Kam jsme se posunuli v IoT?

Jiří Rott

10.12.2019

Agenda

01 Architectures

02 IoT Switching update

03 IoT Routing update

04 IoT Wifi Update

05 Fog/Edge Computing (IoX – Kinetic EFM …)

06 Cisco Cyber Vision

Architecture Focus

IoT architectural areas

Extended Enterprise

- IT Buyer
- Horizontal Play

Warehouses Distribution Centers

Port Infrastructure

Remote & Mobile Assets

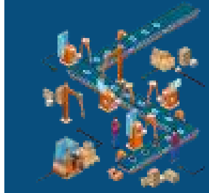
- IT implements for OT outcomes
- Horizontal Play

Public Safety Fleets

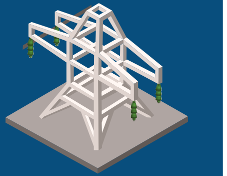
Kiosks

Industry Plays

- Validated use cases for OT/LOB
- Typically vertical specific



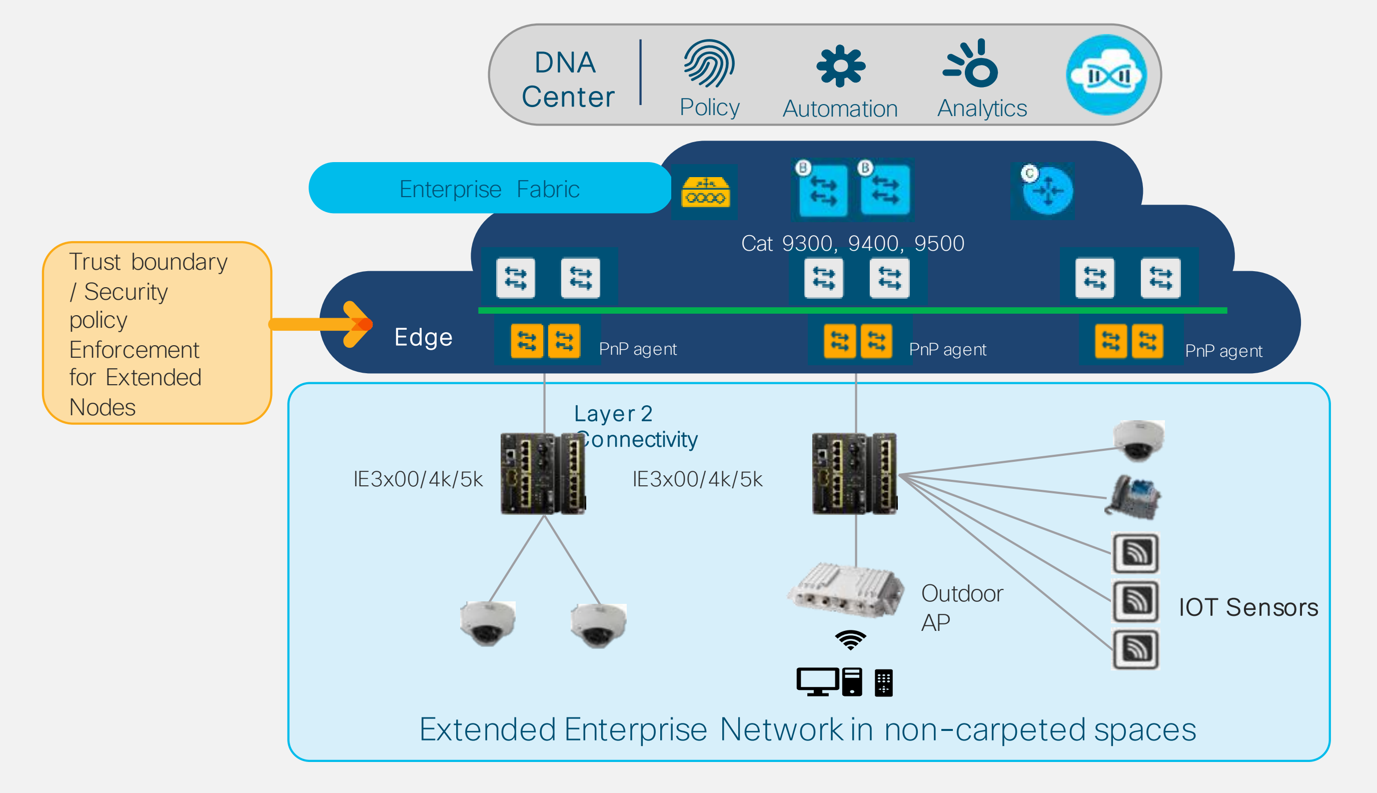
Factories



Utilities

New CVD: Cisco Extended Enterprise v1.0

Intent-based Networking to the IoT Edge



CVD Use Case

- Parking Lots
- Warehouses
- Outdoor Spaces
- Ports, etc…

Outcomes

- Reduce operating resources
- Extend security policy
- Faster deployment

New Features

- Simplicity
  - Plug and Play
  - Assurance
  - Software Image Management
- Scalability: Multi-site
- Security: Automated segmentation

Innovation around Extended Node

Layer

Macro-segmentation

Micro-segmentation

Security Enforcement

Shipping Extended Node

Layer 2 node

VLAN to VRF mapping

Industrial Ethernet IE5000

Industrial Ethernet IE4010

Industrial Ethernet IE4000

Catalyst IE3300 Rugged Series

Catalyst IE3400 Rugged Series

Catalyst IE3400H Heavy Duty Series

DEC '19 Secure Extended Node

Layer 2 node

VLAN to VRF mapping

Secure Group Tag (Inline Tagging)

SGACL At IoT Edge

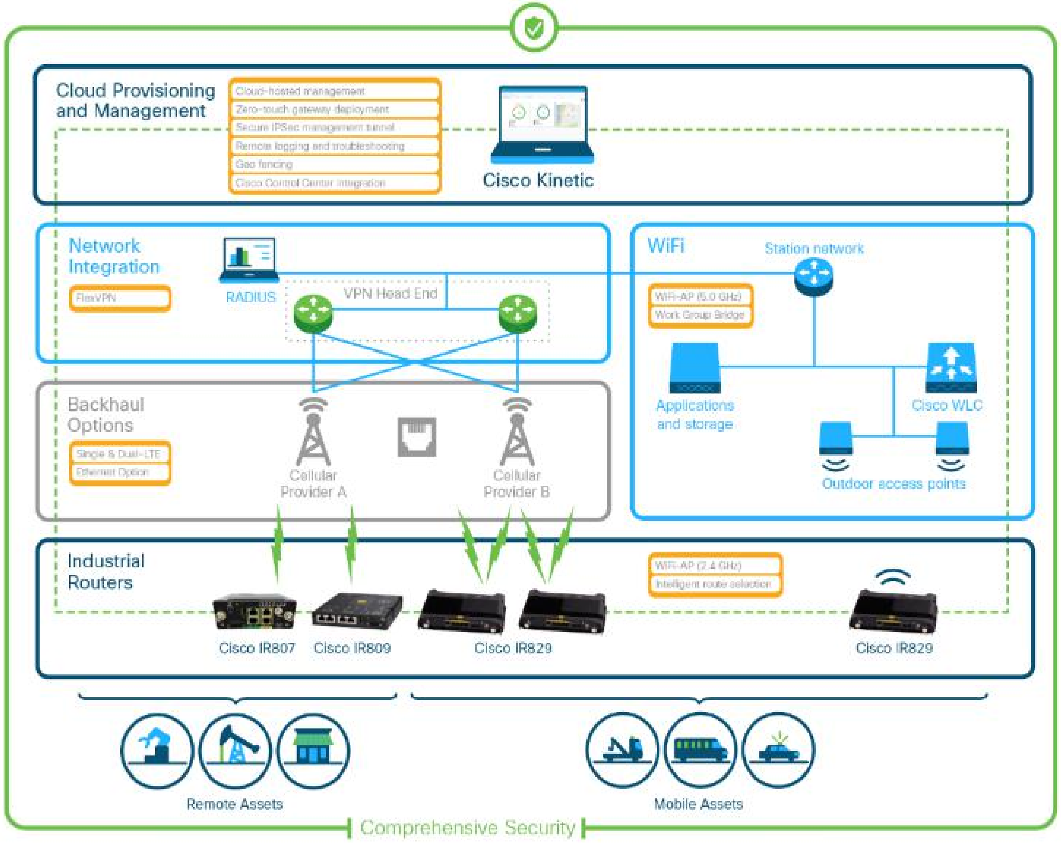
Catalyst IE3400 Rugged Series

Catalyst IE3400H Heavy Duty Series

Cisco Remote and Mobile Assets

RAMA

Cisco Validated Design



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:

- IR 1101 addition to solution
- IOX initial partner integration testing

Simplicity:

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

IoT Portfolio

Industrial Switching

IE 1K, 2K, 3K, 3200, 3300, 3400, 3400H, 4K, 5K, CGS

IoT Gateways / Compute

819-MNA, IR807, IR809, IR829, IR1101 IC3000

Industrial Routing

ASR 902U/903U/920U, CGR 1000, CGR 2000

Cisco Resilient Mesh

IR500, DevNet

Low Power Wide Area Wireless

LoRaWAN
IXM Gateway

Industrial Wireless

AP1552, IW3702, IW6300

Industrial Security

ISA 3000
Cybervision

Embedded IoT

ESS, ESR, ESW

Edge Computing Software

IOx

Management & Automation

Field Network Director
Industrial Network Director
Control Center & GMM

Cisco Vision

Dynamic Signage Director
Digital Media Players

Delivering a steady stream of product innovations

Catalyst IE 3x00
Rugged Series

Cisco IR1101
Integrated
Services
Router Rugged

Catalyst IW6300
Heavy Duty Access Points

Catalyst IE3400
Heavy Duty Series

Cisco Cyber Vision
Visibility & Security

Powered by
IOS- XE

Managed by
DNA Center

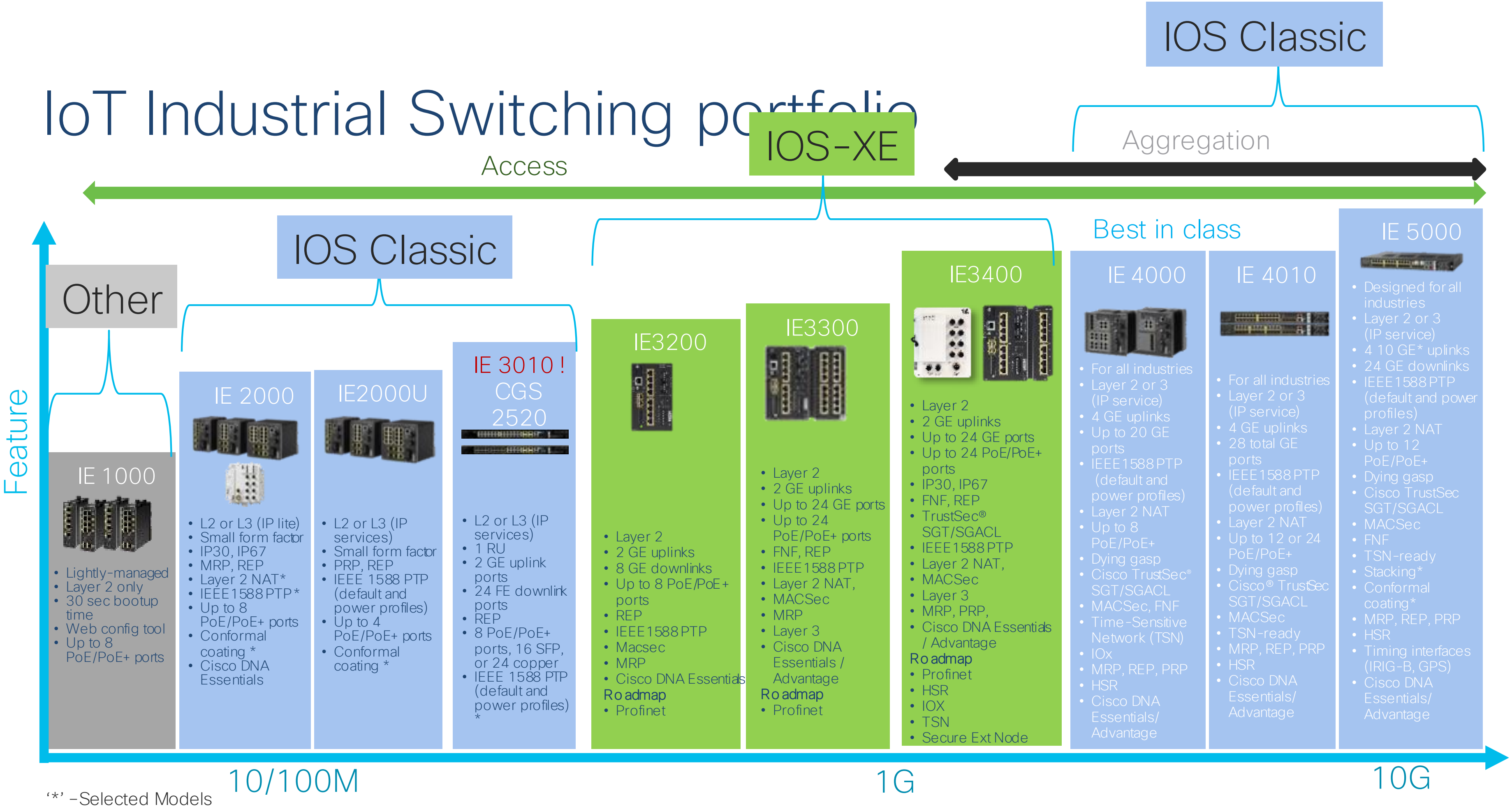
Visibility with
Stealthwatch

Edge Compute
Enabled

Security via
ISE (Identity Services Engine)

