

Designing IoT Aware Enterprise

Vinay Saini – Sr. Solutions Architect
@vinsaini
DGTL-BRKENS-1200



June 2-3, 2020 | ciscolive.com/us

#CiscoLive





Agenda

Exploring IoT in Enterprise

- Defining IoT
- IoT use cases for enterprise
- Challenges for adopting

Creating IoT ready Secure Architecture

- IoT visibility using Cisco ISE and IND
- Secure Onboarding using MUD
- OT visibility using Cybervision

Auto Segmentation using Cisco SD-Access

- Cisco SD-Access basics
- Micro and macro segmentation
- Policy Extension for OT areas

Your Presenter Today



Vinay Saini 

Sr. Solutions Architect – Cisco CX

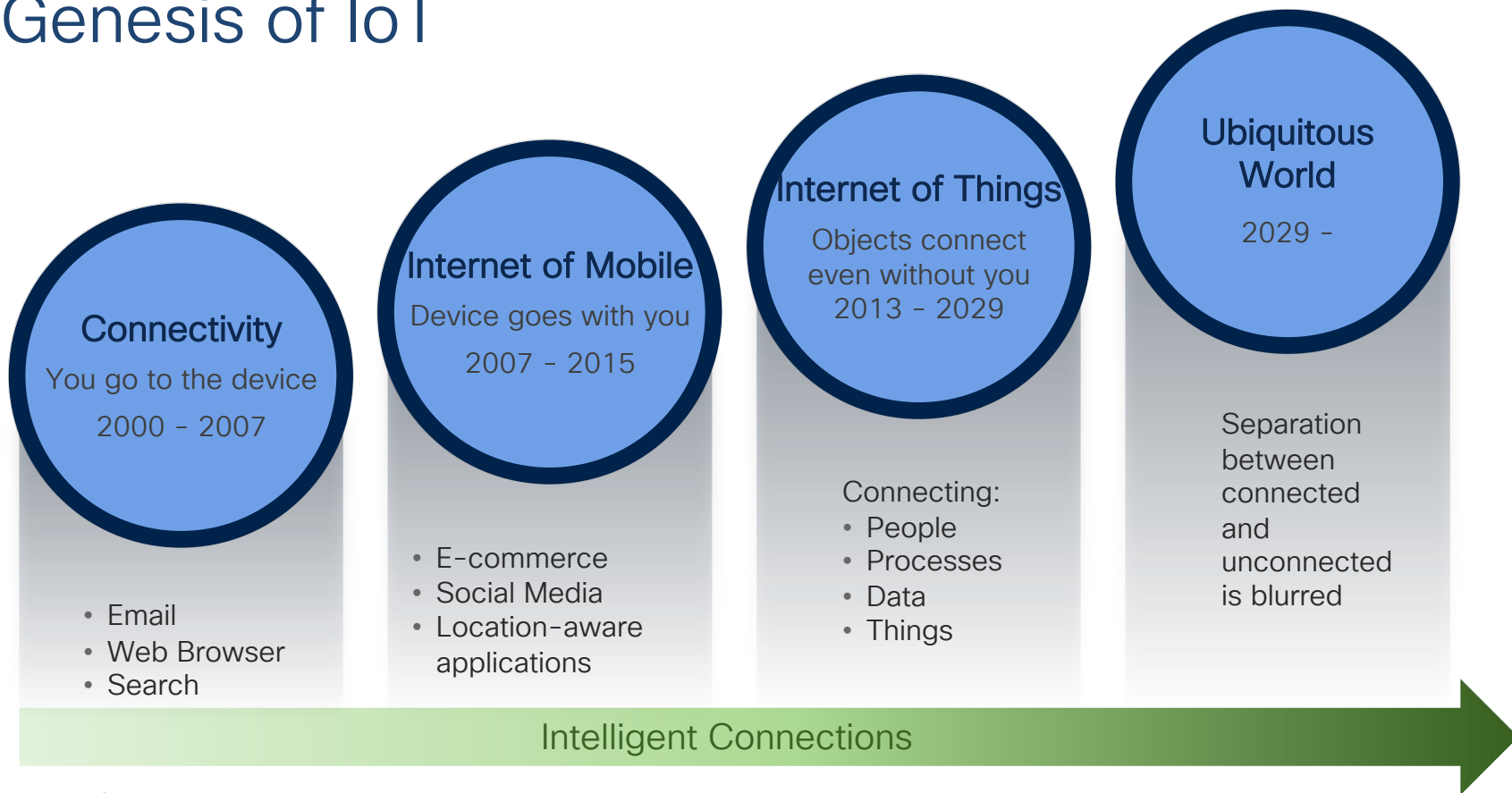
- 16+ years in Enterprise & IIoT Industry
- CCIE Wireless#38448, CWNE#69
- Active Contributor to Cisco Certification programs.
- Tsdsi (3gpp) member.



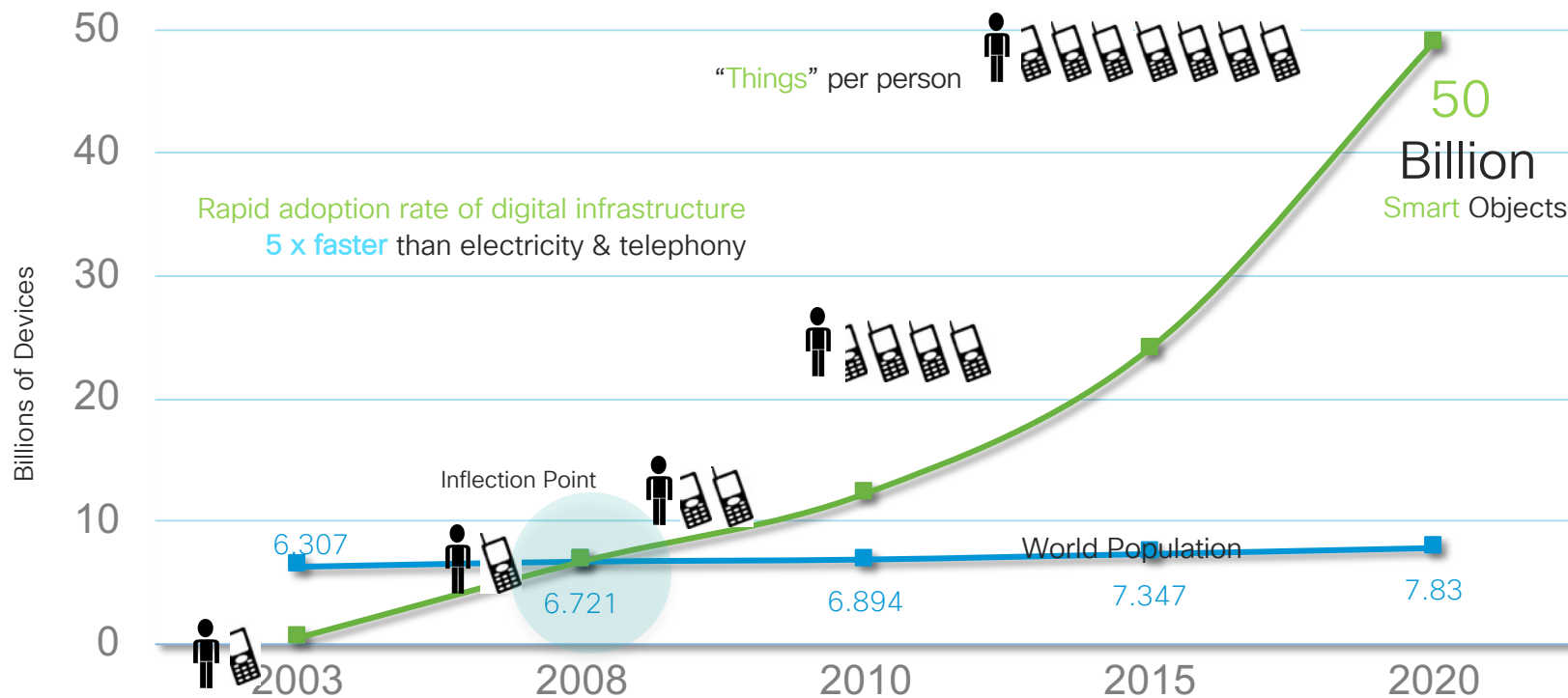
IoT is confusing



Genesis of IoT

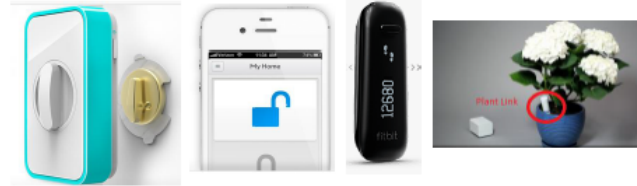


Are There That Many “Things”?



Digitization: Connecting More Than “Things”

Things – Includes machines, devices, sensors, consumer products, vehicles, etc.



Systems – Includes business applications, ERP/CRM/PLM systems, analytics systems, data warehouses, and control systems

