Power Consumption

- Battery powered endpoint
- Up to 10 years lifetime

A disruptive wireless technology for long range and low power consumption

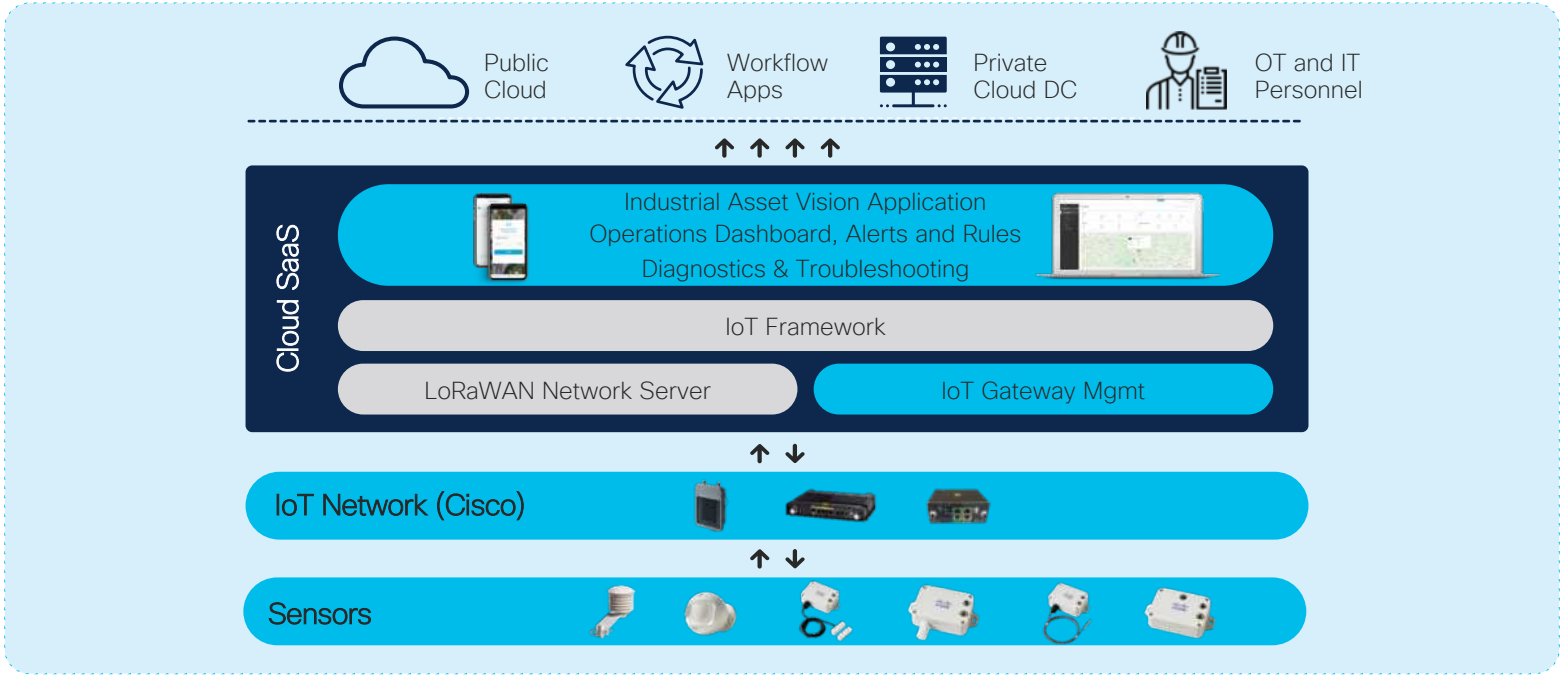
LoRaWAN End-to-End Architecture





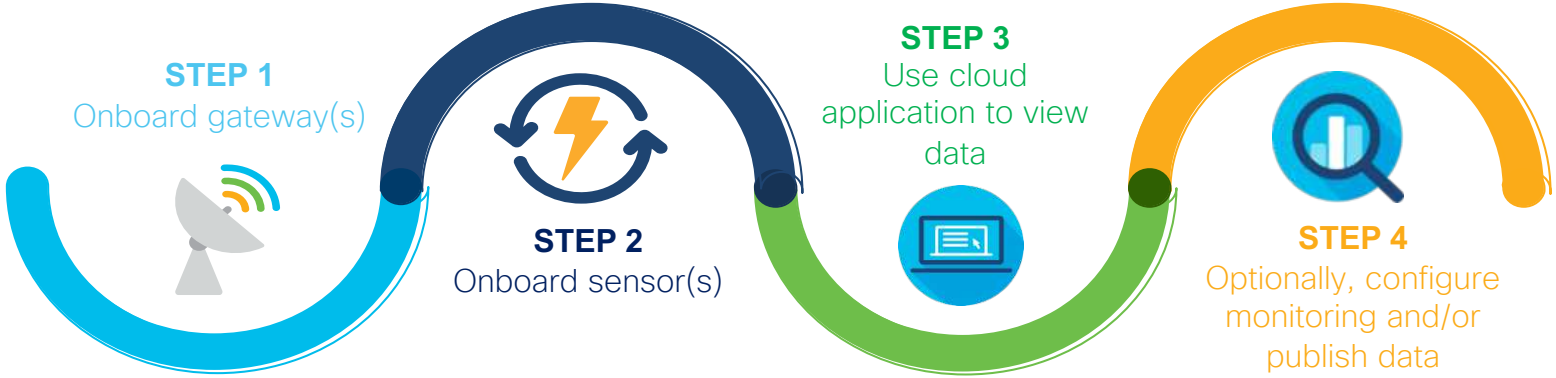
Note: IAV encompasses all stages of the traditional LoRaWAN architecture shown above

IAV Technology Stack



Industrial Asset Vision

Simple initial deployment journey



- Add Gateway to Inventory
- Onboard Gateway

- Create Asset Type
- Create Asset
- Onboard sensor and assign to asset

- Dashboard landing page
- Asset, Sensor, Network Device pages
- Reports

- Create Alerts
- Create Integrations

Cisco Industrial Asset Vision sensors

A variety of options for telemetry and location tracking

Monitoring Environments

AV206
Light

AV200
Outdoor Temp

AV201
Indoor Temp

AV207
Occupancy

AV204
Door/Window

AV205
Water Leak

Monitoring Assets

AV250
Machine Temp

Coming Soon!

AV251
Machine Vibration

AV300
Geolocation

AV202
Product Temp

AV203
Refrigeration

Telemetry Sensor Reference Page

Sensor	Report on State change?	Default Reporting Interval	Expected Battery Life
AV200 (Outdoor temp)	-	60 mins	4 years
AV201 (Indoor temp)	-	15 mins	5 years
AV202 (Product temp)	-	15 mins	5 years
AV203 (Refrig temp)	-	15 mins	5 years
AV204 (Door open/close)	Yes	60 mins	5 years (~100 triggers/day)
AV205 (Water leak)	Yes	60 mins	5 years
AV206 (Light)	-	15 mins	5 years
AV207 (Occupancy)	Yes	60 mins	2.5 years (~100 triggers/day)
AV250 (Machine temp)	-	15 mins	4.8 years
AV251 (Machine vibration)	-	60 mins	3 years

GPS sensor reports as follows:

State	Reporting Interval
“In Trip”	15 mins
“Out of Trip”	24 hours

CISCO

ciscolive.com/emea

CISCO Live!

February 9-11, 2021 • EMEAR