Switching

IoT Industrial Switching portfolio



IOS Classic

Aggregation

IOS-XE

Access

Best in class

IOS Classic

Other

Feature

IE 1000

- Lightly-managed
- Layer 2 only
- 30 sec bootup time
- Web config tool
- Up to 8 PoE/PoE+ ports

IE 2000

- L2 or L3 (IP lite)
- Small form factor
- IP30, IP67
- MRP, REP
- Layer 2 NAT*
- IEEE1588PTP*
- Up to 8 PoE/PoE+ ports
- Conformal coating *
- Cisco DNA Essentials

IE2000U

- L2 or L3 (IP services)
- Small form factor
- PRP, REP
- IEEE 1588 PTP (default and power profiles)
- Up to 4 PoE/PoE+ ports
- Conformal coating *

IE 3010 ! CGS 2520

- L2 or L3 (IP services)
- 1 RU
- 2 GE uplink ports
- 24 FE downlink ports
- REP
- 8 PoE/PoE+ ports, 16 SFP, or 24 copper
- IEEE 1588 PTP (default and power profiles) *

IE3200

- Layer 2
- 2 GE uplinks
- 8 GE downlinks
- Up to 8 PoE/PoE+ ports
- REP
- IEEE1588PTP
- Macsec
- MRP
- Cisco DNA Essentials

Roadmap
- Profinet

IE3300

- Layer 2
- 2 GE uplinks
- Up to 24 GE ports
- Up to 24 PoE/PoE+ ports
- FNF, REP
- IEEE1588PTP
- Layer 2 NAT,
- MACSec
- MRP
- Layer 3
- Cisco DNA Essentials / Advantage

Roadmap
- Profinet

IE3400

- Layer 2
- 2 GE uplinks
- Up to 24 GE ports
- Up to 24 PoE/PoE+ ports
- IP30, IP67
- FNF, REP
- TrustSec® SGT/SGACL
- IEEE1588PTP
- Layer 2 NAT,
- MACSec
- Layer 3
- MRP, PRP,
- Cisco DNA Essentials / Advantage

Roadmap
- Profinet
- HSR
- IOX
- TSN
- Secure Ext Node

IE 4000

- For all industries
- Layer 2 or 3 (IP service)
- 4 GE uplinks
- Up to 20 GE ports
- IEEE1588PTP (default and power profiles)
- Layer 2 NAT
- Up to 8 PoE/PoE+
- Dying gasp
- Cisco TrustSec® SGT/SGACL
- MACSec, FNF
- Time-Sensitive Network (TSN)
- IOx
- MRP, REP, PRP
- HSR
- Cisco DNA Essentials/ Advantage

IE 4010

- For all industries
- Layer 2 or 3 (IP service)
- 4 GE uplinks
- 28 total GE ports
- IEEE1588PTP (default and power profiles)
- Layer 2 NAT
- Up to 12 or 24 PoE/PoE+
- Dying gasp
- Cisco® TrustSec SGT/SGACL
- MACSec
- TSN-ready
- MRP, REP, PRP
- HSR
- Cisco DNA Essentials/ Advantage

IE 5000

- Designed for all industries
- Layer 2 or 3 (IP service)
- 4 10 GE* uplinks
- 24 GE downlinks
- IEEE1588PTP (default and power profiles)
- Layer 2 NAT
- Up to 12 PoE/PoE+
- Dying gasp
- Cisco TrustSec SGT/SGACL
- MACSec
- FNF
- TSN-ready
- Stacking*
- Conformal coating*
- MRP, REP, PRP
- HSR
- Timing interfaces (IRIG-B, GPS)
- Cisco DNA Essentials/ Advantage

10/100M

1G

10G

'*' -Selected Models

Shipping

Cisco Catalyst IE3x00 Rugged Series

IE3400 PoE+ switch orderable now !!!

IE 3400 modular advanced

IE 3300 modular

IE 3200 fixed

Up to 24 ports of PoE/PoE+ (up to 480W power budget)

All Gigabit Ethernet – up to 26 ports

Modern Cisco® IOS –XE OS
Layer 2 and Layer 3*

10 module options – Add 8-16 copper, fiber, PoE ports

Cisco® DNA Center
IOx edge compute*
SDA Secure Extended node*

Advanced security Cisco TrustSec®, MACsec, 802.1x

Industrial protocols – REP, HSR*, PRP, Profinet*, MRP, EtherNet/IP

** In roadmap*

Systems and modules at a glance

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

2p SFP and 8p Cu

1. IE3300 copper basic modular system
2. IE3300 POE+ basic modular system
3. IE3400 advanced modular system

IEM3300, IEM3400 expansion modules

8p Cu

1. IEM-3300 8p copper
2. IEM-3300 8p PoE+
3. IEM-3400 Adv copper

2p Fi + 6p Cu

4. IEM-3300 6p copper + 2p fiber mixed

16p Cu

5. IEM-3300 16p copper
6. IEM-3300 16p PoE+

2p Fi, 14p Cu

7. IEM-3300 14p copper + 2p fiber mixed

8p Fi

8. IEM-3300 8p fiber

8p Fi

9. IEM-3400 Advanced 8p fiber

Note: IEM-3400 expansion modules only work with IE3400 base

Cisco Catalyst IE3400 Heavy Duty Series

IE-3400H-8FT

IE-3400H-8T

IE-3400H-16FT

IE-3400H-16T

IE-3400H-24FT

IE-3400H-24T

🟧 Fast Ethernet

🟩 Gigabit Ethernet

Enhanced network-based security, segmentation, and visibility

Up to 24 all Fast Ethernet or all Gigabit Ethernet, M12 interface

Cisco® DNA Center
IOx edge compute *
Secure Extended node*

SD Swap Drive

Feature Parity with Catalyst IE3x00 Rugged Series*

Modern Cisco®
IOS –XE OS Layer 2 and Layer 3*

IP67

Dust and Water Protection

* In roadmap

IE-3400H and IE-3400 comparison

Similarities of IE-3400H and IE-3400

- Same SW image: ‘ie-3x00-universalk9-….bin’
- Same IO-XE release same features support
- Same HW forwarding Architecture
    - Same FPGA for advanced services

Differences	IE-3400 Heavy Duty	IE-3400
Deployment	Deploy without enclosure	Deploy on din rail in enclosure
Modularity	Not Modular. Fixed port count	Modular. Add up to 16 ports to base system
Ingress Protection	IP67	IP30

IoT Licensing alignment with EN

Network Management Tools

Licenses for advanced network management tools

Vmanage — Cloud / On Prem

GMM — Cloud

DNAC, FND — On Prem

Subscriptions Options Only

Additional IoT Products

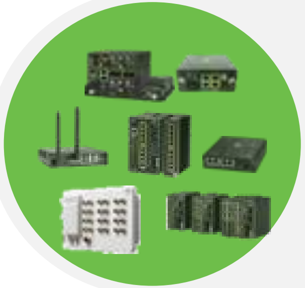
IND — On Prem

CyberVision — On Prem

Subscriptions Options Only

Platform Feature Packages

Licenses to upgrade software features on the platform



Advanced Switching Features

Advanced Routing Features

Additional Security Capabilities

Perpetual Options Only

Routing

Industrial Routing Products Overview

Smart City, Utility (FAN), Transportation, Plant

Plant, WAN,SA

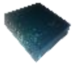
WAN

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, vibration, Ignation
- Raw Sockets
- 2 radios, SSD
- Security
- 4FE Copper
- 1GE Fiber
- WiFi, PoE
- IOX

IR 1101

- Modular Radio (2 radios)
- Interface Module
- IoS XE
-1 x Serial RS232
- Security, SSD
- 4FE Copper
- 1GE Combo
- 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

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

New Products in IoT Gateways

Shipping

1st Industrial SD-WAN

IR1101+ 5G ready

Available Now

IR1101 Expansion Modules

IRM1100 – SPMI/SP

Available Now

5 LTE Pluggables

Cat4 & Cat6 Modules

Available Now

Storage for Edge Computing

IR829M/B

Available Now

Dust and Water Protection

IP54 Kit

Available Now

vManage

SDWAN Management Platform

Available Q2FY20

IOS-XE

Modularity

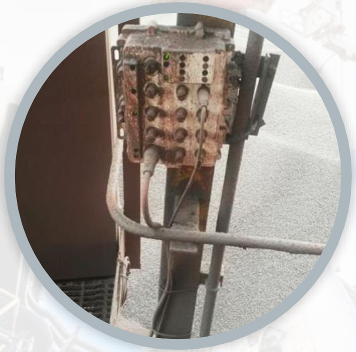
Dual LTE & Extended Bands

SDWAN

IP54

Dust and Water Protection

Storage for Edge Computing



Cisco Industrial Routers Purpose Built for Harsh Environments

1 Size Weight Form-factor

2 Shock and Vibration

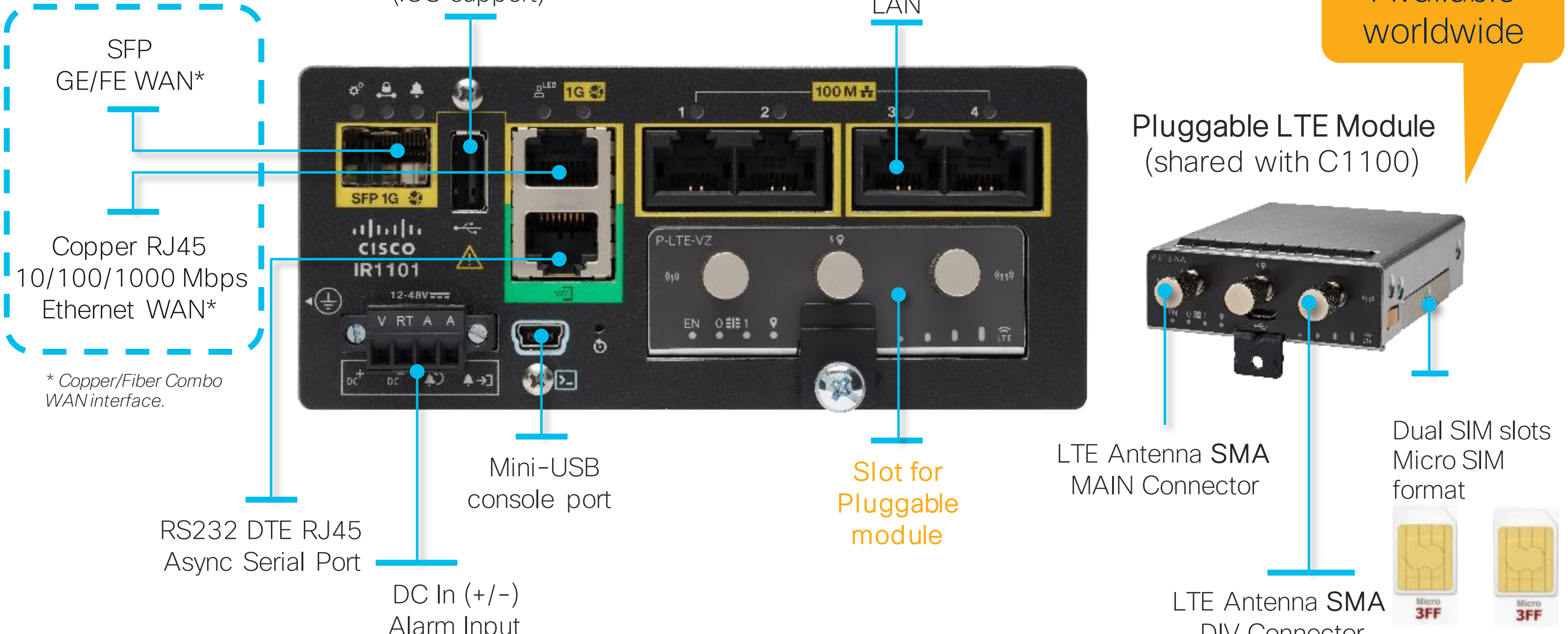
3 High MTBF Resilient Network Topologies

4 Din-Rail or Rack Mounts

5 Fanless -40 - +75°C Self-cooled

6 Industry Certifications

IR1101- Base Platform – Compact and Flexible



SFP
GE/FE WAN*

Copper RJ45
10/100/1000 Mbps
Ethernet WAN*

* Copper/Fiber Combo
WAN interface.