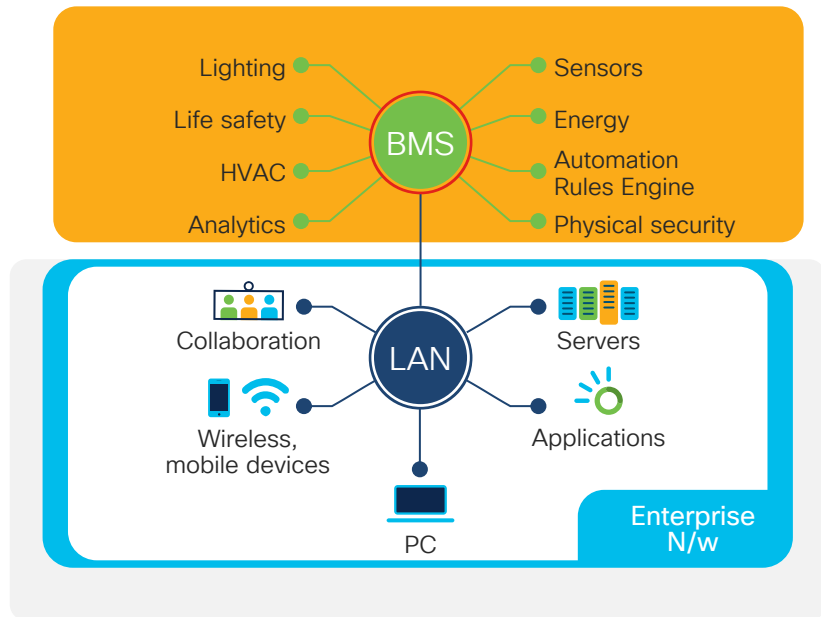


People – Includes workers and consumers, employees, partners and customers

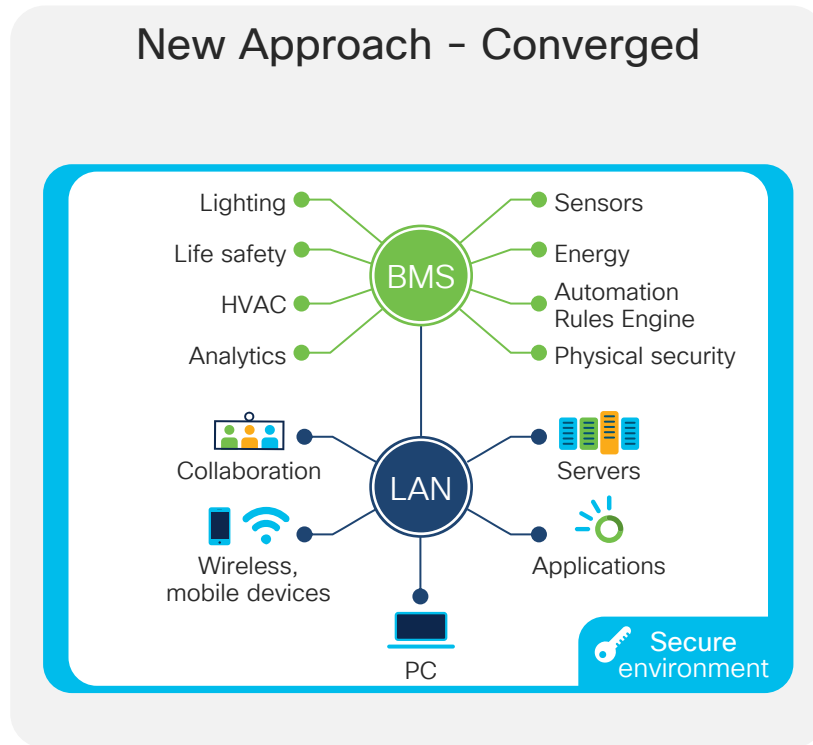


IoT landscape in the Enterprise

Traditional – Isolated BMS & IoT



New Approach – Converged



Enterprise boundaries are Extending

Non-Carpeted / Outdoor Spaces



Roadways



Parking Lot



Distribution Center



Airport



Manufacturing



Port/Terminal

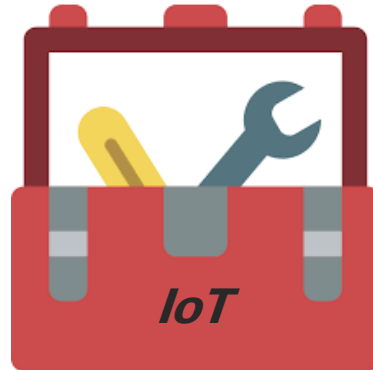


Warehouse

Extended Enterprise areas

Building an Architecture

- An IoT Project should be just like any other project
 - You work on the requirements to develop a blueprint before buying the tools to start building
- However, IoT was not “designed”, it “happened”:
 - Multiple specialized / vertical solutions
 - Multiple requirements
 - Multiple sensor types
 - Multiple applications
 - Multiple protocols



IoT use-cases for an Enterprise

Digital Building



- Sensor Networks
- Building Management System
- HVAC
- Video Surveillance

Extended Enterprise



- Outdoor Areas
- OT Area
- Non carpeted Sensor network area
- Security Surveillance

IoT Networking Portfolio



Industrial Switching



IE 1K, 2K, 3K, 4K, 5K, CGS, 3x00

IoT Gateways



819-MNA, IR807, IR809,
IR829, IR1101

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



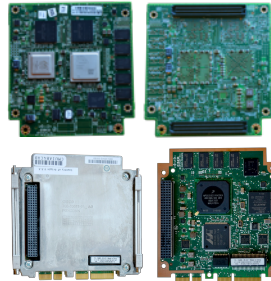
AP1552, IW3702

Industrial Security



ISA 3000

Embedded IoT



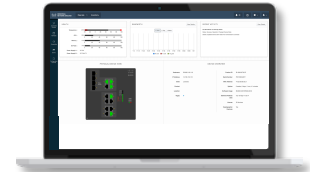
ESS, ESR

Edge Computing



IOx
IC 3000







Management & Automation



Field Network Director
Industrial Network Director



IoT Architecture Requirements & Challenges

Large Scale 	Hundreds of clients in a single network! IPv4 vs IPv6
Security 	Sensors exposed to the world, data travels through public networks...
Constrained Devices 	Lossy networks, low bandwidth, small batteries...
Large Volume 	Small but large amount of data
Legacy Support 	Non-IP, specialized devices, multiple vertical solutions...
Need for Real Time 	What happens now may result in proactive action...

Business Challenges for IoT Use-cases



Device Visibility

Do you know
devices well
enough to
differentiate
service?



Intent-based Policy

Does you know
behavior of devices
to build their
policy?



On Boarding

Is there any
standard way of
connecting IoT
devices to
enterprise network?

Device visibility and network segmentation are critical

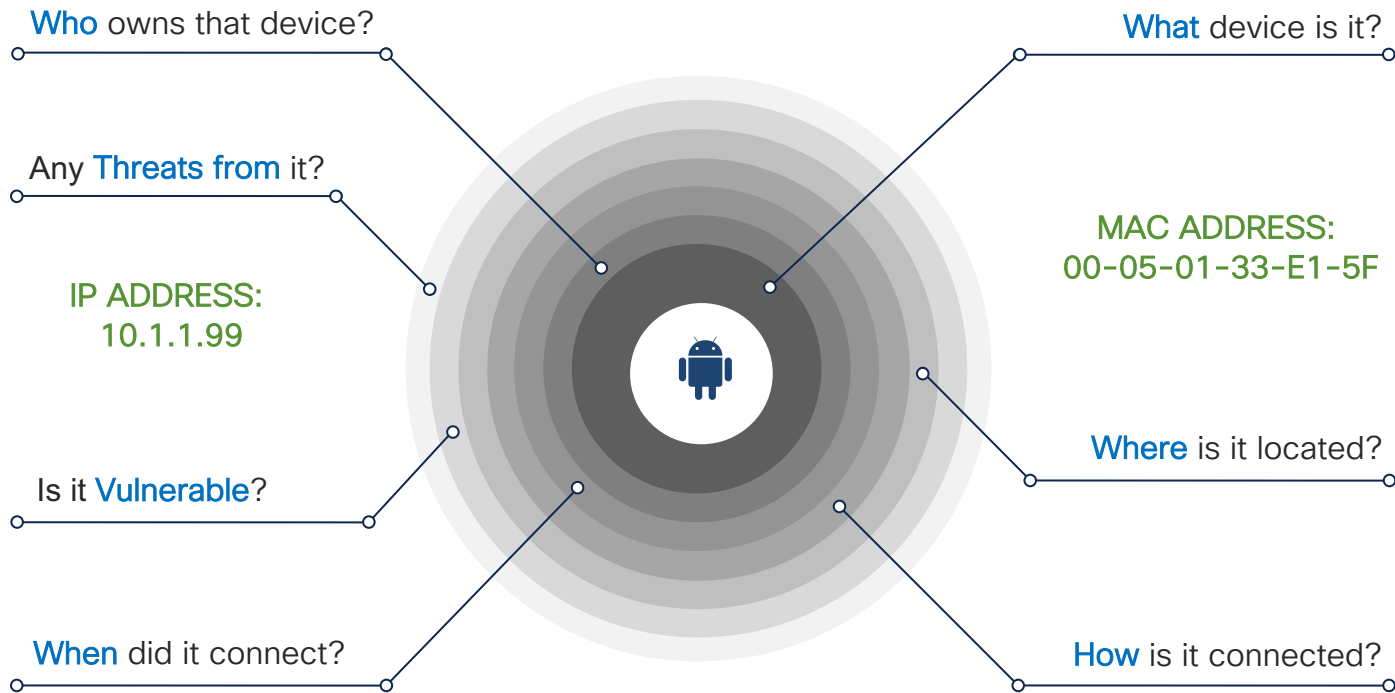


How do I know what's on my network?

How do I make sure devices only have access to what they need?

Lack of visibility

How to run the network with so many unknowns?



Take Away from this section



- Enterprise networks needs to evolve for IoT use-cases
- IoT use-cases could be in carpeted or extended outdoor areas.
- Security, Visibility & Onboarding are key challenges for IoT onboarding.



Agenda

Exploring IoT in Enterprise

- Defining IoT
- IoT use cases for enterprise
- Challenges for adopting

Creating IoT ready Secure Architecture

- IoT visibility using Cisco ISE and IND
- Secure Onboarding using MUD
- OT visibility using Cybervision

Auto Segmentation using Cisco SD-Access

- Cisco SD-Access basics
- Micro and macro segmentation
- Policy Extension for OT areas

The background is a dark blue field filled with numerous small, semi-transparent squares and dots in various colors including light blue, green, yellow, orange, and red. These elements are scattered across the frame, with a higher concentration of larger squares in the upper left and a trail of smaller dots and squares extending from the upper right towards the bottom right.