USB port Type A
(IOS support)

Four 10/100Mbs
RJ45 Ethernet
LAN

Available
worldwide

Pluggable LTE Module
(shared with C1100)

RS232 DTE RJ45
Async Serial Port

DC In (+/-)
Alarm Input

Mini-USB
console port

Slot for
Pluggable
module

LTE Antenna SMA
MAIN Connector

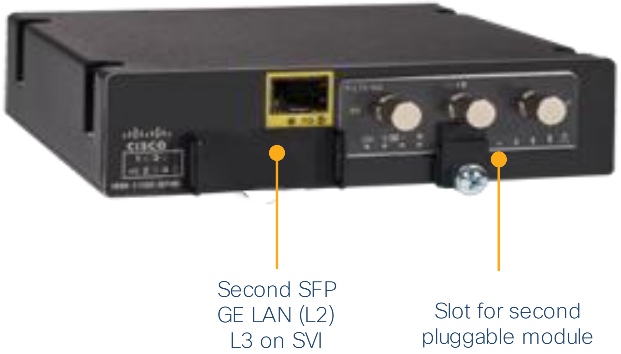
LTE Antenna SMA
DIV Connector

Dual SIM slots
Micro SIM
format

Expansion Module

IRM-1100-SP

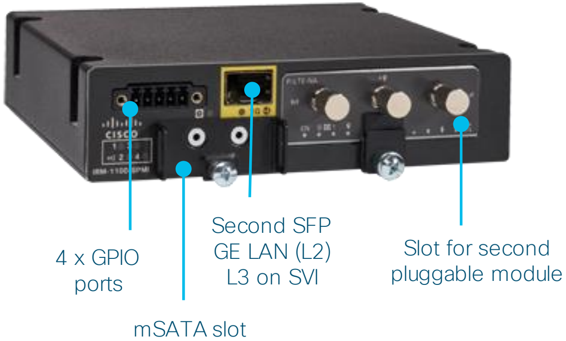
- SFP GE LAN (L2)
- Slot for LTE pluggable module



IRM-1100-SPMI

- **4x GPIO ports**
- **mSATA slot**
- SFP GE LAN (L2)
- Slot for pluggable module

IR1100-SSD-100GB
for Edge Computing



IR1101 Software Features / Benefits & Licenses

- IPv4/IPv6
- QoS
- Security
- Routing
- Single/Dual LTE
- Manageability

High-end Security

- Next-gen encryption
- Quantum computer resistant crypto algorithm
- Hardware Crypto-acceleration
- Cisco Trust Anchor
- Firewall, Umbrella

- 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
- GPS (Geo-fencing on management tool)

Resilient

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

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

NEW IR1101-A-K9

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

IR1101-K9

* future release

Industrial Din-Rail Power Supplies – At a glance

** IEC SKU also available
* DC – DC also available

50W	50W**	65W*	160W (IP67)	170W*	180W (IP67)	240W	480W
PWR-IE50W-AC-L=	PWR-IE50W-AC=	PWR-IE65W-PC-AC=	PWR-IE160W-67-DC=	PWR-IE170W-PC-AC=	PWR-IE180W-67-AC=	PWR-IE240W-PCAC-L=	PWR-IE480W-PCAC-L=

Wide range of din-rail power supply SKUs to power your
Industrial Ethernet Switches, Industrial Routers and Industrial Computing products.

IR1101 Network Management Solution

Cisco IOS-XE Network Management

- IOS-XE CLI and WebUI
- Telnet
- SNMPv1, v2 and v3, MIBs
- Secure Shell (SSH) Protocol
- Telemetry: Netconf, Yang…
- HTTP/HTTPS
- RADIUS and TACACS+
- XML/CGNA/WSMA
- Plug-n-Play agent
- Configuration rollback
- EEM for WAN Monitoring
- IP SLA,…

OT Driven

Extended Enterprise

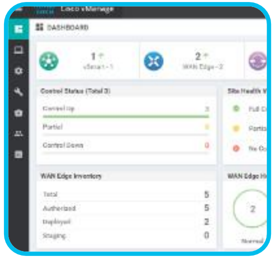
Cisco IoT Field Network Director

Single platform to manage a complete FAN solution

Raw Socket sessions management and monitoring

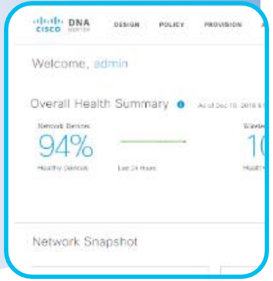
Cisco Kinetic GMM

Cloud-based management for IR1101, IR800



Control Center support-SIM management

Control center support for IRX9 platforms without any IOS configurations



Cisco DNA Center

Cisco SDWAN

will require IOS-XE 16.12 release (Q3 CY2019)

Viptela vManage, vBond, v

Cisco Prime Infrastructure

Single platform to manage an infrastructure with a broad range of static Cisco devices

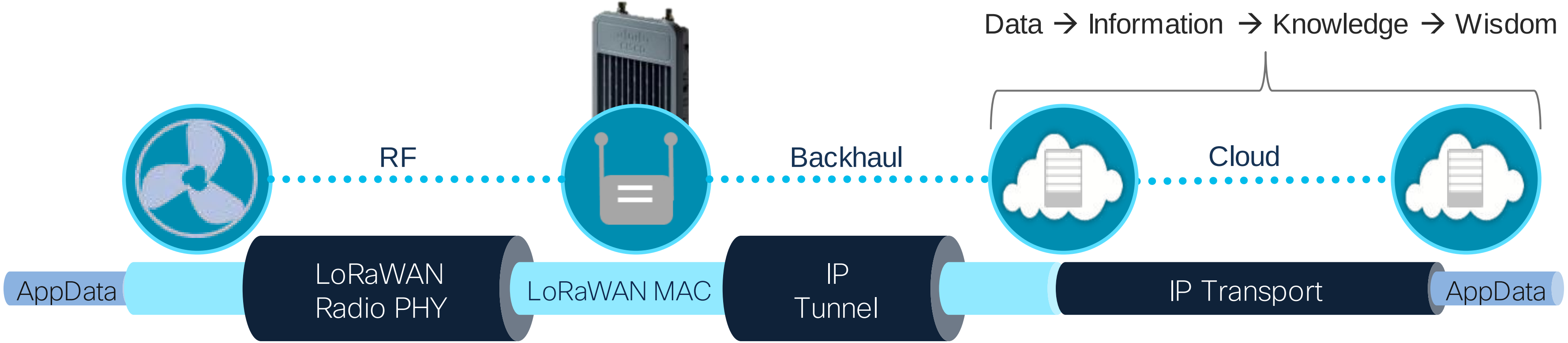
LoRaWAN

LoRaWAN End-to-End Architecture

Cisco IXM LoRaWAN Interface Module

Cloud Based Sensor Platform

This is where data can be stored and monetized
Data → Information → Knowledge → Wisdom



LoRaWAN Sensor
Standards Compliant
Low power sensor

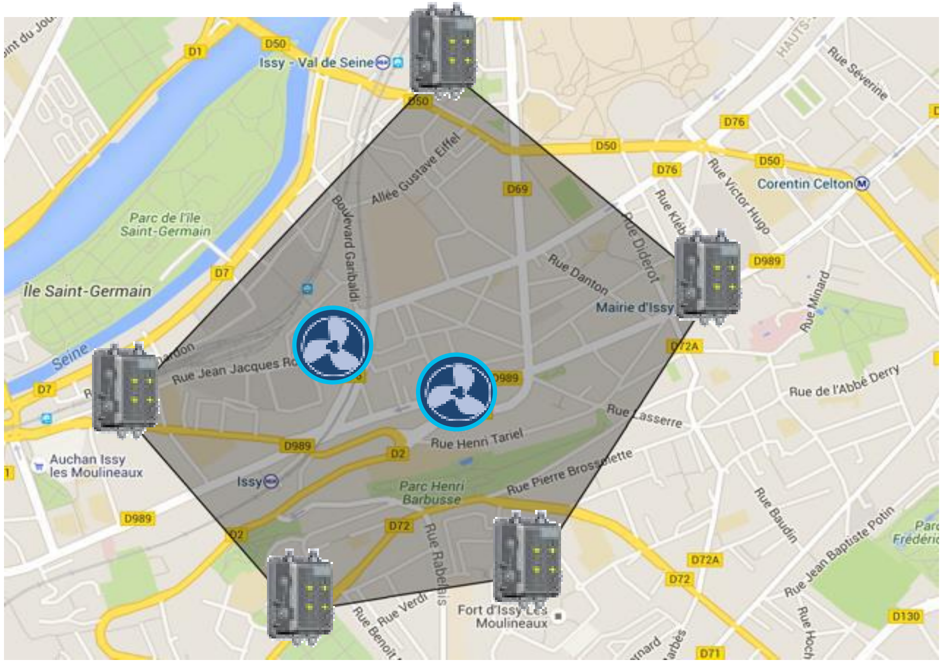
Access Point
Contains Radios
RF Termination of 1000s

Network Server
MAC decaps, Security
Network/Radio management
Message scheduling, ZTD etc…

Application Server
Platform for ASP
e.g., Parking, Air quality,
Meter reading

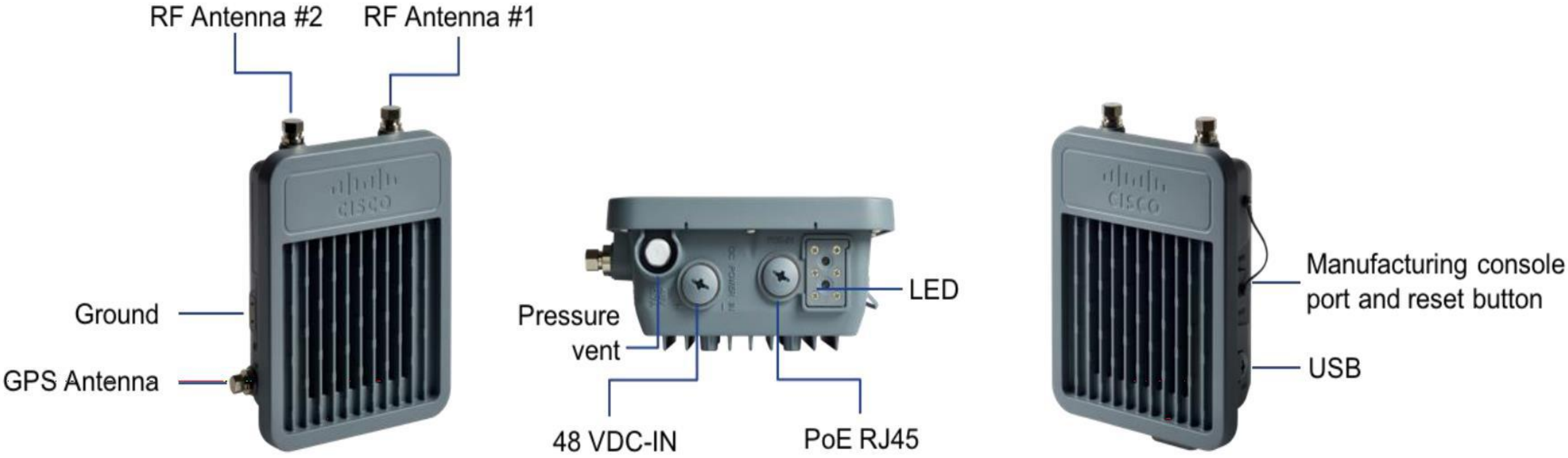
Introduce Geo-location Capability

- TDOA/RSSI based gateway triangulation algorithm
- Any LoRaWAN endpoint, GPS chipset-free, stationary or mobility
- Applicable use case – Asset tracking and Geo-fencing
- Cisco is the only vendor capable to provide this solution in current LPWA market



Cisco LoRaWAN Interface Module

Part of IoT eXtension Module Series (IXM)



Wireless

IoT Wireless portfolio

IW6300

IW3702

ESW6300

Wireless Connectivity In Extreme Environments

Intent Based Networking at the Industrial Edge

Cisco Catalyst IW6300 Heavy Duty Series Access Points

Purpose-built for Class I Division 2 hazardous environments

Flexible connectivity: Three PoE and one SFP port

AC/DC and PoE-in for power redundancy

Intelligence beyond boundaries: IOx, compute at the IoT edge

Lightweight, compact design built for simpler deployments in extreme temperature ranges

IoT modules for enhanced capabilities

Resilient mesh architecture support based on 802.11 AC Wave 2

Cisco end-to-end security including ISE

Extend intent-based networking to hazardous environments

Cisco Catalyst IW6300 IoT Partner module

Enabling partners to provide enhanced capabilities for their customers

Go further in your digital transformation. Connect to WirelessHART, ISA100 and more.

Easy-to-install
Expansion modules

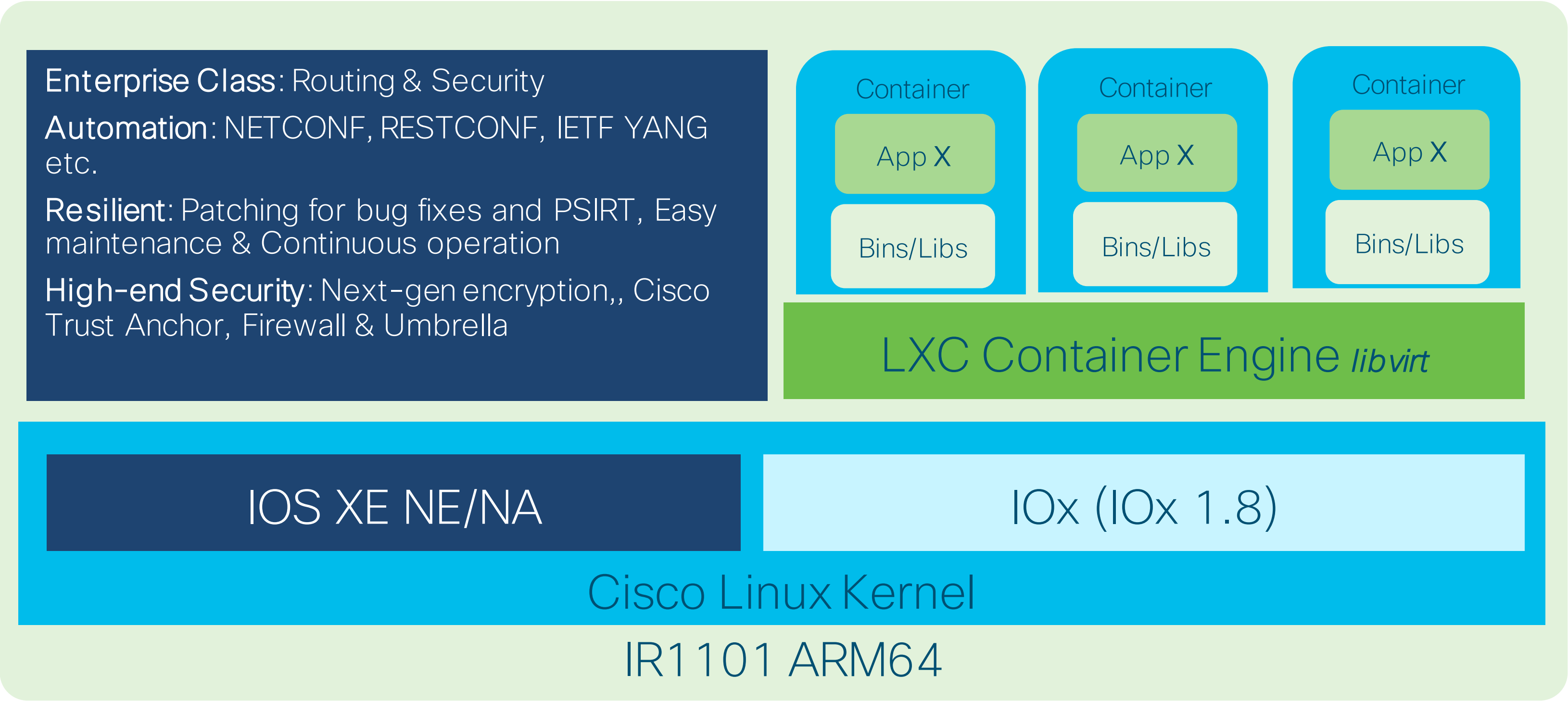
WirelessHART | ISA100 | GPS* | Bluetooth Low-Energy* | Zigbee*

- Future-proof your deployments
- Industrial IoT multi-lingual access brings IoT devices together
- Extend value to hazardous locations

*under future consideration

Edge/Fog computing

Cisco IR1101 Application View



Enterprise Class: Routing & Security

Automation: NETCONF, RESTCONF, IETF YANG etc.

Resilient: Patching for bug fixes and PSIRT, Easy maintenance & Continuous operation

High-end Security: Next-gen encryption,, Cisco Trust Anchor, Firewall & Umbrella

Container

App X

Bins/Libs

Container

App X

Bins/Libs

Container

App X

Bins/Libs

LXC Container Engine *libvirt*

IOS XE NE/NA

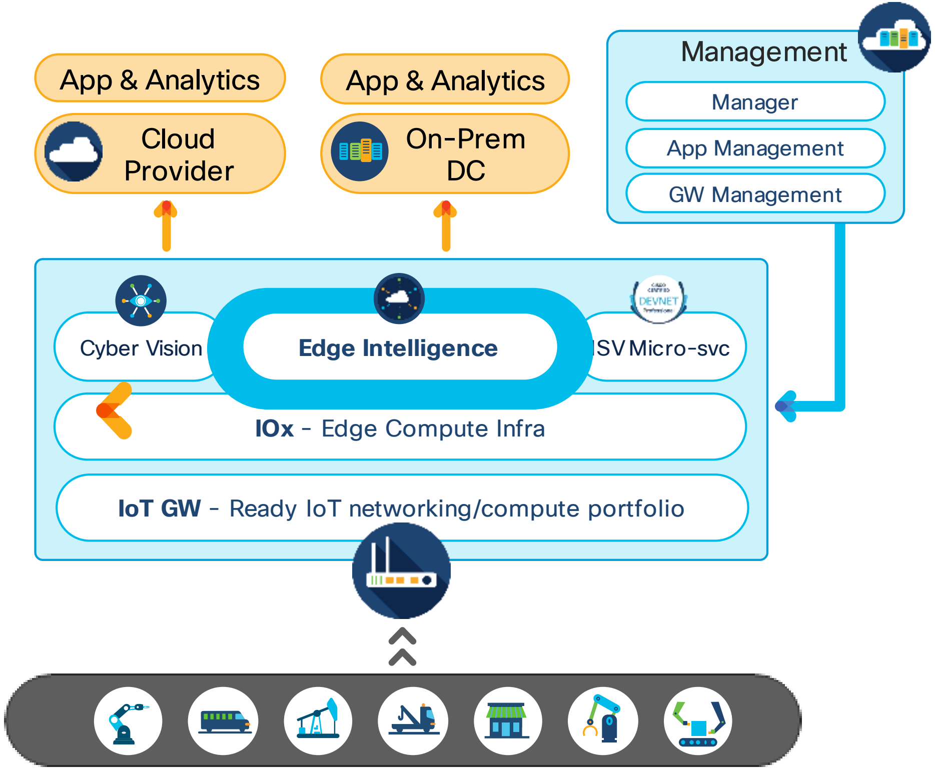
IOx (IOx 1.8)

Cisco Linux Kernel

IR1101 ARM64

Introducing Cisco Edge Intelligence :

An edge to cloud data SW purpose built for device makers & device owners



Introducing Cisco Edge Intelligence:

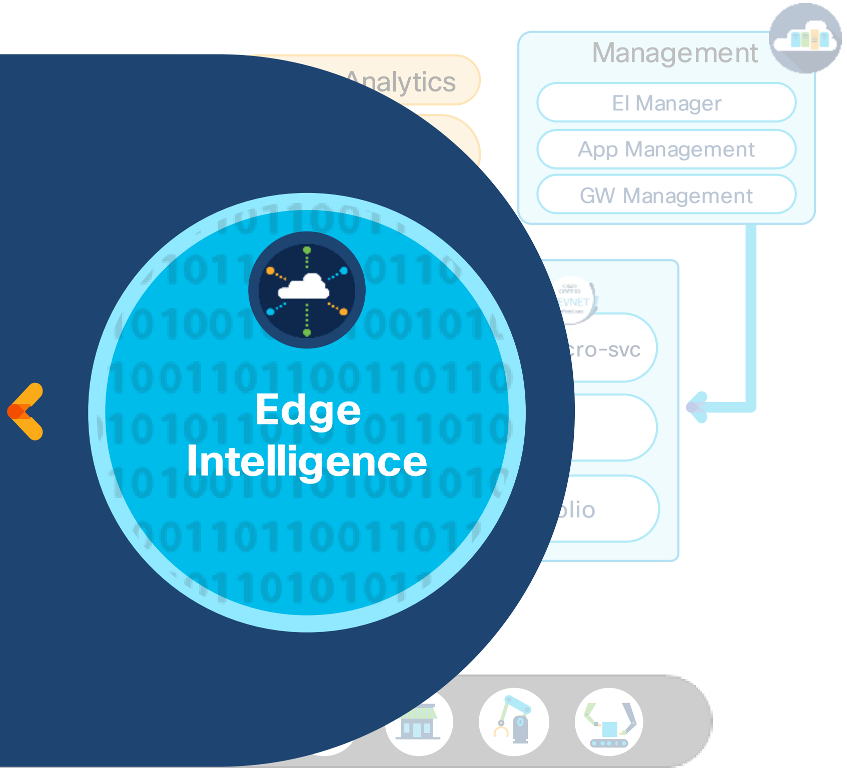
An edge to cloud data SW purpose built for device makers & device owners

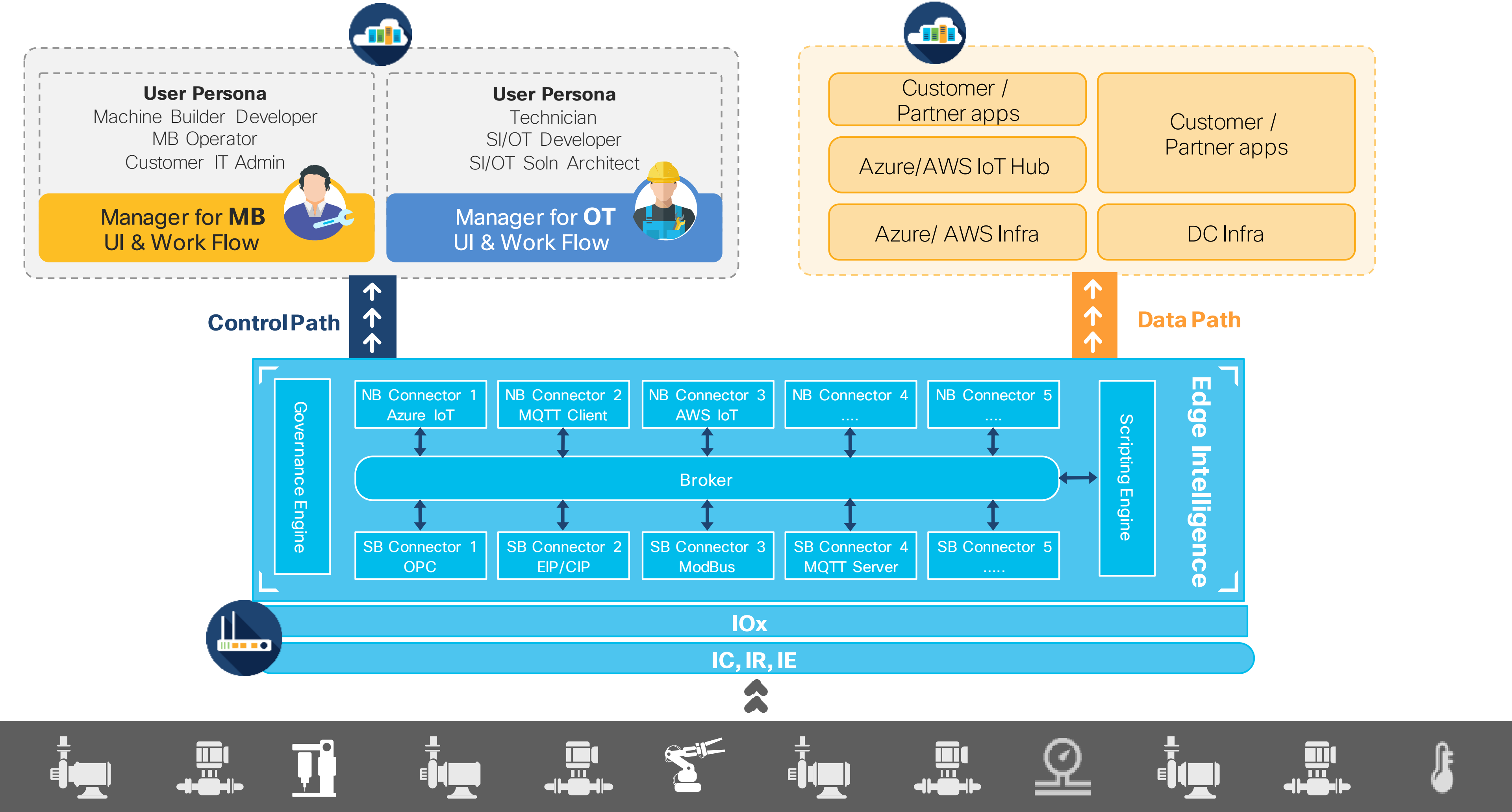
Share
Securely share the data to it’s destination

Govern
Control point to decide where the raw or transformed data should go

Transform
Developer Friendly Tools to transform & modify data

Ingest
Various heterogenous devices need data ingested seamlessly




User Persona
Machine Builder Developer
MB Operator
Customer IT Admin
Manager for MB
UI & Work Flow
User Persona
Technician
SI/OT Developer
SI/OT Soln Architect
Manager for OT
UI & Work Flow
Customer /
Partner apps
Azure/AWS IoT Hub
Azure/ AWS Infra
Customer /
Partner apps
DC Infra
Control Path
Data Path
Governance Engine
NB Connector 1
Azure IoT
NB Connector 2
MQTT Client
NB Connector 3
AWS IoT
NB Connector 4
....
NB Connector 5
....
Broker
SB Connector 1
OPC
SB Connector 2
EIP/CIP
SB Connector 3
ModBus
SB Connector 4
MQTT Server
SB Connector 5
.....
Scripting Engine
Edge Intelligence
IOx
IC, IR, IE