Creating IoT Aware Network

Pillars of IoT aware network



Security with Scale



Monitoring & Visibility across domains

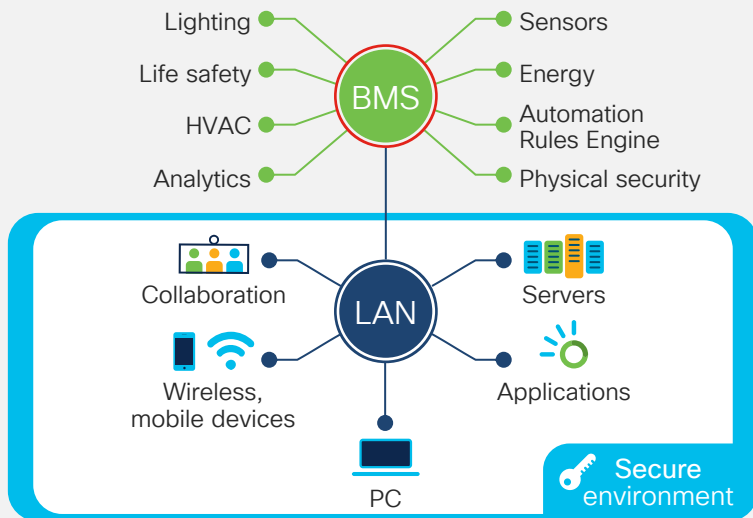


Segmentation with automation

Converged Systems

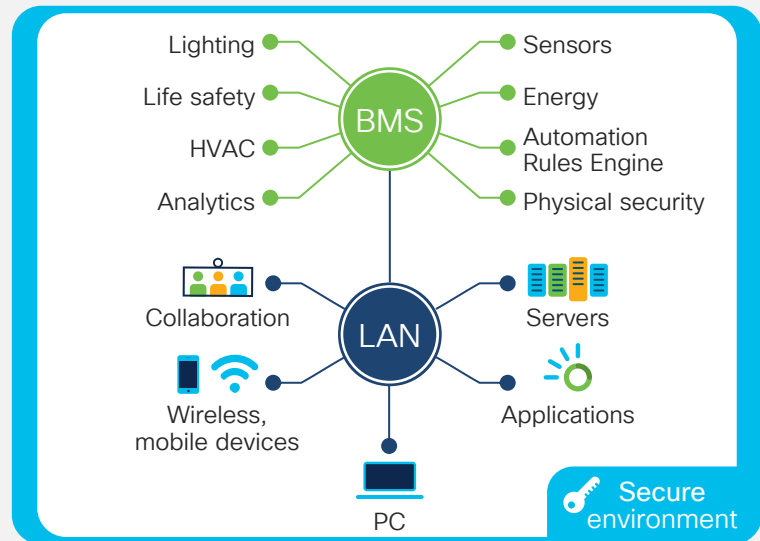
Traditional approach

Isolated BMS and OT networks

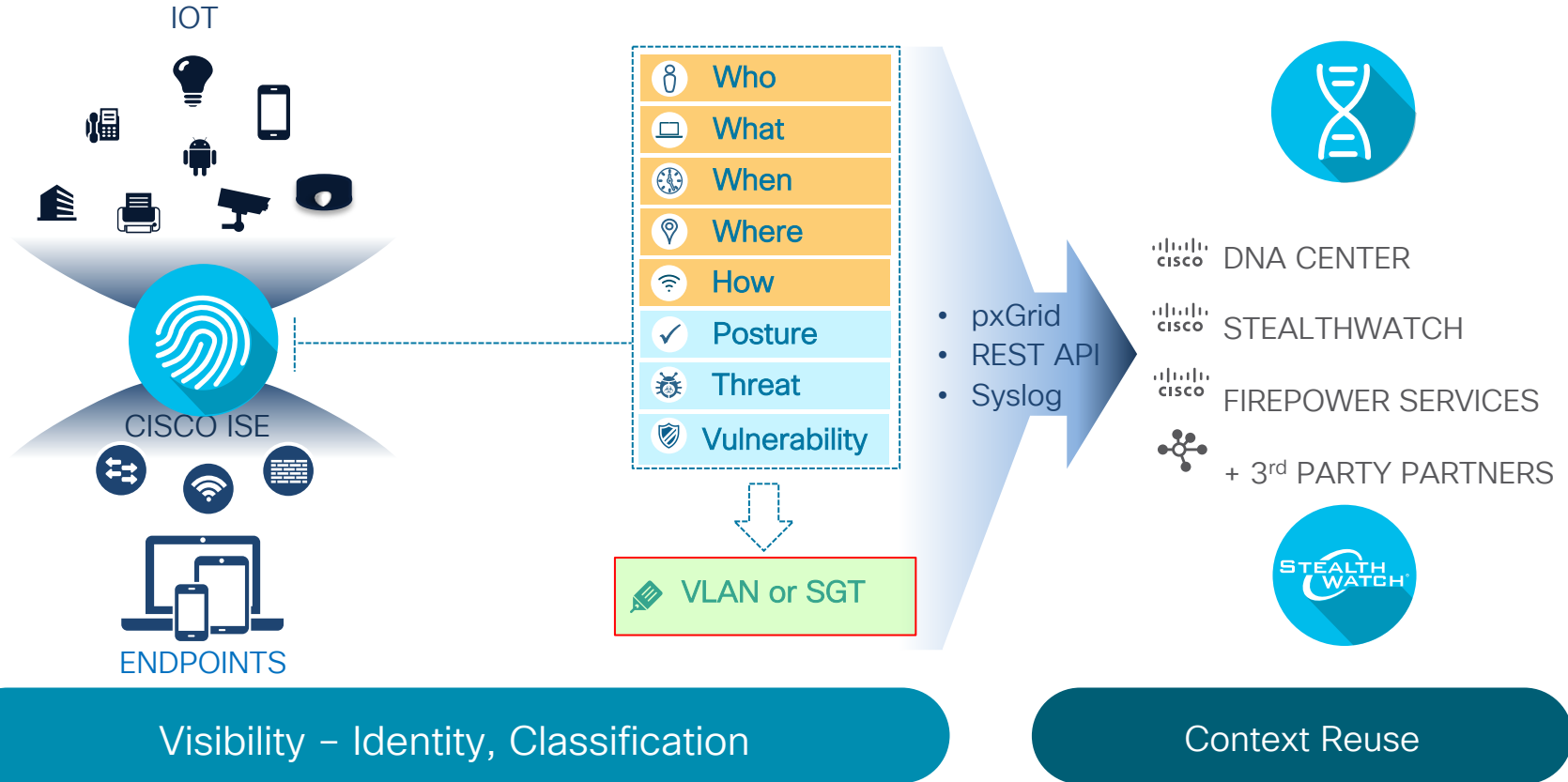


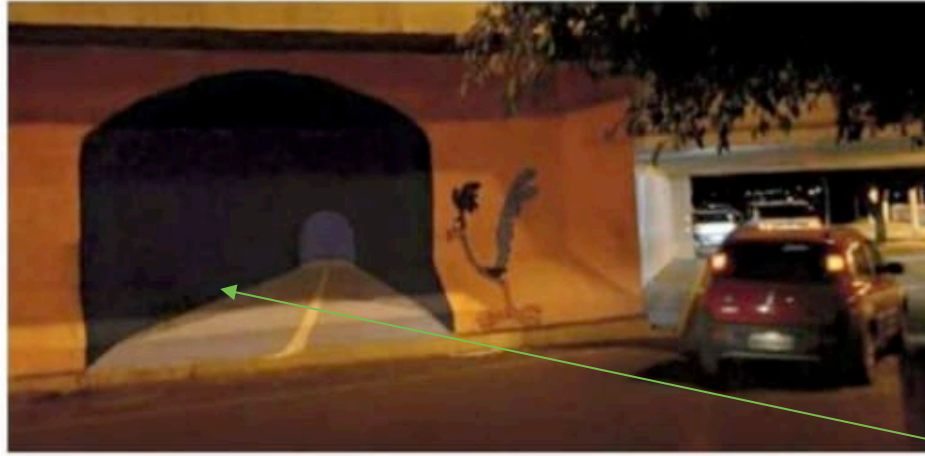
Converged approach

BMS and all smart building automation and control systems are **connected by Cisco technology**.



Standard segmentation using ISE





Graffiti

The background is a dark blue field filled with numerous small, semi-transparent squares and dots in various colors including light blue, green, yellow, orange, and red. These elements are scattered across the frame, with a higher concentration of yellow and orange squares forming a diagonal streak from the top right towards the bottom right.

Extending IoT visibility using ISE & IND

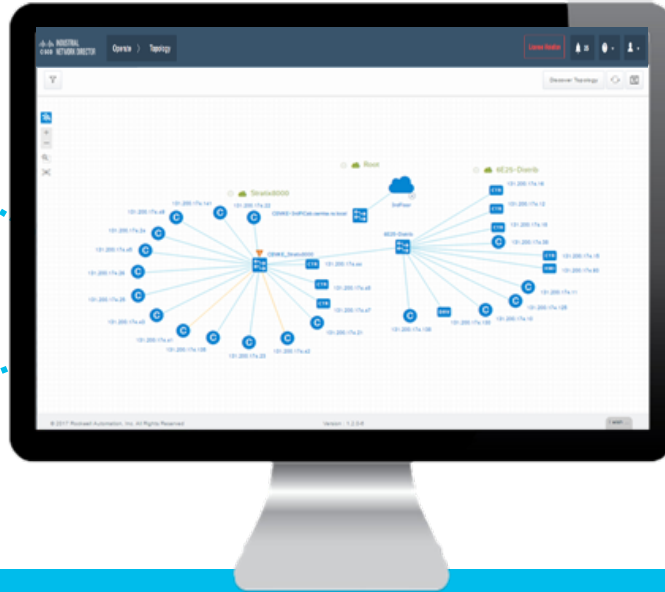
Cisco Industrial Network Director

Network Management, Simplified & Automated



Native industrial
protocol support

Plug-and-Play Day-0
configuration



Dashboard for monitoring
system health, metrics,
and traffic statistics

Alarm management
with real-time alerts of
network events



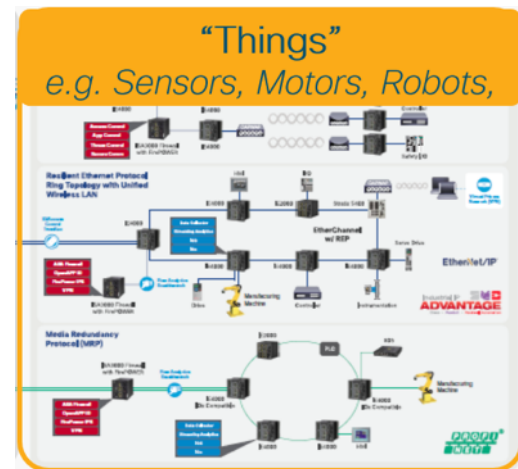
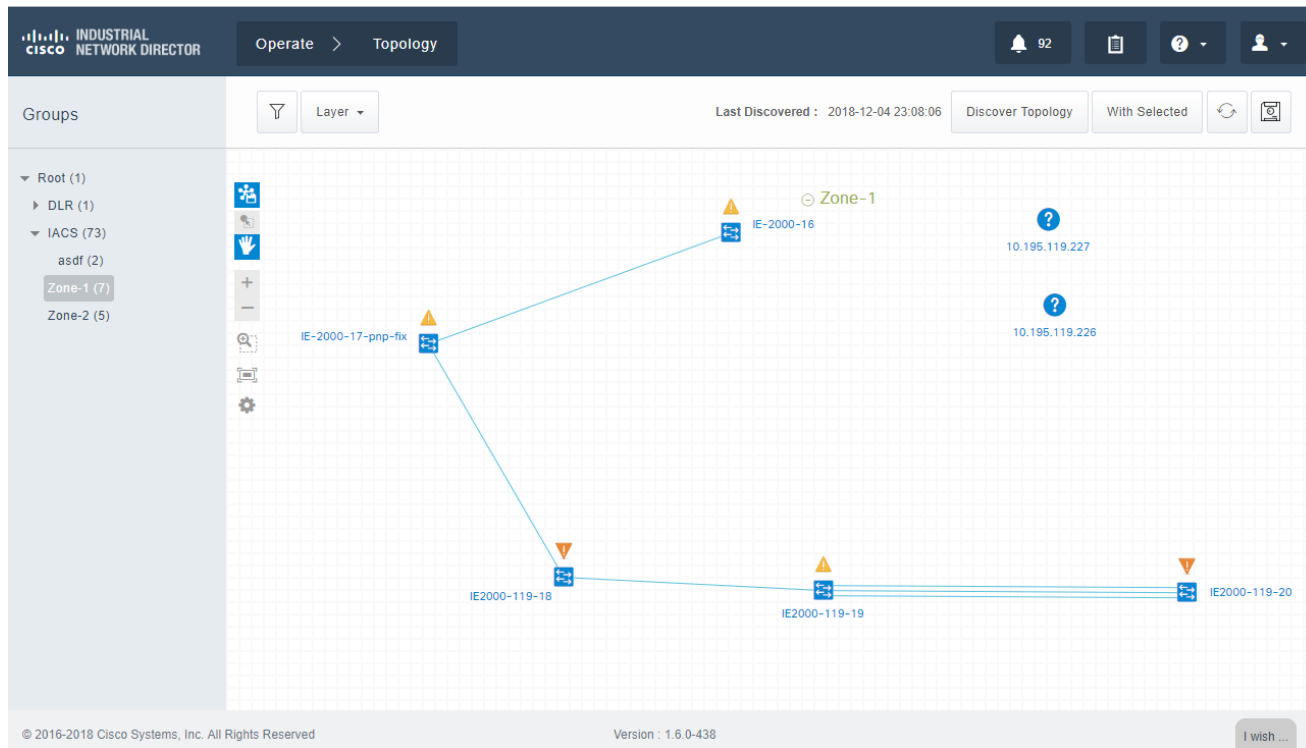
Plug-and-Play for Zero-Touch
Switch Commissioning