Cisco Cyber Vision

CYBERSECURITY FOR THE INDUSTRIAL INTERNET

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

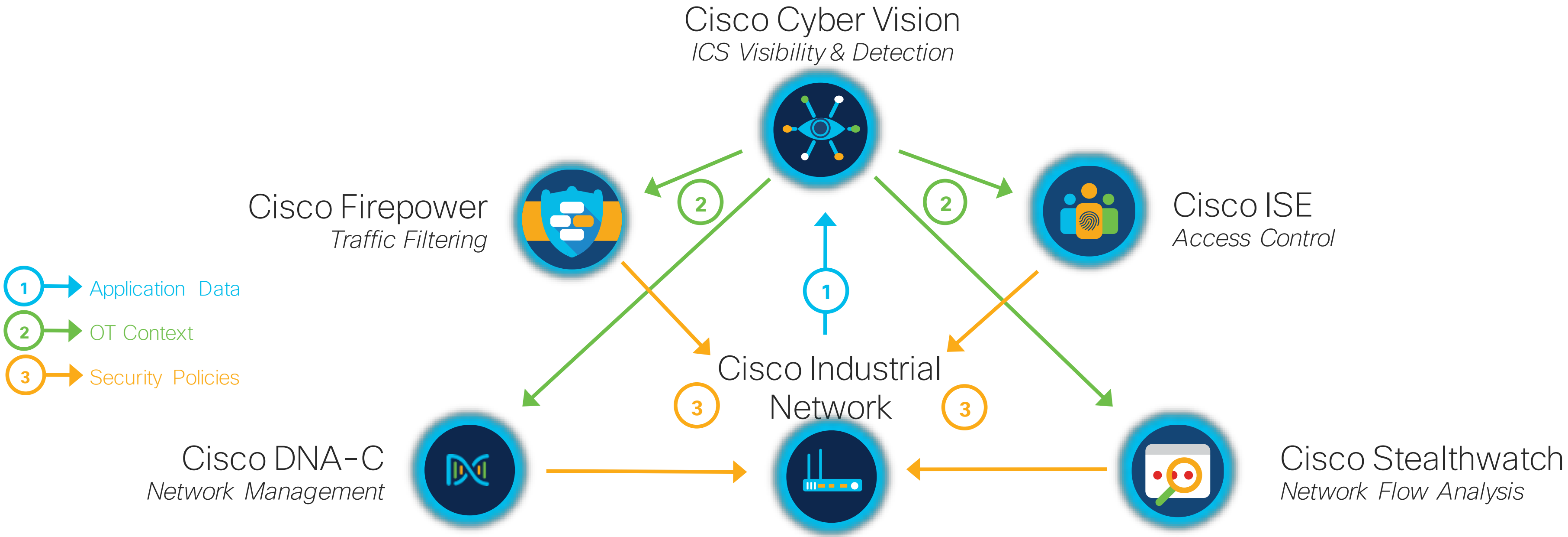
Threat Detection

Behavioral Anomaly Detection
Signature based IDS
Real-time alerting

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

The Only Fully Integrated OT Security Solution

Working together to define & apply IoT security policies



Cisco Cyber Vision
ICS Visibility & Detection

Cisco Firepower
Traffic Filtering

Cisco ISE
Access Control

Cisco Industrial Network

Cisco DNA-C
Network Management

Cisco Stealthwatch
Network Flow Analysis

1 → Application Data

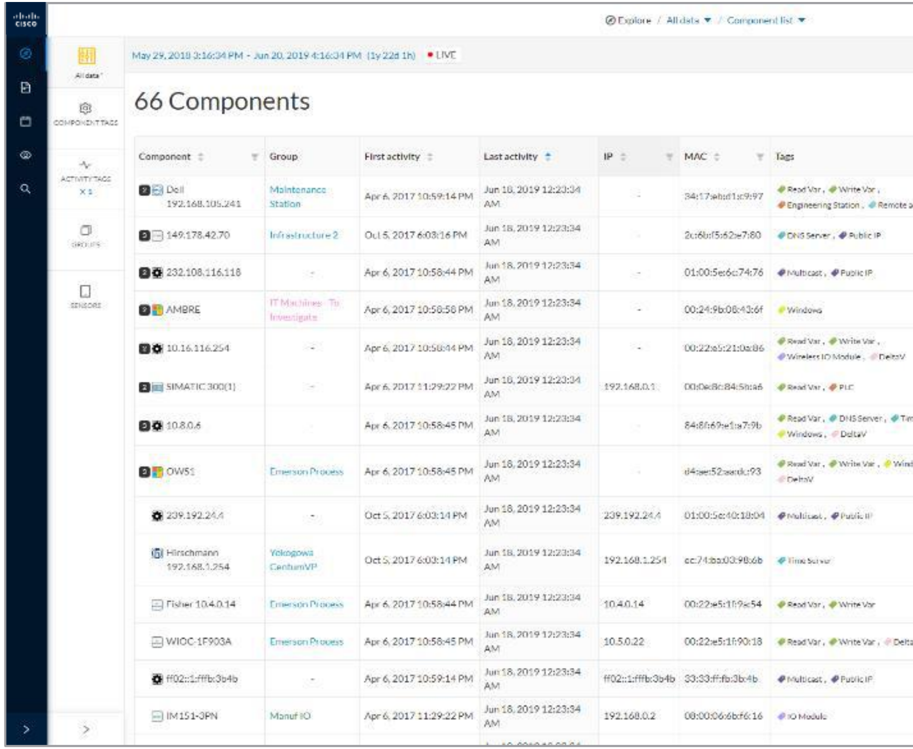
2 → OT Context

3 → Security Policies

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 easily to understand asset functions and properties

Track the industrial assets to protect throughout their life cycles



May 29, 2018 3:16:34 PM - Jun 20, 2019 4:16:34 PM (1y 22d 1h) ● LIVE

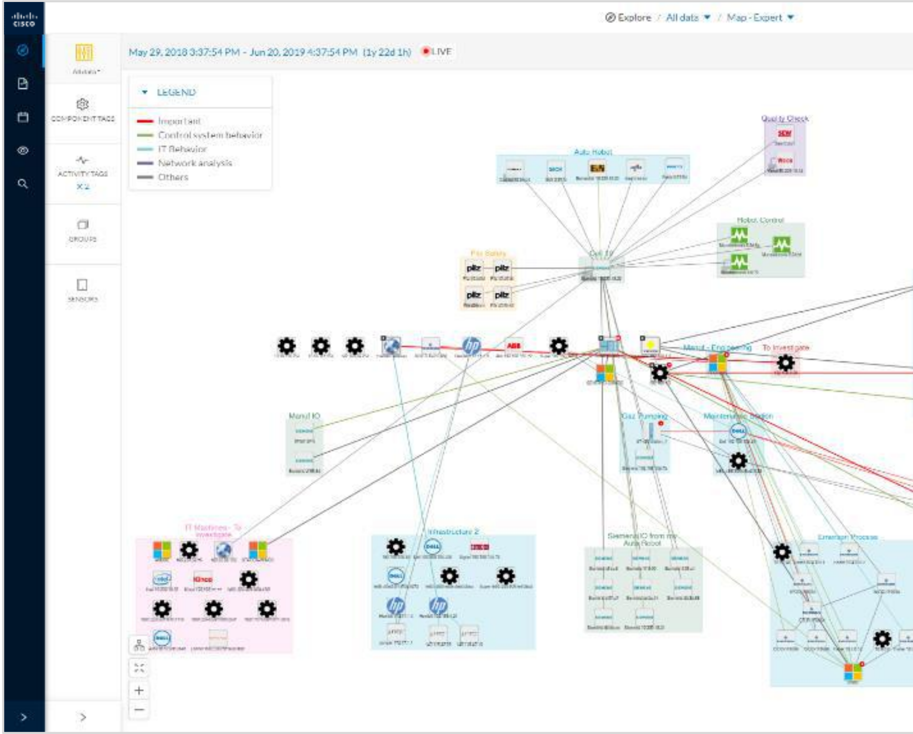
66 Components

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:eb:d1:c9:97	Read Var, Write Var, Engineering Station, Remote a
149.178.42.70	Infrastructure 2	Oct 5, 2017 6:03:16 PM	Jun 18, 2019 12:23:34 AM	-	2c:6b:f5:62:e7:80	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:6c:74:76	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:69:e1:a7:9b	Read Var, DNS Server, Tim Windows, DeltaV
OW51	Emerson Process	Apr 6, 2017 10:58:45 PM	Jun 18, 2019 12:23:34 AM	-	d4:ae:52:ae:dc:93	Read Var, Write Var, Wind 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	Yokogowa 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
WIOC-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:fffb:3b4b	-	Apr 6, 2017 10:59:14 PM	Jun 18, 2019 12:23:34 AM	ff02::1:fffb:3b4b	33:33:ff:fb: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	08:00:06:6b: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



Explore / All data ▾ / Map - Expert ▾

May 29, 2018 3:37:54 PM - Jun 20, 2019 4:37:54 PM (1y 22d 1h) ● LIVE

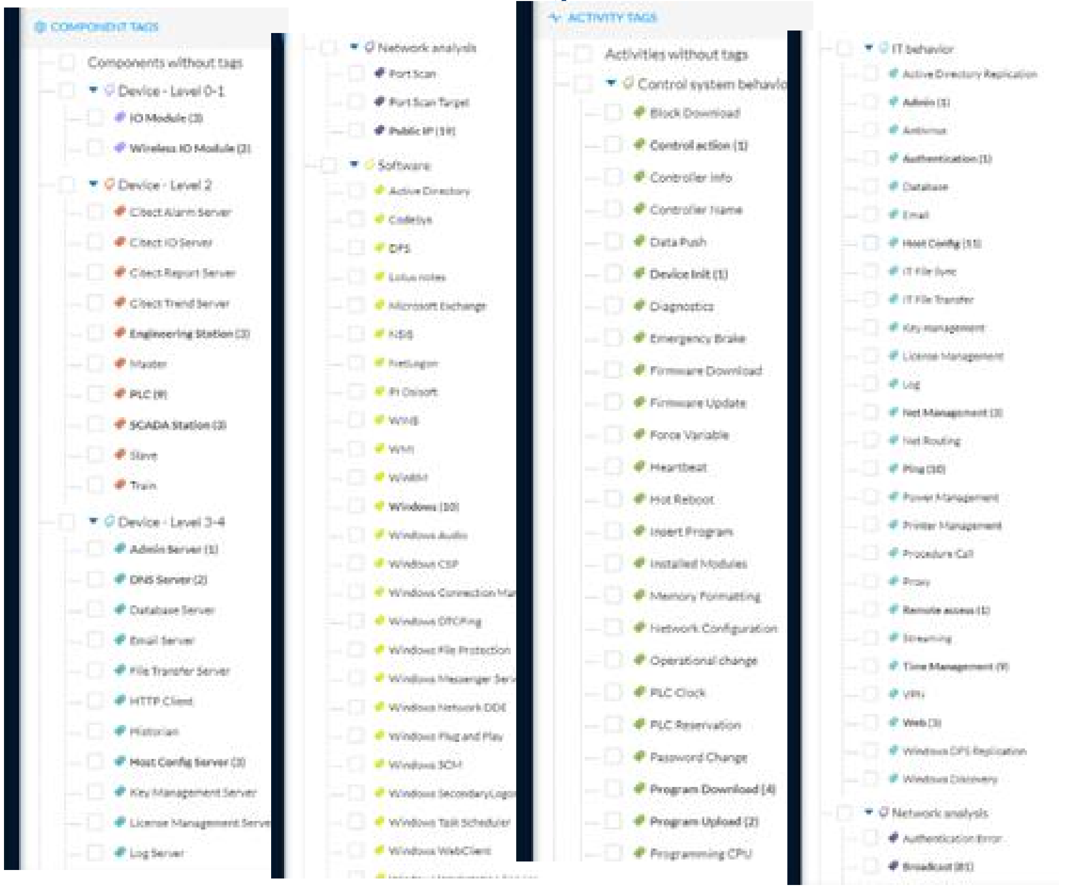
▾ LEGEND
- 🟥 Important
- 🟩 Control system behavior
- 🟦 IT Behavior
- 🟪 Network analysis
- ⬜ Others

Cyber Vision Tags to Drive Data Analysis

Cyber Vision
Universal OT Language

- Asset characteristics and communications are translated to Tags any user can understand
- A common language, whatever the vendor reference
- Users do not need to be protocol experts to understand what is going on
- Automatically assigned based on behaviors and device information
- Can be modified or added via RESTful API

Quickly see asset and communication information in standard format



COMPONENT TAGS

- □ Components without tags
- □ ▾ Device - Level 0-1
  - □ IO Module (3)
  - □ Wireless IO Module (2)
- □ ▾ Device - Level 2
  - □ Citect Alarm Server
  - □ Citect IO Server
  - □ Citect Report Server
  - □ Citect Trend Server
  - □ Engineering Station (3)
  - □ Master
  - □ PLC (9)
  - □ SCADA Station (3)
  - □ Slave
  - □ Train
- □ ▾ Device - Level 3-4
  - □ Admin Server (1)
  - □ DNS Server (2)
  - □ Database Server
  - □ Email Server
  - □ File Transfer Server
  - □ HTTP Client
  - □ Historian
  - □ Host Config Server (3)
  - □ Key Management Server
  - □ License Management Serve
  - □ Log Server
- □ ▾ Network analysis
  - □ Port Scan
  - □ Port Scan Target
  - □ Public IP (19)
- □ ▾ Software
  - □ Active Directory
  - □ Codesys
  - □ DFS
  - □ Lotus notes
  - □ Microsoft Exchange
  - □ NDS
  - □ NetLogon
  - □ PI Osisoft
  - □ WINS
  - □ WMI
  - □ WinRM
  - □ Windows (10)
  - □ Windows Audio
  - □ Windows CSP
  - □ Windows Connection Man
  - □ Windows DTCPing
  - □ Windows File Protection
  - □ Windows Messenger Serv
  - □ Windows Network DDE
  - □ Windows Plug and Play
  - □ Windows SCM
  - □ Windows SecondaryLogon
  - □ Windows Task Scheduler
  - □ Windows WebClient