Improved Industrial
Asset Visibility

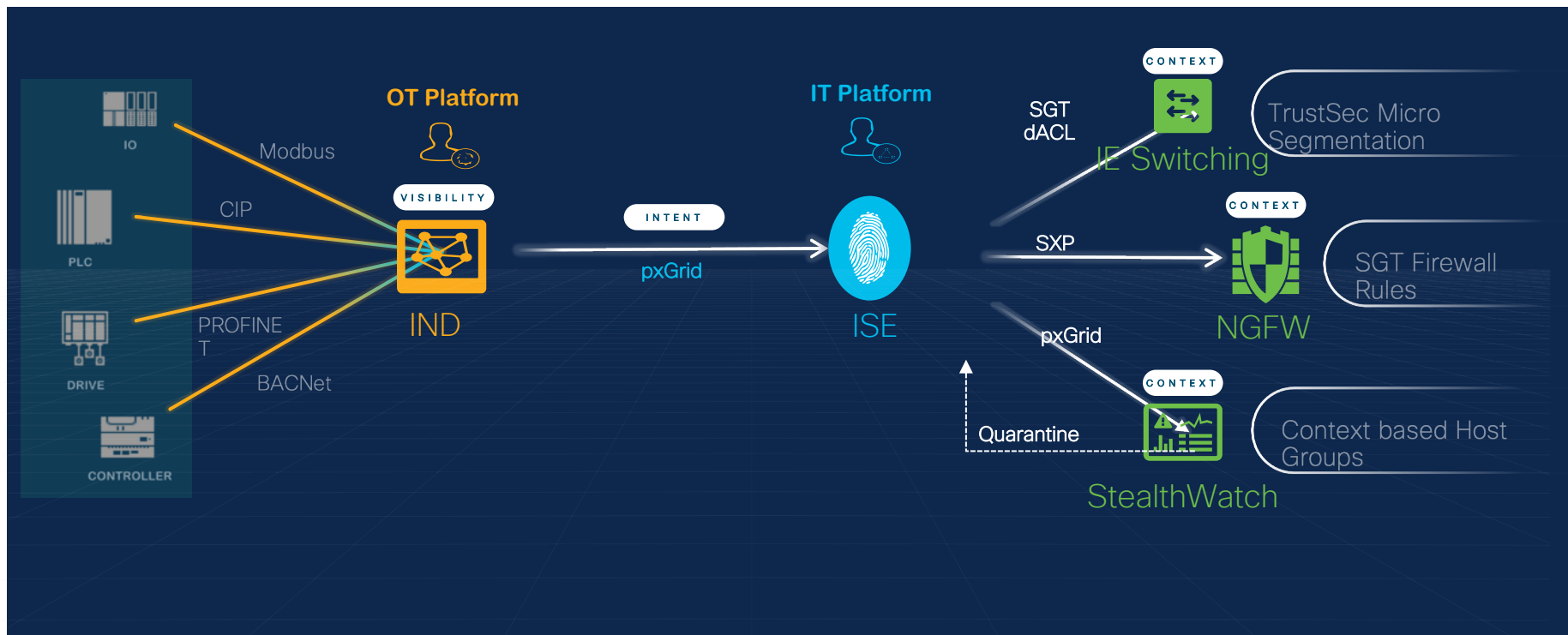
Network Troubleshooting with
Automation Context

APIs for Integration with
Automation Systems

Industrial Network Director: Machine Level Discovery



IoT Threat Defense



Visibility in IoT Networks

Security starts with Visibility

Discover Industrial Assets
using CIP, PROFINET,
Modbus, BACNet
Protocols



Visualize connectivity
between automation and
networking assets



Industrial
Network
Director



Identity
Services
Engine

Context Enhances Security

Who		Bob
What		Rockwell PLC
When		11:00 AM EST on April 10 th
Where		Extrusion, Zone-2, Cell-1
How		Wired Access
Compliance		Yes
Threat		None
Vulnerability		CVSS score of 6

IND shares OT asset identity with ISE over pxGrid

... this Visibility combined with Context, becomes a force-multiplier for Security

ISE device profiles

Medical profiles XML upload. Profiling data collection via usual means



Industrial Asset Visibility with IND



IND Asset Inventory

```
{
  "iotId": 105,
  "iotName": "172.27.162.184",
  "iotIpAddress": "172.27.162.184",
  "iotMacAddress": "00:1d:9c:c2:7d:d2",
  "iotVendor": "Rockwell Automation/Allen-Bradley",
  "iotProductId": "1756-EN2TR/B",
  "iotSerialNumber": "10423738",
  "iotDeviceType": "Ethernet/IP Node",
  "iotSwRevision": "4.2",
  "iotHwRevision": "2.0",
  "iotProtocol": "CIP",
  "iotConnectedLinks": [
    {
      "iotId": 103,
      "iotDeviceType": "Switch",
      "iotName": "IE3010-TrunkSwitch",
      "iotPortName": "FastEthernet0/13",
      "iotIpAddress": "172.27.162.162"
    }
  ],
  "iotCustomAttributes": [
    {
      "attrName": "deviceProfile",
      "Value": "Communications Adapter"
    },
    {
      "attrName": "productNode",
      "Value": "242"
    }
  ]
}
```

pxGrid



Identity
Services
Engine

ISE Profiler Attributes

iotMacAddress

iotIpAddress

iotName

iotVendor

iotProductId

iotSerialNumber

iotDeviceType

iotSwRevision

iotHwRevision

iotProtocol

iotConnectedLinks

iotCustomAttributes

ISE profiling rules based on attributes like *Make, Model, Serial Number, Device Type* etc. instead of just IP address

Custom Attributes allows IND to signal higher order information that is common to a group of assets

pxGrid-In

Probe Attributes

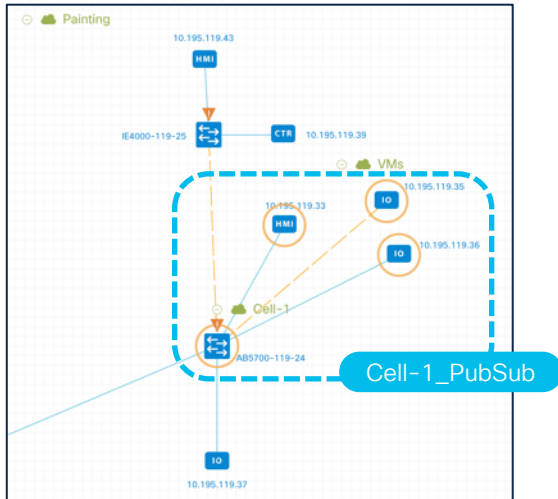
- Endpoint Attribute Details
- Core set of pxGrid Profile attributes
- Vendors can also send custom attributes

Cisco Identity Services Engine	
Home	Context Visibility
Operations	
Endpoints	Users
Network Devices	Application
MACAddress	00:1D:9C:CA:85:8B
MatchedPolicy	Rockwell-Automation-Device
StaticAssignment	false
StaticGroupAssignment	false
Total Certainty Factor	5
assetConnectedLinks.assetDeviceType	Switch
assetConnectedLinks.assetId	40109
assetConnectedLinks.assetIpAddress	10.195.119.22
assetConnectedLinks.assetName	IE4000-119-22
assetConnectedLinks.assetPortName	GigabitEthernet1/2
assetDeviceType	Controller
assetId	60100
assetIpAddress	10.195.119.38
assetMacAddress	00:1d:9c:ca:85:8b
assetName	10.195.119.38
assetProductId	1756-EN2TR/C 217021900
assetProtocol	CIP
assetSerialNumber	12174476
assetVendor	Rockwell Automation/Allen-Bradley
ip	10.195.119.38

pxGrid Probe
Attributes
from IND

IND to ID Assets > ISE for Policy > NW as Enforcer

IND Topology View



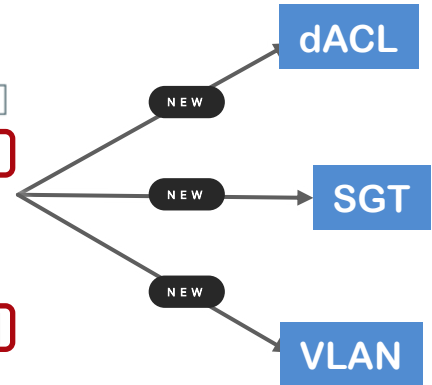
ISE Profiling Policy

Profiler Condition List > **New Profiler Condition**

Profiler Condition

* Name	Custom_Attribute_Check5
* Type	CUSTOMATTRIBUTE
* Attribute Name	AssetDB_Device_Type
* Operator	STARTSWITH
* Attribute Value	Cell-1_PubSub
System Type	Administrator Created

ISE Authorization Policy



1

OT user selects assets on IND topology and assigns Label = Cell-1_PubSub, which results in a pxGrid update

2

ISE profiling based on Custom Attribute results in new TrustSec Policy Assignment

Onboarding IoT device using MUD

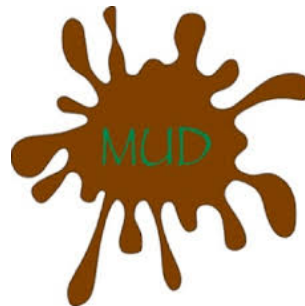
We need something to answer these ?

What is this thing?

Who is responsible for it?

What access does it need?

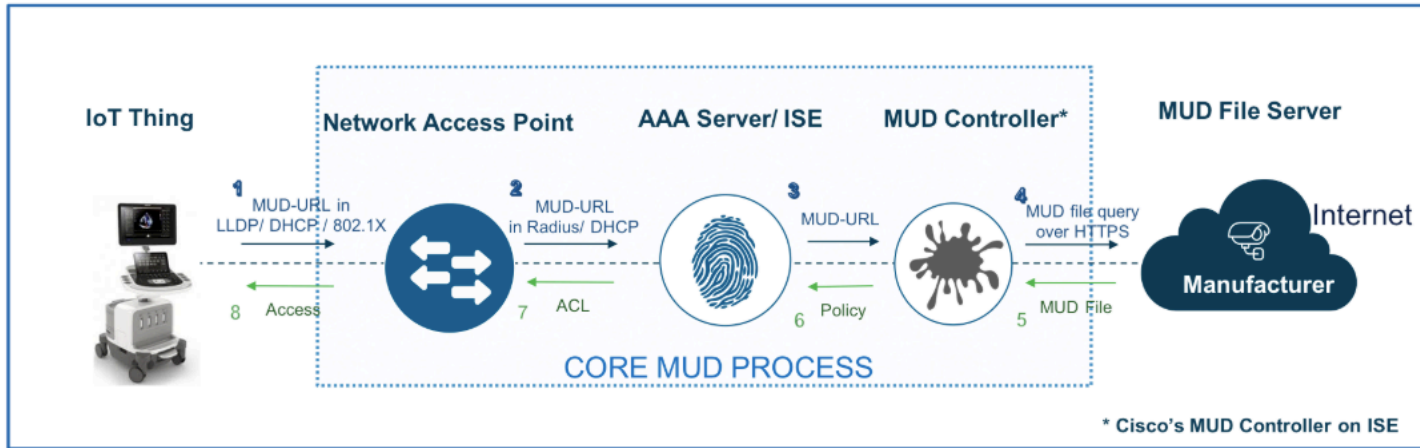
Is it doing what it should be doing?



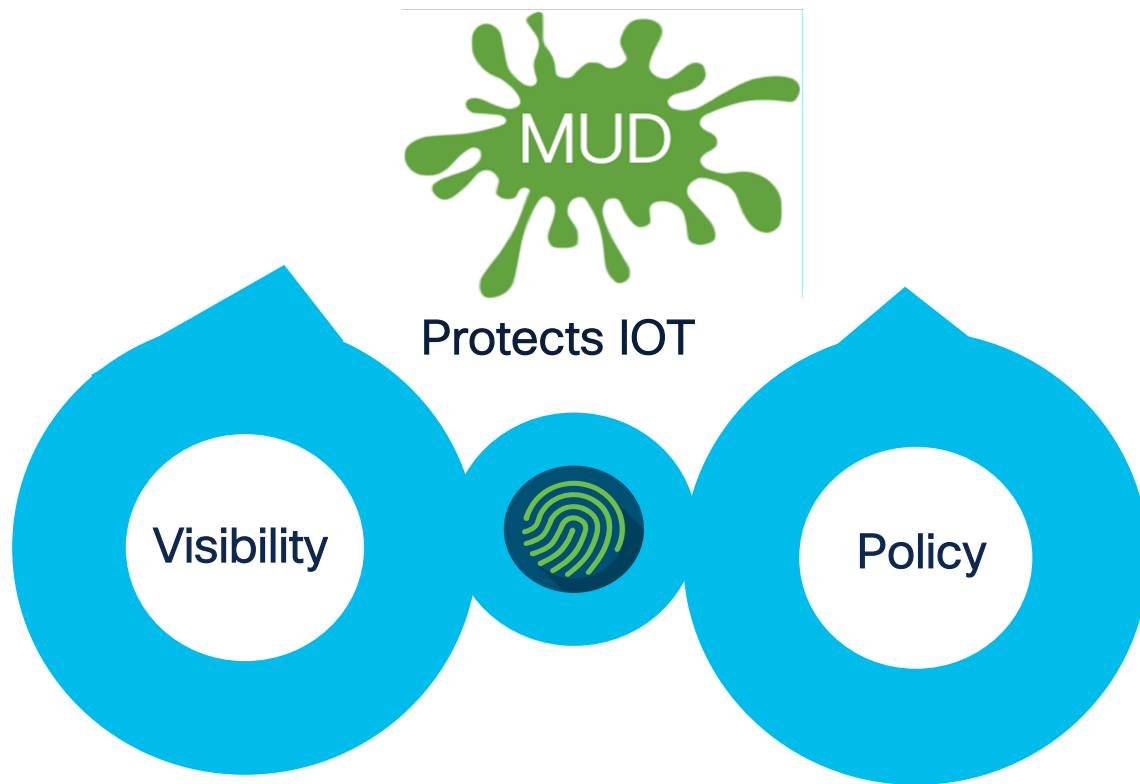
Manufacturer Usage Description

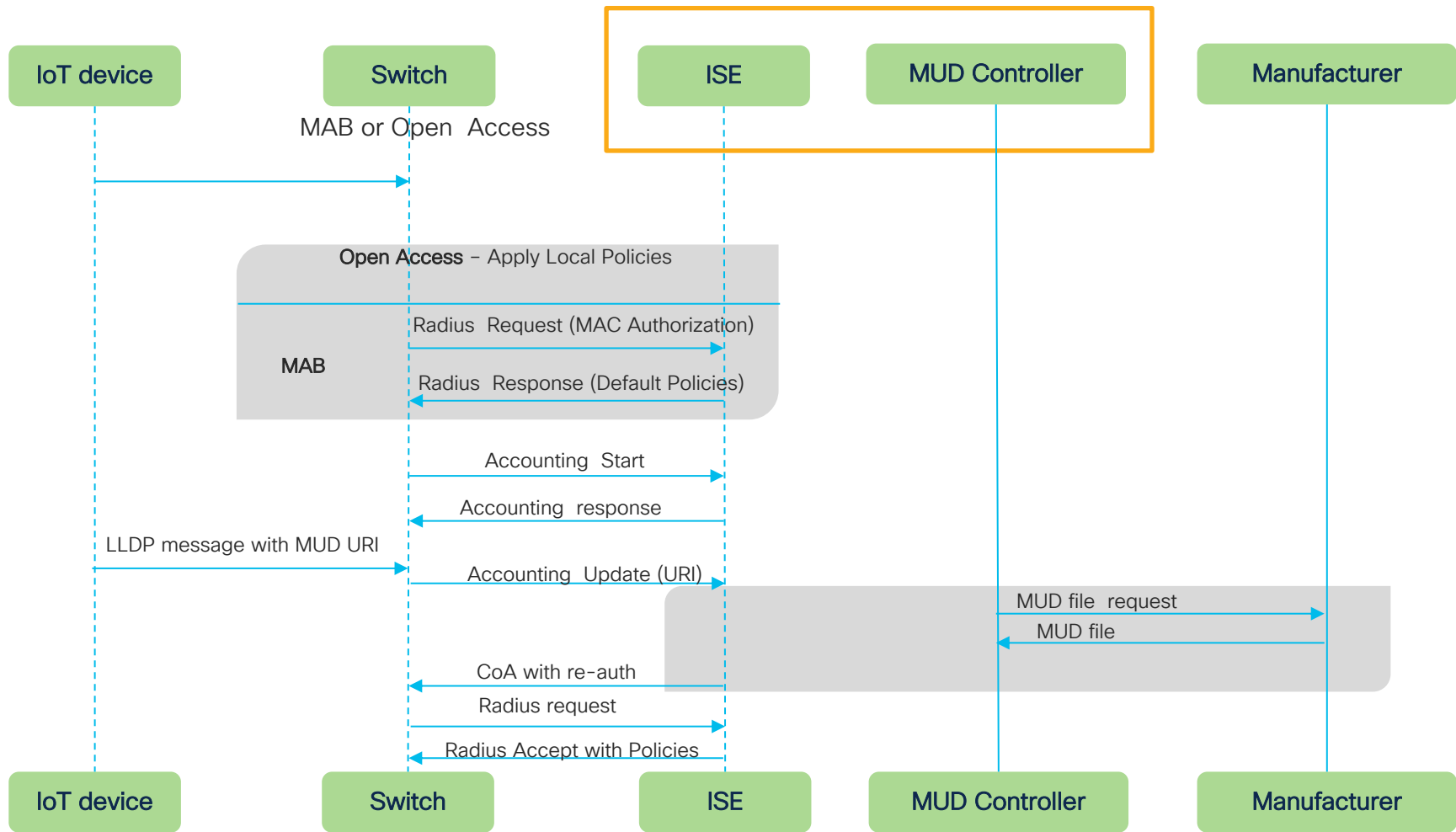
IETF Approved Internet Standard

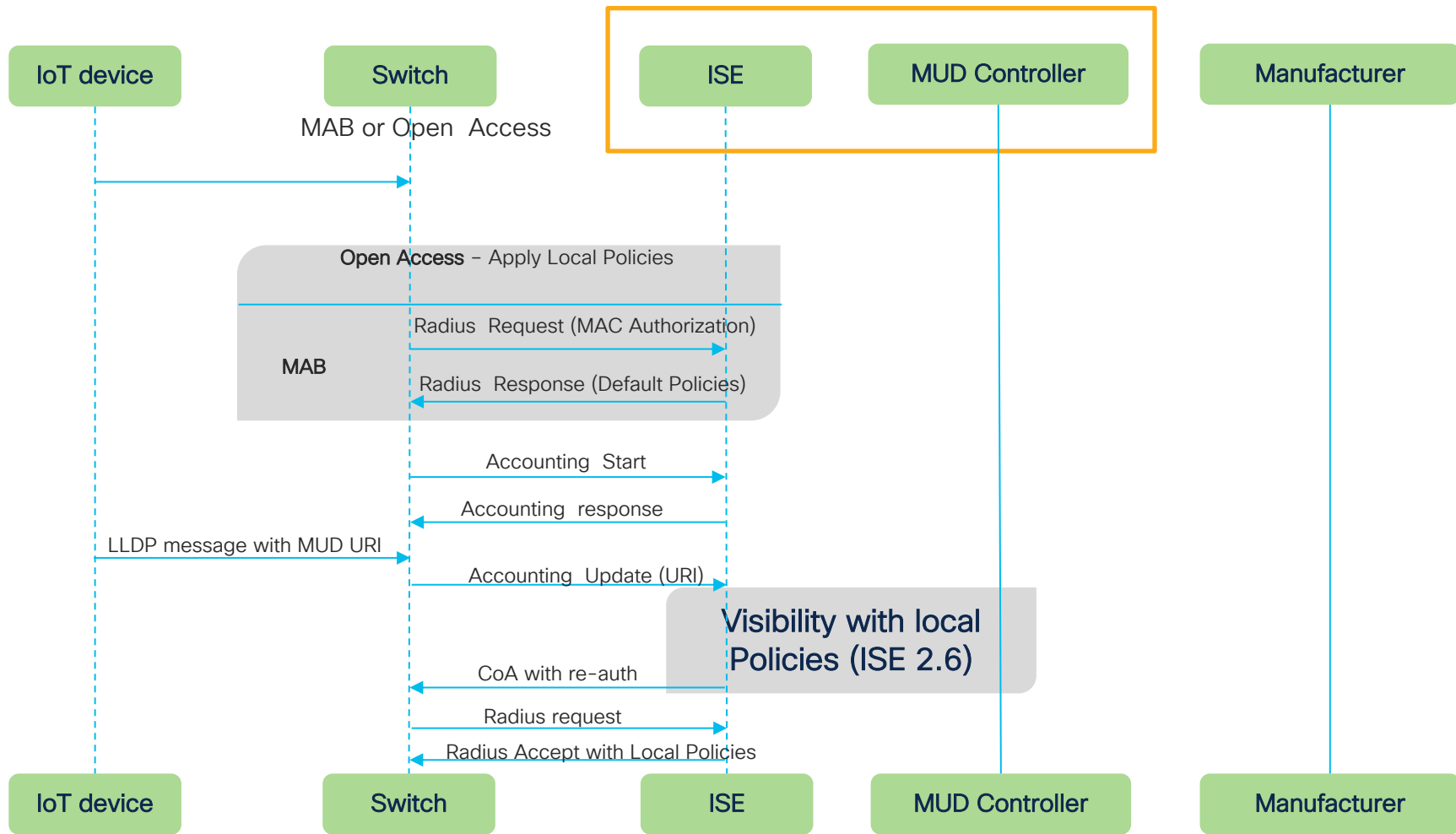
MUD Architecture and Components

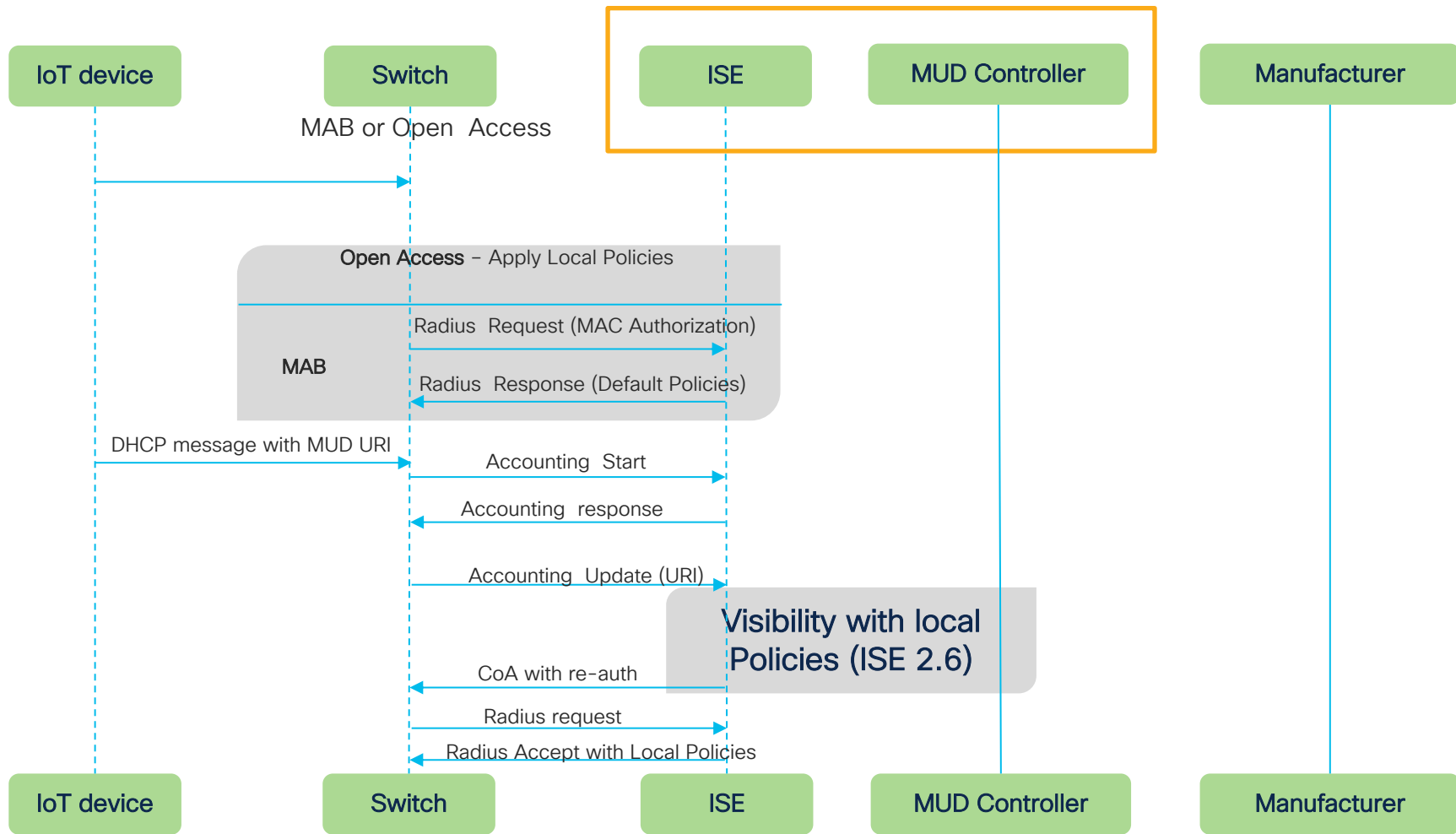


MUD with ISE provides Visibility and Policy









MUD is supported on

Catalyst 9000 series Switches



IE4000



- Both LLDP and DHCP methods are supported.
- RADIUS accounting needs to be enabled.

Profiling Policies

Change the name

Search Results

IOT-MUD-genisyslighting_files_MUD_75

All Profiling Policies

IOT-MUD-genisyslighting_files_MUD_75950001...

Profiler Policy List > Gen_Light_Type1

Profiler Policy

* Name: Gen_Light_Type1 Description: Profile policy created for IOT devices

Policy Enabled: ☒

* Minimum Certainty Factor: 10 (Valid Range 1 to 65535)

* Exception Action: NONE

* Network Scan (NMAP) Action: NONE

Create an Identity Group for the policy: ☒ Yes, create matching Identity Group ☐ No, use existing Identity Group hierarchy

* Parent Policy: NONE

* Associated CoA Type: Global Settings

System Type: IOT Created

Rules

If Condition: MUD_MUD-URL_EQUALS_https://www.ge... Then: Certainty Factor Increases 10

Save Reset

Identity Groups

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Identities **Groups** External Identity Sources Identity Source Sequences Settings

Identity Groups

Endpoint Identity Groups

User Identity Groups

Endpoint Identity Groups

Edit Add Delete

Name	Description
<input type="checkbox"/> Android	Identity Group for Profile: Android
<input type="checkbox"/> Apple-iDevice	Identity Group for Profile: Apple-iDevice
<input type="checkbox"/> Axis-Device	Identity Group for Profile: Axis-Device
<input type="checkbox"/> BlackBerry	Identity Group for Profile: BlackBerry
<input type="checkbox"/> Blacklist	Blacklist Identity Group
<input type="checkbox"/> Cisco-IP-Phone	Identity Group for Profile: Cisco-IP-Phone
<input type="checkbox"/> Cisco-Meraki-Device	Identity Group for Profile: Cisco-Meraki-Device
<input type="checkbox"/> Epson-Device	Identity Group for Profile: Epson-Device
<input type="checkbox"/> Gen_Light_Type1	Identity Group for Profile: Gen_Light_Type1
<input type="checkbox"/> GuestEndpoints	Guest Endpoints Identity Group