ACTIVITY TAGS

- □ Activities without tags
- □ ▾ Control system behavio
  - □ Block Download
  - □ Control action (1)
  - □ Controller Info
  - □ Controller Name
  - □ Data Push
  - □ Device Init (1)
  - □ Diagnostics
  - □ Emergency Brake
  - □ Firmware Download
  - □ Firmware Update
  - □ Force Variable
  - □ Heartbeat
  - □ Hot Reboot
  - □ Insert Program
  - □ Installed Modules
  - □ Memory Formatting
  - □ Network Configuration
  - □ Operational change
  - □ PLC Clock
  - □ PLC Reservation
  - □ Password Change
  - □ Program Download (4)
  - □ Program Upload (2)
  - □ Programming CPU
- □ ▾ IT behavior
  - □ Active Directory Replication
  - □ Admin (1)
  - □ Antivirus
  - □ Authentication (1)
  - □ Database
  - □ Email
  - □ Host Config (11)
  - □ IT File Sync
  - □ IT File Transfer
  - □ Key management
  - □ License Management
  - □ Log
  - □ Net Management (3)
  - □ Net Routing
  - □ Ping (10)
  - □ Power Management
  - □ Printer Management
  - □ Procedure Call
  - □ Proxy
  - □ Remote access (1)
  - □ Streaming
  - □ Time Management (9)
  - □ VPN
  - □ Web (3)
  - □ Windows DFS Replication
  - □ Windows Discovery
- □ ▾ Network analysis
  - □ Authentication Error
  - □ Broadcast (81)

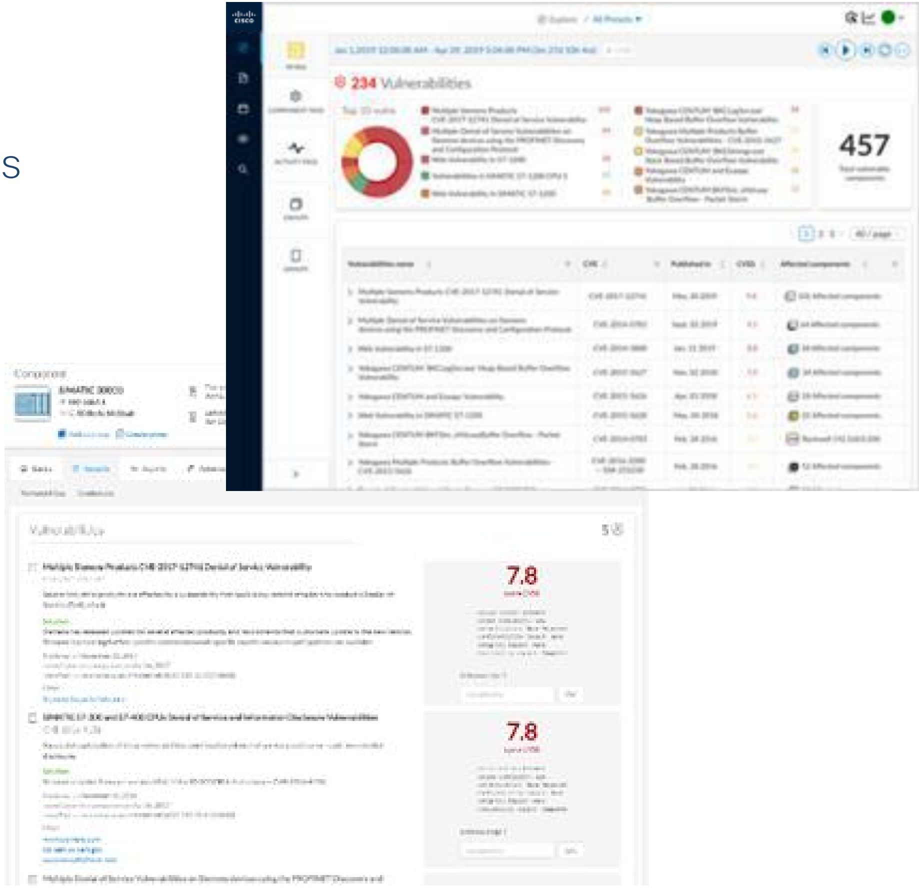
Visibility: Instantaneous **Vulnerability** Identification

- 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

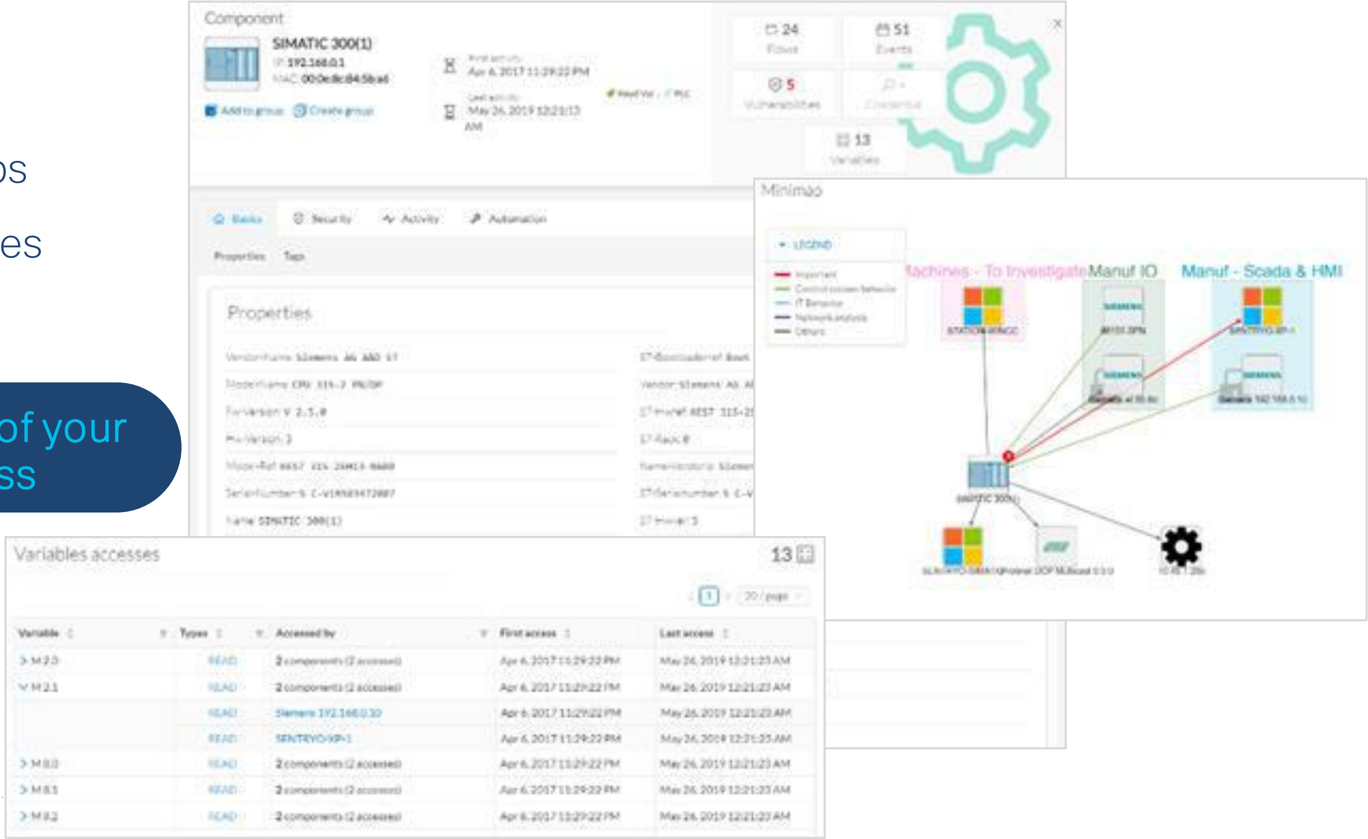
Enforce Cyber-Hygiene best practices



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:84:5b:a6

Add to group Create group

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

Properties

VendorName Siemens AG A&D ET

ModelName CPU 315-2 PN/DP

FwVersion V 2.5.0

HwVersion 3

Model-Ref 6ES7 315 2EH13 0AB0

SerialNumber S C-V1N583472007

Name SIMATIC 300(1)

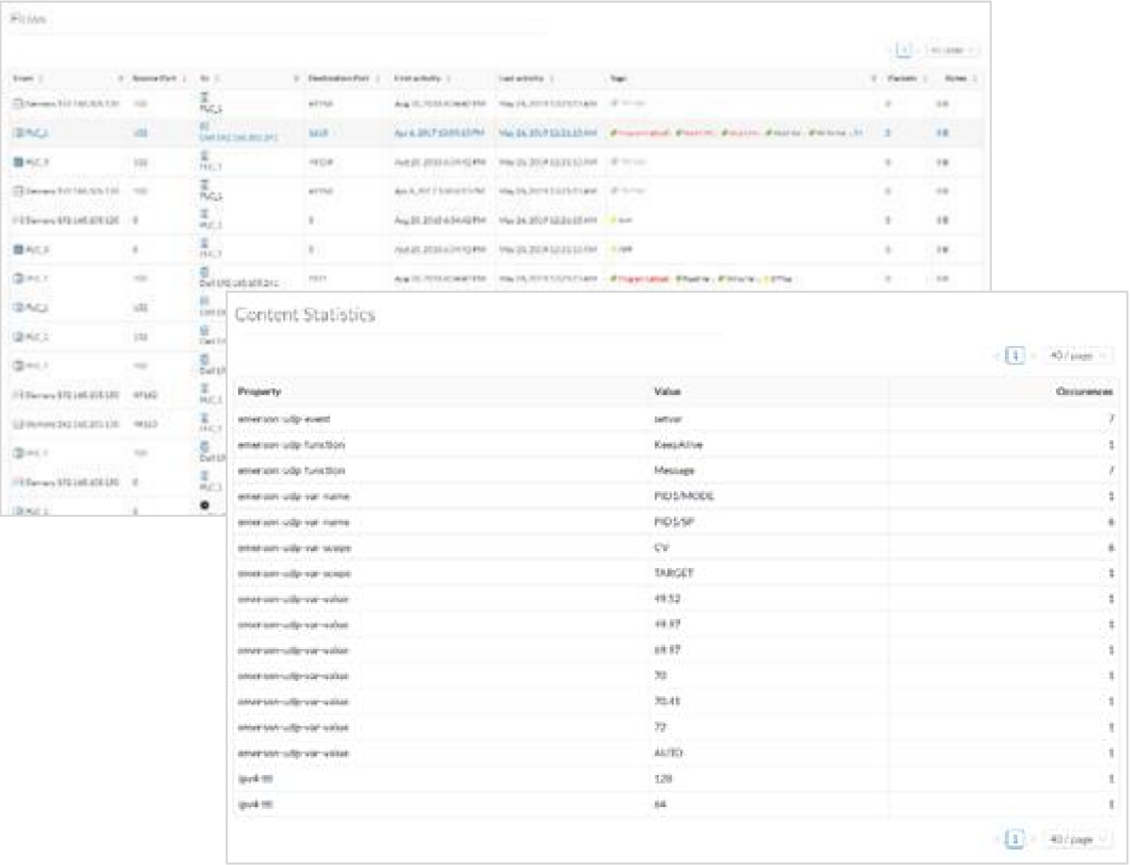
Variables accesses 13

Variable	Types	Accessed by	First access	Last access
› M 2.0	READ	2 components (2 accessed)	Apr 6, 2017 11:29:22 PM	May 26, 2019 12:21:23 AM
˅ M 2.1	READ	2 components (2 accessed)	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 accessed)	Apr 6, 2017 11:29:22 PM	May 26, 2019 12:21:23 AM
› M 8.1	READ	2 components (2 accessed)	Apr 6, 2017 11:29:22 PM	May 26, 2019 12:21:23 AM
› M 8.2	READ	2 components (2 accessed)	Apr 6, 2017 11:29:22 PM	May 26, 2019 12:21:23 AM

Operational Insights: **Views for Security Leaders**

- Access the full history of all communication flows
- View detailed properties and content statistics for each flow
- View live information or go back in time for forensic search

Your ICS Flight Recorder



Flows

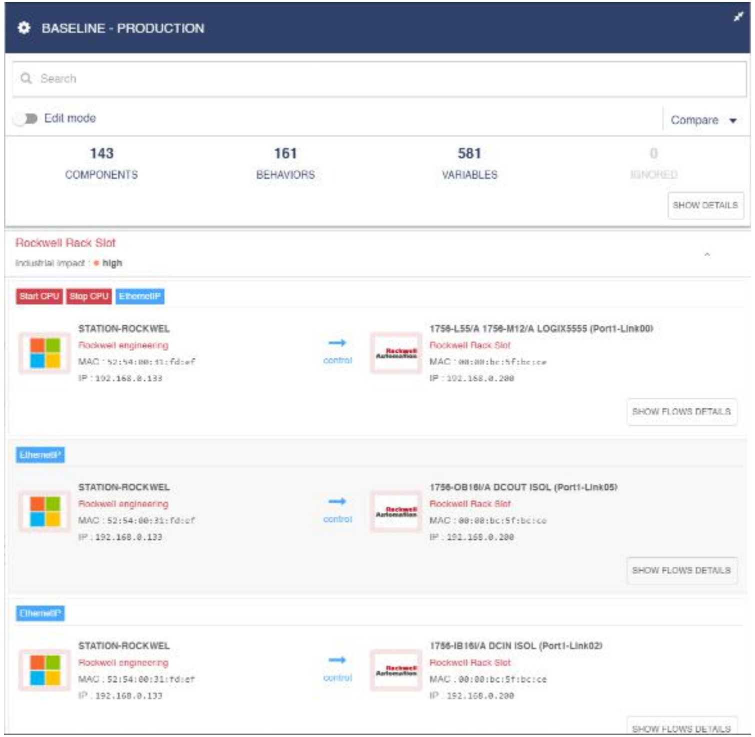
Content Statistics

Property	Value	Occurrences
emerson-udp-event	setvar	7
emerson-udp-function	KeepAlive	1
emerson-udp-function	Message	7
emerson-udp-var-name	PID1/MODE	1
emerson-udp-var-name	PID1/SP	6
emerson-udp-var-scope	CV	6
emerson-udp-var-scope	TARGET	1
emerson-udp-var-value	49.52	1
emerson-udp-var-value	49.97	1
emerson-udp-var-value	69.97	1
emerson-udp-var-value	70	1
emerson-udp-var-value	70.41	1
emerson-udp-var-value	72	1
emerson-udp-var-value	AUTO	1
ipv4-ttl	128	1
ipv4-ttl	64	1