<input type="checkbox"/> Juniper-Device	Identity Group for Profile: Juniper-Device
<input type="checkbox"/> Profiled	Profiled Identity Group
<input type="checkbox"/> RegisteredDevices	Asset Registered Endpoints Identity Group
<input type="checkbox"/> Sony-Device	Identity Group for Profile: Sony-Device
<input type="checkbox"/> Synology-Device	Identity Group for Profile: Synology-Device
<input type="checkbox"/> Trendnet-Device	Identity Group for Profile: Trendnet-Device
<input type="checkbox"/> Unknown	Unknown Identity Group
<input type="checkbox"/> Vizio-Device	Identity Group for Profile: Vizio-Device
<input type="checkbox"/> Workstation	Identity Group for Profile: Workstation

Authorization Policy

Conditions Studio

Library

i

📍 📄 📱 🌐 🖨️ 📧 📅 🕒 📶 📶

📄 BYOD_is_Registered	i
📄 Catalyst_Switch_Local_Web_Authentication	i
📄 Compliance_Unknown_Devices	i
📄 Compliant_Devices	i
📄 MAC_in_SAN	i
📄 Network_Access_Authentication_Passed	i
📄 Non_Cisco_Profiling_Phones	i

Editor

IdentityGroup·Name

Equals

Set to 'Is not' Duplicate Save

+ New AND OR

Authorization Result

Identity Services Engine

Home Context Visibility Operations Policy Administration Work Centers

License Warning Click here to do wireless setup and visibility setup Do not show this again.

Policy Sets Profiling Posture Client Provisioning Policy Elements

Authentication Policy (3)

Authorization Policy - Local Exceptions

Authorization Policy - Global Exceptions

Authorization Policy (13)

+	Status	Rule Name	Conditions	Results		Hits	Actions
				Profiles	Security Groups		
Search							
	✓	Gen_Light	IdentityGroup Name EQUALS Endpoint Identity Groups:Profiled:Gen_Light_Type1	* Gen-light	Select from list		⚙
	✓	Wireless Black List Default	AND IdentityGroup Name EQUALS Endpoint Identity Groups:Blacklist	* Blackhole_Wireless_Access	Select from list	0	⚙
	✓	Profiled Cisco IP Phones	IdentityGroup Name EQUALS Endpoint Identity Groups:Profiled:Cisco-IP-Phone	* Cisco_IP_Phones	Select from list	0	⚙
	✓	Profiled Non Cisco IP Phones	Non_Cisco_Profiled_Phones	* Non_Cisco_IP_Phones	Select from list	0	⚙
	⚙	Unknown_Compliance_Redirect	AND Network_Access_Authentication_Passed Compliance_Unknown_Devices	* Cisco_Temporal_Onboard	Select from list	0	⚙

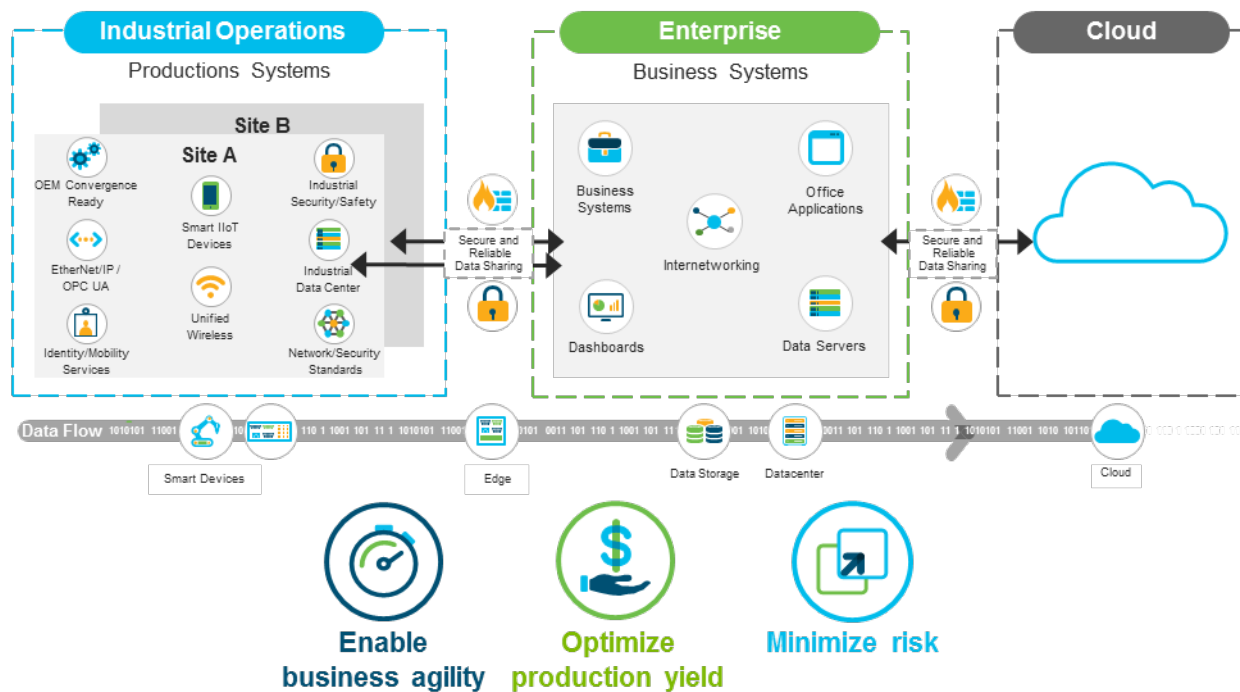
Who says playing in MUD is just for kids?



Cybervision for OT areas

CPwE

The Converged Plantwide Ethernet (CPwE) Architectures



You cannot secure what you don't know



Most customers don't have accurate OT asset inventory

55% have no or low confidence that they know all devices in their network

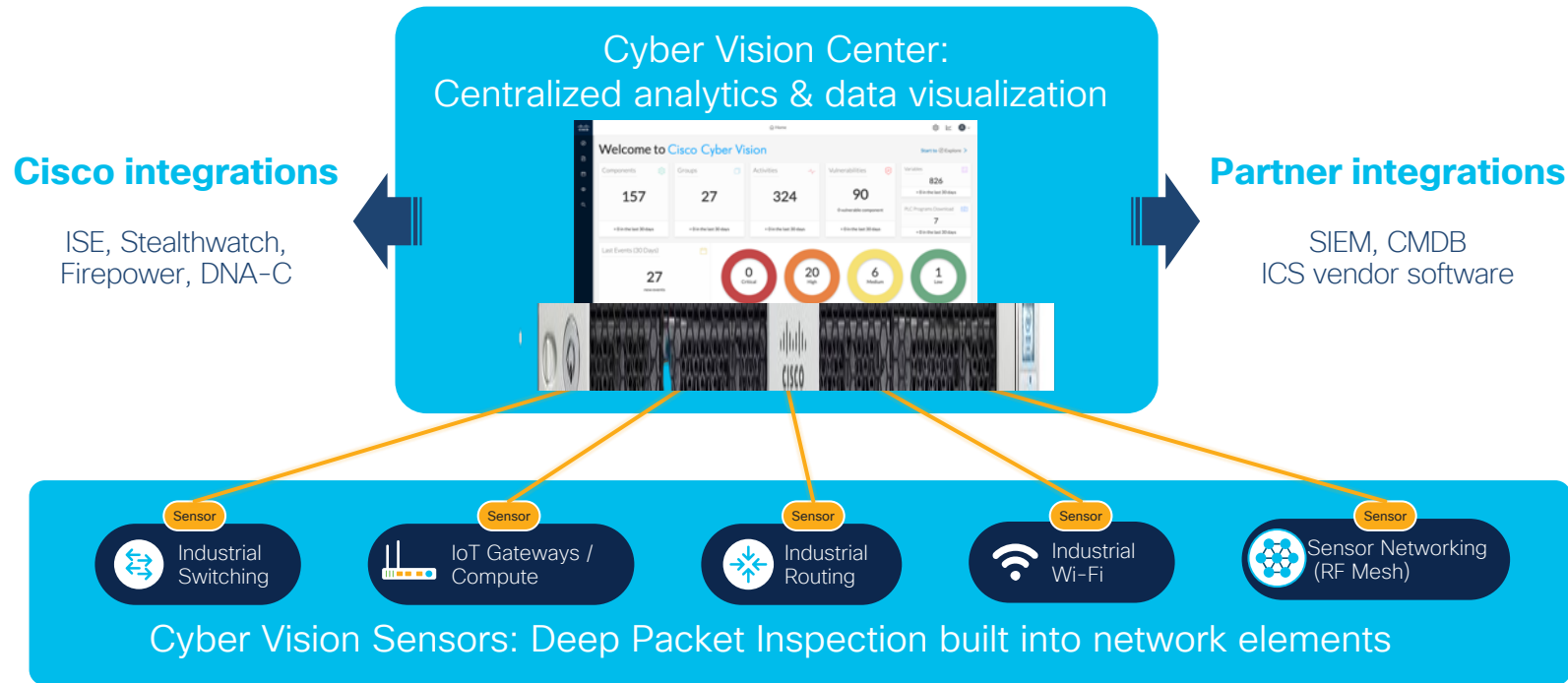


Blind to what their assets are communicating with

ICS equipment deployed over the years without strict security policies

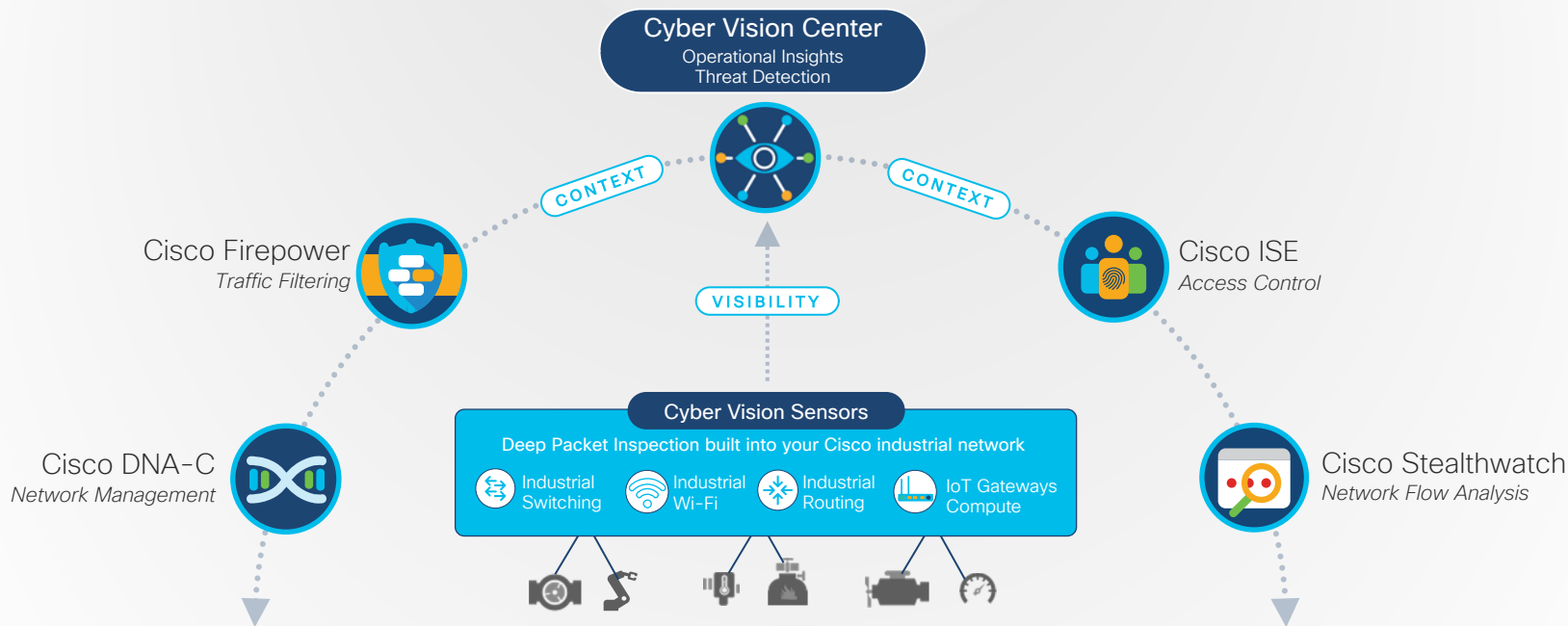
Two tier **edge monitoring** architecture

Industrial cybersecurity that can be deployed at scale

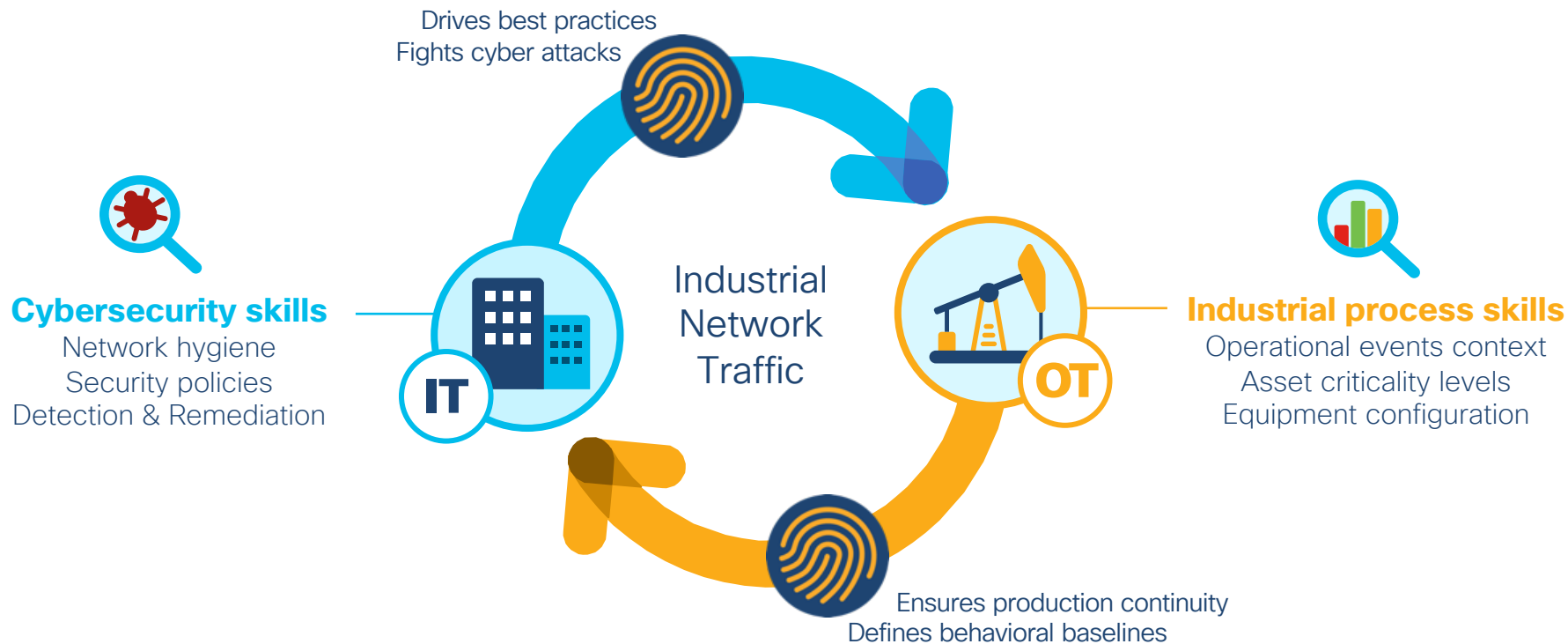


A fully **integrated IT-OT security** solution

Working together to define & apply IoT security policies



IT-OT collaboration is vital for securing ICS



Cisco Cyber Vision **portfolio**

Cyber Vision Center

Hardware Appliance

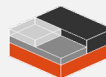
CV-CNTR-S5



Intel 2.3GHz (16 Core) CPU, 32GB RAM
x2 800GB SSD RAID-1 or x4 800GB SSD RAID-10

Software Appliance

CV-CNTR-ESXI



VMWare ESXi 6.x+
OVA

Minimum requirements

CPU: Intel Xeon, 4 cores

RAM: 8GB

Storage: 50GB

SSD highly recommended

Network: 2 network
interfaces

Cyber Vision Sensors

Hardware-Sensor

Dedicated hardware sensor



IC3000 Industrial Compute

Network-Sensors

Software built into Cisco's industrial network equipment

Available Spring 2020



IE 3400 Switch



IR 1101 Gateway



Catalyst 9300

Take away from this section



- IoT segmentation requires extending functionality of traditional Security components like ISE.
- Robust and secure IoT design by integrating ISE with IND and Cybervision.
- Auto segmentation and access control using Cisco MUD