Threat Detection: **Behavioral Analytics**

- Create Baselines to define normal behaviors and configurations
- Behavior modeling automatically triggers alerts on deviations to the baselines
- Import IoC to detect known malicious behaviors
- Continuously improve detection with classification of new events

Detect unknown attacks and malfunctions



BASELINE - PRODUCTION

Search

Edit mode

Compare

143	161	581	0
COMPONENTS	BEHAVIORS	VARIABLES	IGNORED

SHOW DETAILS

Rockwell Rack Slot

Industrial impact : ● high

Start CPU Stop CPU EthernetIP

STATION-ROCKWEL
Rockwell engineering
MAC : 52:54:00:31:fd:ef
IP : 192.168.0.133

→ control

1756-L55/A 1756-M12/A LOGIX5555 (Port1-Link00)
Rockwell Rack Slot
MAC : 00:00:bc:5f:bc:ce
IP : 192.168.0.200

SHOW FLOWS DETAILS

EthernetIP

STATION-ROCKWEL
Rockwell engineering
MAC : 52:54:00:31:fd:ef
IP : 192.168.0.133

→ control

1756-OB16I/A DCOUT ISOL (Port1-Link05)
Rockwell Rack Slot
MAC : 00:00:bc:5f:bc:ce
IP : 192.168.0.200

SHOW FLOWS DETAILS

EthernetIP

STATION-ROCKWEL
Rockwell engineering
MAC : 52:54:00:31:fd:ef
IP : 192.168.0.133

→ control

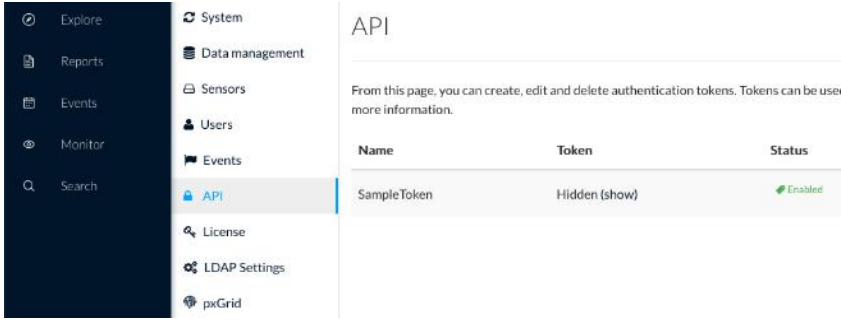
1756-IB16I/A DCIN ISOL (Port1-Link02)
Rockwell Rack Slot
MAC : 00:00:bc:5f:bc:ce
IP : 192.168.0.200

SHOW FLOWS DETAILS

Integrations and customization via **RESTful API**

- Access data about components and communication flows available in Cyber Vision
- Leverage sandboxed application hosting to automate functions and integrations
- Modify tag assignment, presets and groups programmatically
- Define custom analyzers for unknown traffic in environment

Integrate data from Cyber Vision into additional tools

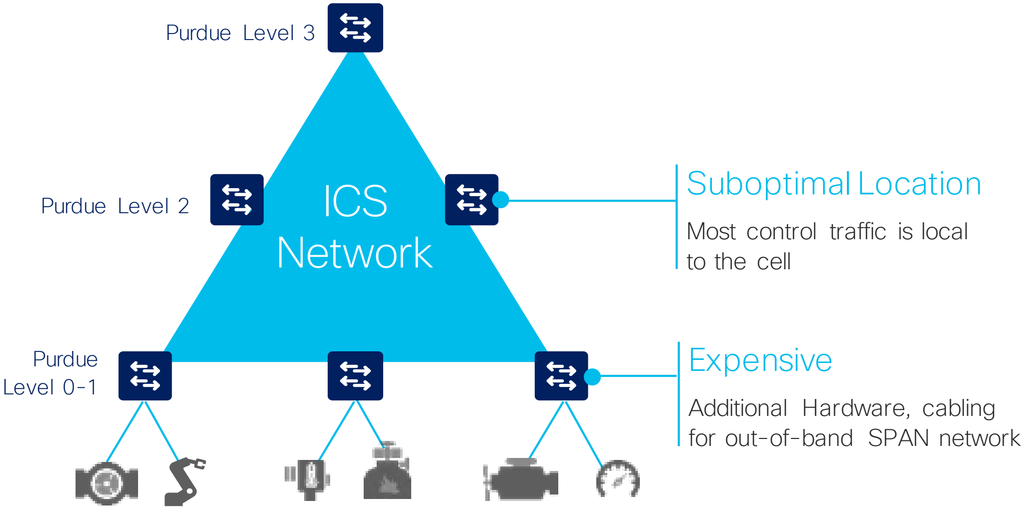


API

From this page, you can create, edit and delete authentication tokens. Tokens can be use
more information.

Name	Token	Status
SampleToken	Hidden (show)	Enabled

Why is a network-sensor important?



Suboptimal Location

Most control traffic is local to the cell

Expensive

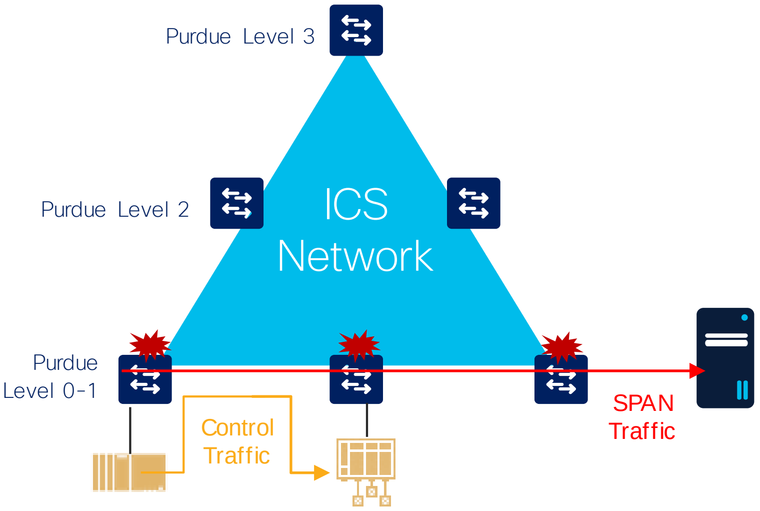
Additional Hardware, cabling for out-of-band SPAN network

DPI Location Matters!

- Mirroring traffic in at the aggregation layer results in visibility to only North-South traffic
- Mirroring traffic at the cell layer requires an expensive out-of-band SPAN network

Sensor embedded in the network sees everything that attaches to it

Why is a network-sensor important?



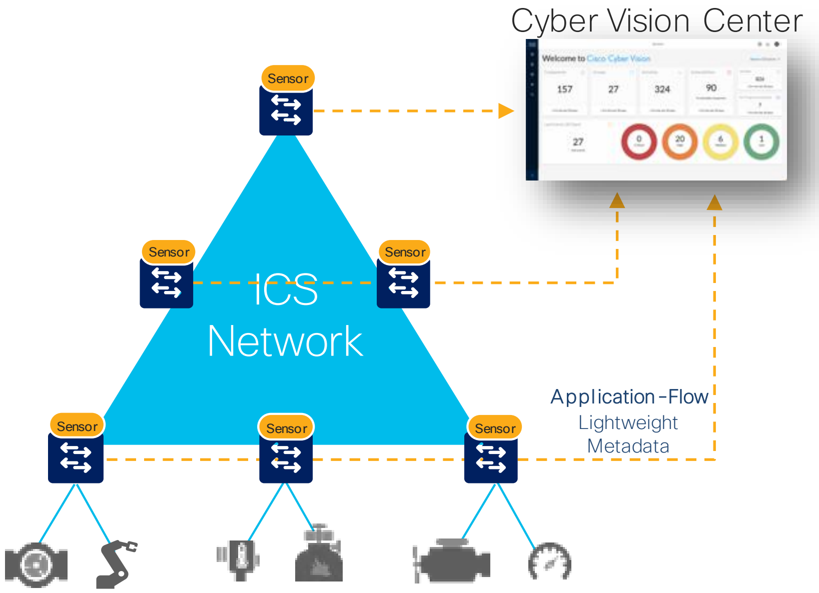
RSPAN introduces Jitter!

- Head-of-line blocking caused by Inline SPAN traffic negatively impacts time-sensitive control loop
- RSPAN in LANs is detrimental to control system performance

Sensor embedded in the network generates lightweight metadata that does not congest QoS queues

Visibility Using your Network Infrastructure

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



Monitoring at the Edge

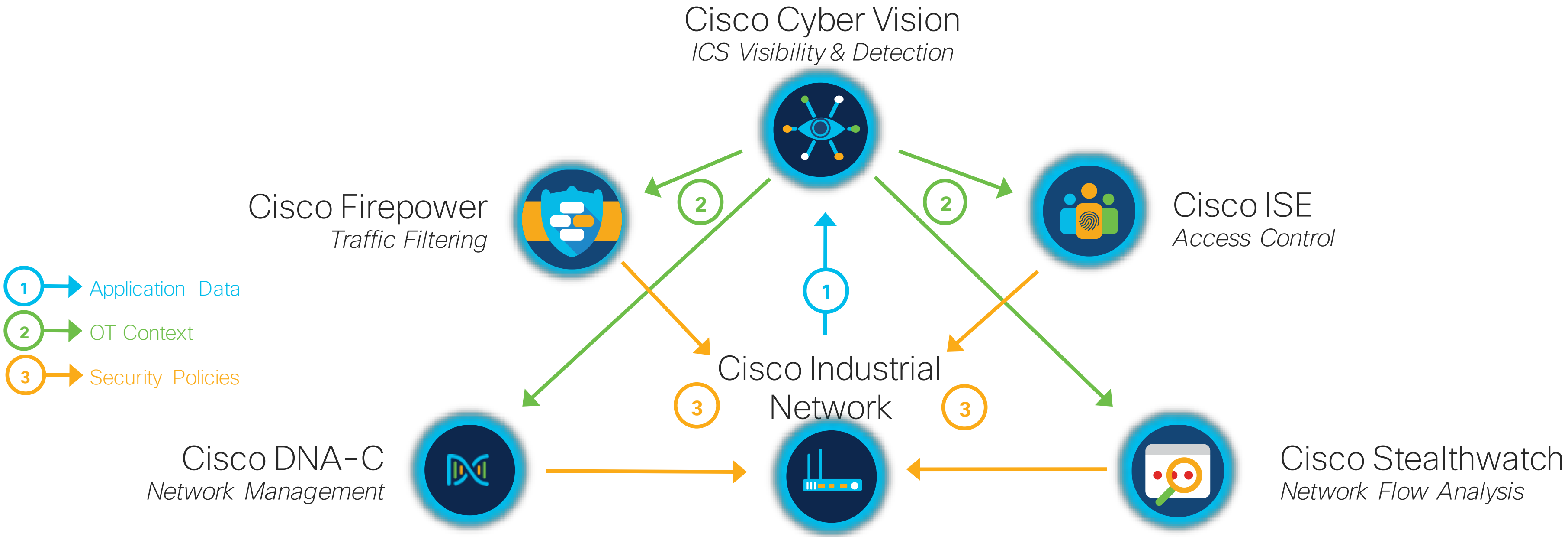
- Cyber Vision Sensors embedded into industrial network equipment
- No additional hardware needed
- No need for an out-of-band monitoring network

Easy deployment
Low TCO

cisco is the only vendor on the market with an edge strategy for OT cybersecurity

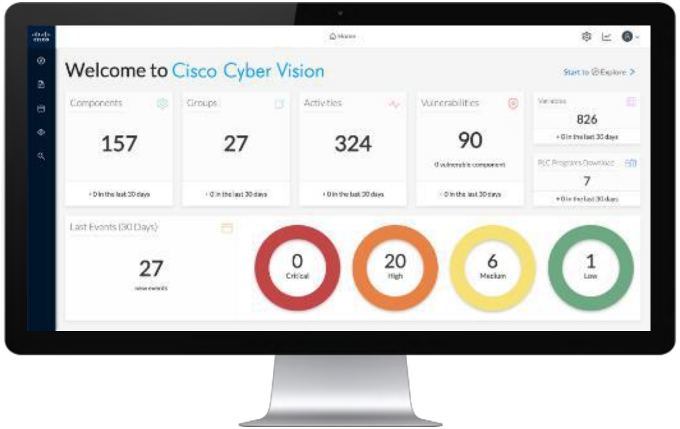
The Only Fully Integrated OT Security Solution

Working together to define & apply IoT security policies



Cisco ISE Integration

Extend security policies to your industrial network



Home

Welcome to Cisco Cyber Vision

Start to Explore >

Components 157 · 0 in the last 30 days

Groups 27 · 0 in the last 30 days

Activities 324 · 0 in the last 30 days

Vulnerabilities 90 · 0 vulnerable component · 0 in the last 30 days

Variables 826 · + 0 in the last 30 days

PLC Programs Download 7 · + 0 in the last 30 days

Last Events (30 Days) 27 new events

0 Critical

20 High

6 Medium

1 Low

pxGrid

Cisco ISE

- ISE endpoints are enriched with context from Cyber Vision
- Use ICS attributes (PLC, Siemens, Cell-1) to define profiling policy
- Segment your network to prevent malware and ransomware from spreading

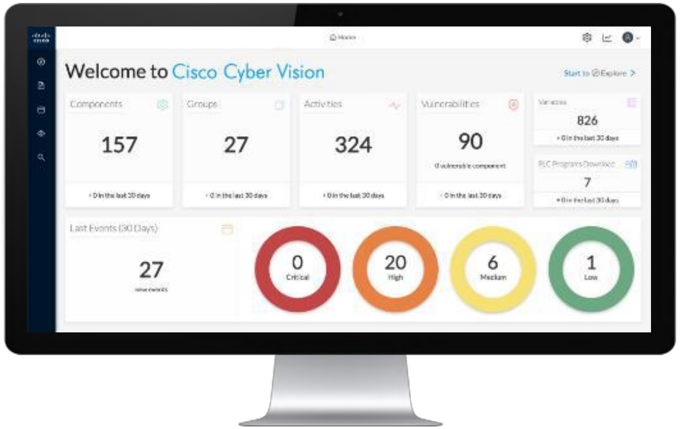
ICS Visibility

TrustSec

Cisco Industrial Network Provides Visibility and Enforces Security Policy

Cisco Stealthwatch Integration

Speed up incident response and forensics



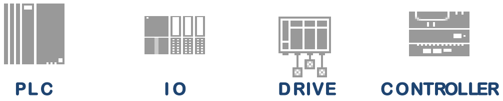
Welcome to Cisco Cyber Vision

Components	Groups	Activities	Vulnerabilities	Variables
157	27	324	90	826
0 in the last 30 days	0 in the last 30 days	0 in the last 30 days	0 in the last 30 days	+0 in the last 30 days

PLC Programs Download: 7

Last Events (30 Days): 27

ICS Visibility



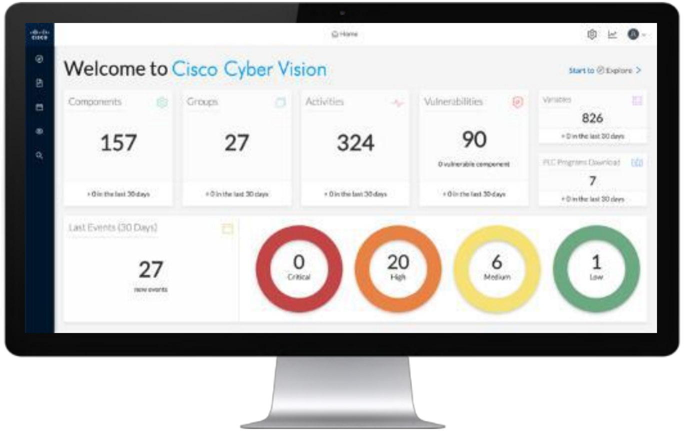
REST API

Cisco Stealthwatch

- Stealthwatch flows enriched with context from Cyber Vision
- Use ICS attributes (PLC, Siemens, Cell-1) to define host-group policy
- Pinpoint ICS assets when Stealthwatch raises alarms at Level-3 for north-south traffic from industrial network to the Enterprise

Cisco Firepower Integration

OT context for creating rules, remediation, and impact assessment



Home

Welcome to Cisco Cyber Vision

Start to Explore >

Components
157
+0 in the last 30 days

Groups
27
+0 in the last 30 days

Activities
324
+0 in the last 30 days

Vulnerabilities
90
0 vulnerable component
+0 in the last 30 days

Variables
826
+0 in the last 30 days

PLC Program Download
7
+0 in the last 30 days

Last Events (30 Days)
27
new events

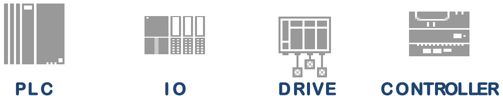
0 Critical

20 High

6 Medium

1 Low

ICS Visibility



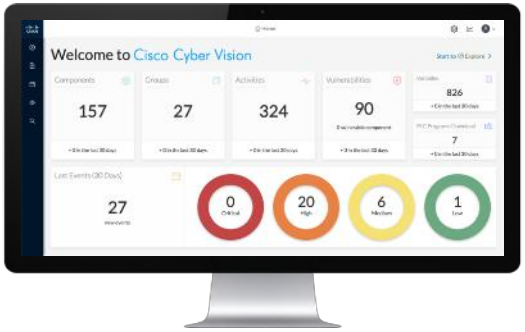
Cisco Firepower

- Map ICS device IP to named objects (PLC, IO, Drive) in Firepower for use in access policy*
- Map ICS device vulnerabilities to Hosts in Firepower for use in correlation policy*
- Identify anomalous flows in Cyber Vision and kill FTD Firewall sessions

* Spring 2020

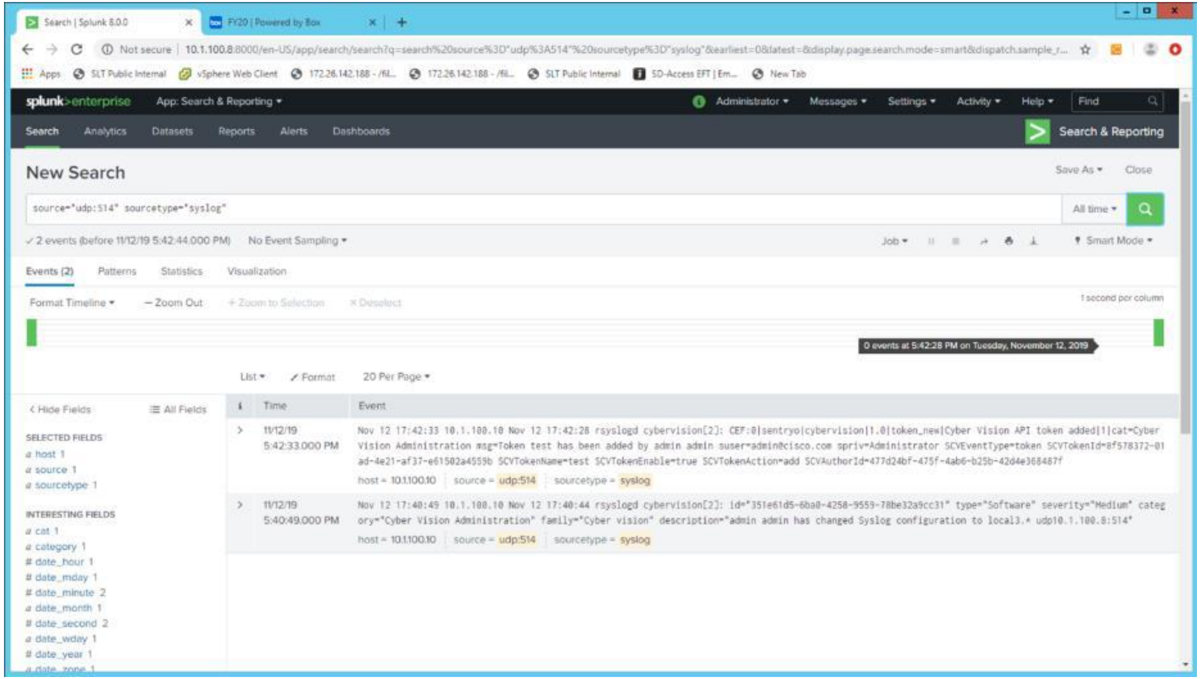
Splunk Integration

Unified IT/OT security events management in SIEM



ICS Visibility

Syslog



New Search

```
source="udp:514" sourcetype="syslog"
```

✓ 2 events (before 11/12/19 5:42:44.000 PM) No Event Sampling ▾

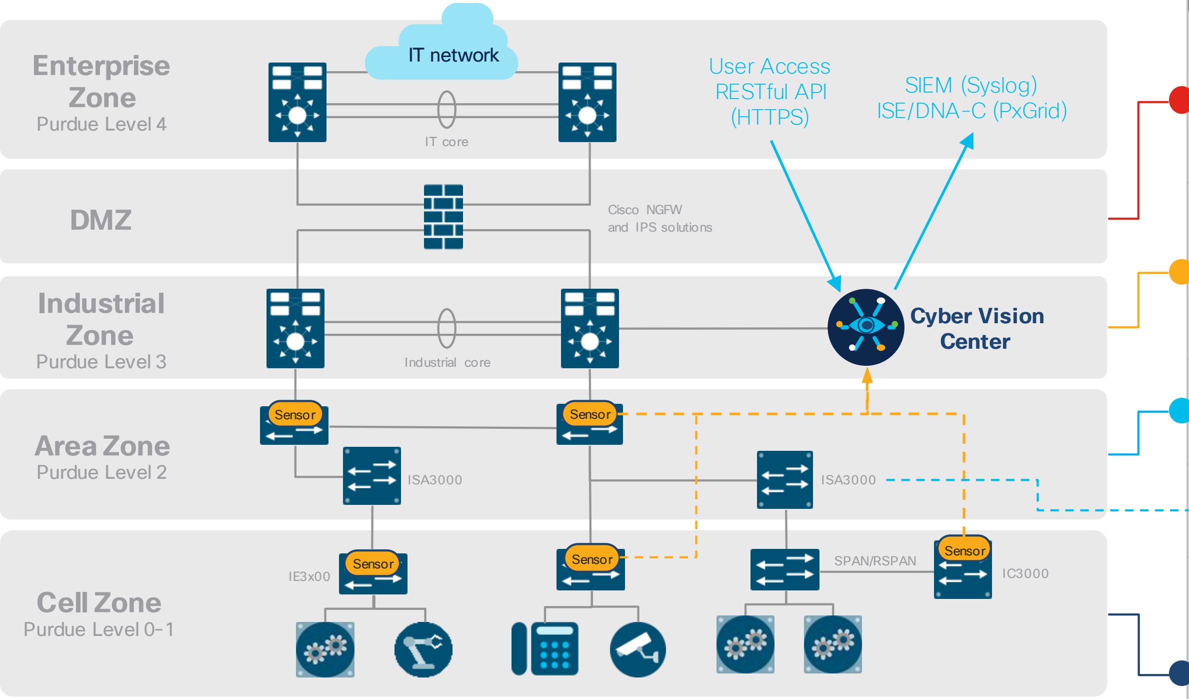
0 events at 5:42:28 PM on Tuesday, November 12, 2019

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
a cat 1
a category 1
# date_hour 1
# date_mday 1
# date_minute 2
a date_month 1
# date_second 2
a date_wday 1
# date_year 1
a date_zone 1

i	Time	Event
>	11/12/19 5:42:33.000 PM	Nov 12 17:42:33 10.1.100.10 Nov 12 17:42:28 rsyslogd cybervision[2]: CEF:0|sentryo|cybervision|1.0|token_new|Cyber Vision API token added|1|cat=Cyber Vision Administration msg=Token test has been added by admin admin suser=admin@cisco.com spriv=Administrator SCVEventType=token SCVTokenId=8f578372-01ad-4e21-af37-e61502a4559b SCVTokenName=test SCVTokenEnable=true SCVTokenAction=add SCVAuthorId=477d24bf-475f-4ab6-b25b-42d4e368487f host = 10.1.100.10 source = udp:514 sourcetype = syslog
>	11/12/19 5:40:49.000 PM	Nov 12 17:40:49 10.1.100.10 Nov 12 17:40:44 rsyslogd cybervision[2]: id="351e61d5-6ba0-4258-9559-78be32a9cc31" type="Software" severity="Medium" category="Cyber Vision Administration" family="Cyber vision" description="admin admin has changed Syslog configuration to local3.* udp10.1.100.8:514" host = 10.1.100.10 source = udp:514 sourcetype = syslog

Converged Industrial Architectures



Cisco Components	
Industrial DMZ	• Access control lists (ACLs) • Intrusion detection systems (IDS) and intrusion prevention systems (IPS) • VPN services • Portal and remote desktop services • Application and data mirrors
Industrial zone	• AAA identity services • Network management • Asset inventory • Anomaly detection • Plant-wide services • Traffic enforcement (plant to IDMZ, north/south)
Area zone	• Traffic Enforcement (Cell to Cell, East/West) • QoS Prioritization • SXP • Netflow
Inter-cell (ISA3000)	• Industrial deep packet inspection (DPI) • Stateful firewall and intrusion prevention (IPS) • Hardware bypass
Cell zone	• PoE/PoE+ • Layer 2 NAT • 802.1X • MAC Authentication Bypass (MAB) • Quality of Service marking • Netflow (IE3x00 and IE4000 only) • TrustSec tagging (IE3x00 and IE4000 only) • Edge compute (IE3x00 only)

cisco