Agenda

Exploring IoT in Enterprise

- Defining IoT
- IoT use cases for enterprise
- Challenges for adopting

Creating IoT ready Secure Architecture

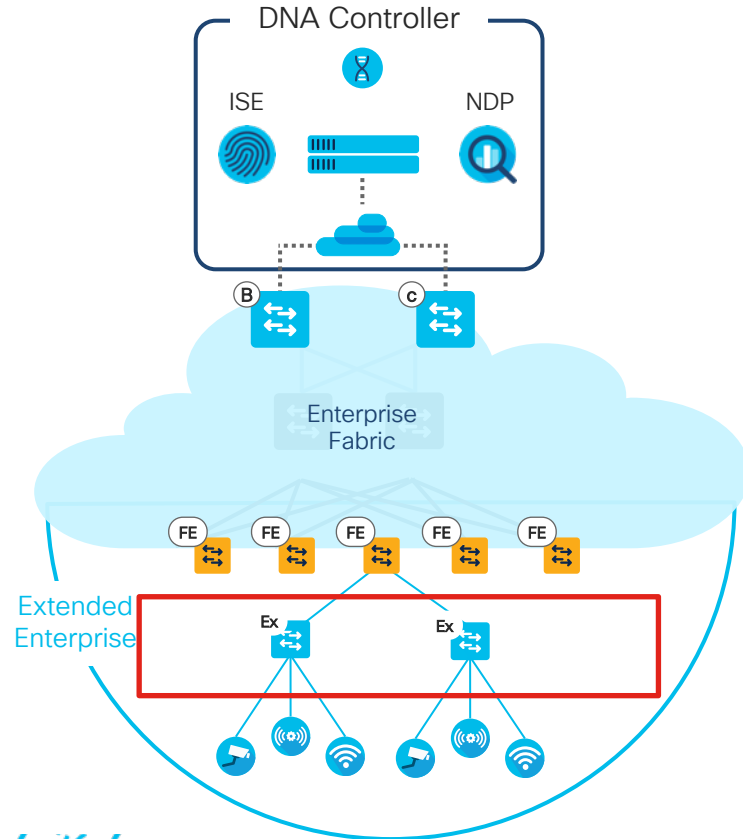
- IoT visibility using Cisco ISE and IND
- Secure Onboarding using MUD
- OT visibility using Cybervision

Auto Segmentation using Cisco SD-Access

- Cisco SD-Access basics
- Micro and macro segmentation
- Policy Extension for OT areas

SD – Access Architecture for IoT

Component Roles & Terminology



- **DNA Controller** – Enterprise SDN Controller (e.g. DNA Center) provides GUI management and abstraction via Apps that share context.
- **Identity Services** – External ID System(s) (e.g. ISE) are leveraged for dynamic Endpoint to Group mapping and Policy definition
- **Control Plane Nodes** – Map System that manages Endpoint to Device relationships
- **Fabric Border Nodes** – A Fabric device (e.g. Core) that connects External L3 network(s) to the SDA Fabric
- **Fabric Edge Nodes** – A fabric device (e.g. Access or Distribution) that connects Wired Endpoints to the SDA Fabric
- **Extended Nodes** – A Edge access device that connects Wired IoT Endpoints to the SDA Fabric via a Fabric Edge Node

Fabric Building Blocks

Control Plane

LISP

- EID : End Point Identifiers
- RLOCs : Routing locators

Data Plane

VXLAN-GPO (group Policy Option)

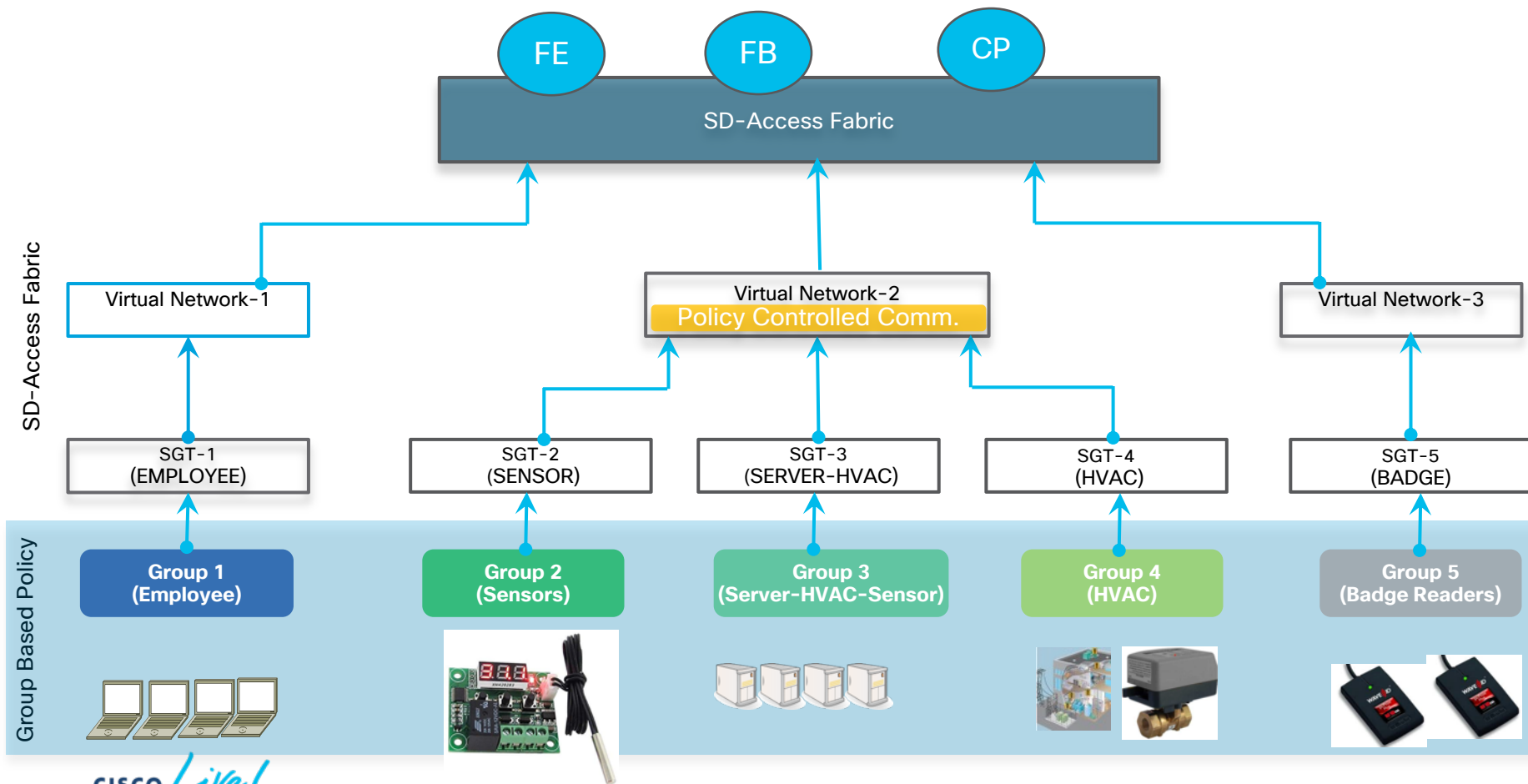
- VNID (VXLAN network identifier)
- Layer 2 overlay scheme over a Layer 3 network

Policy Plane

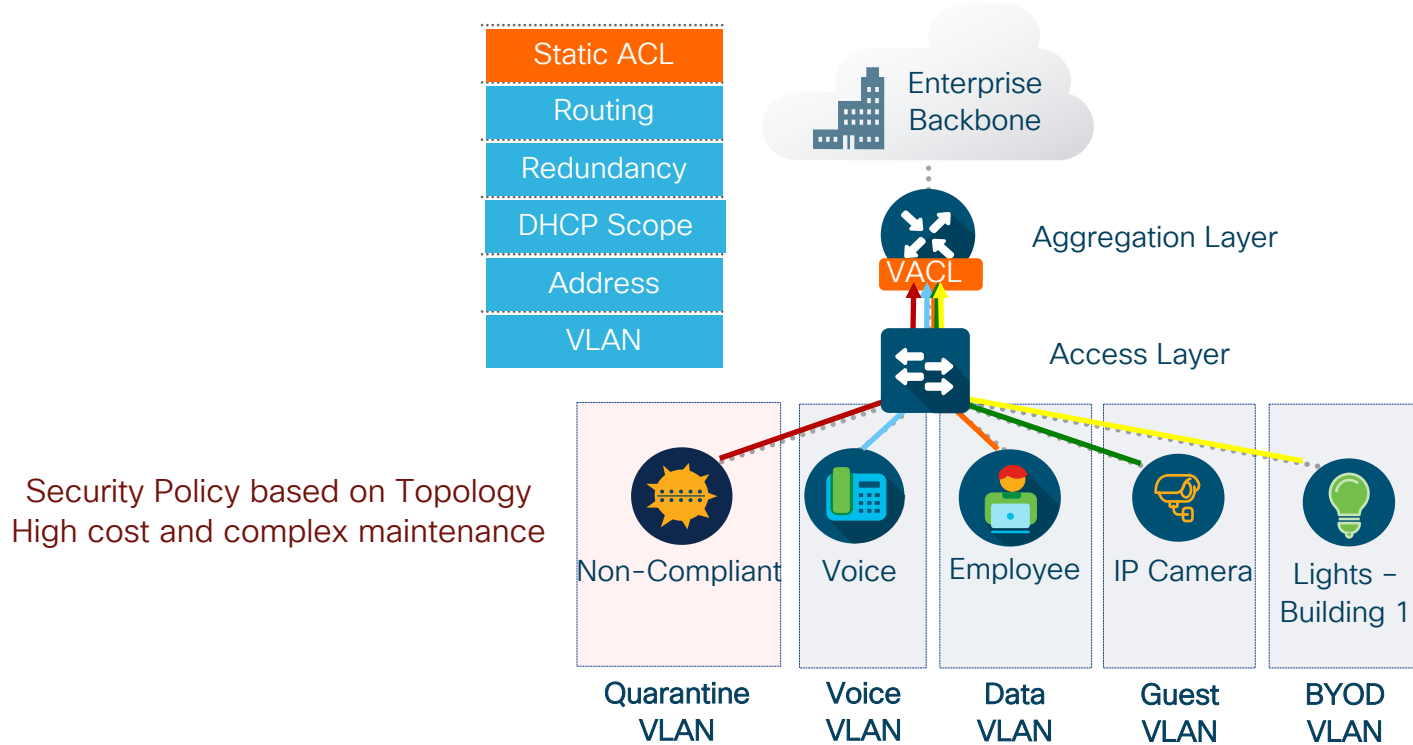
Cisco TrustSec

- SGT (Security Group Tags)
- SGACL (Security Access Group Lists)

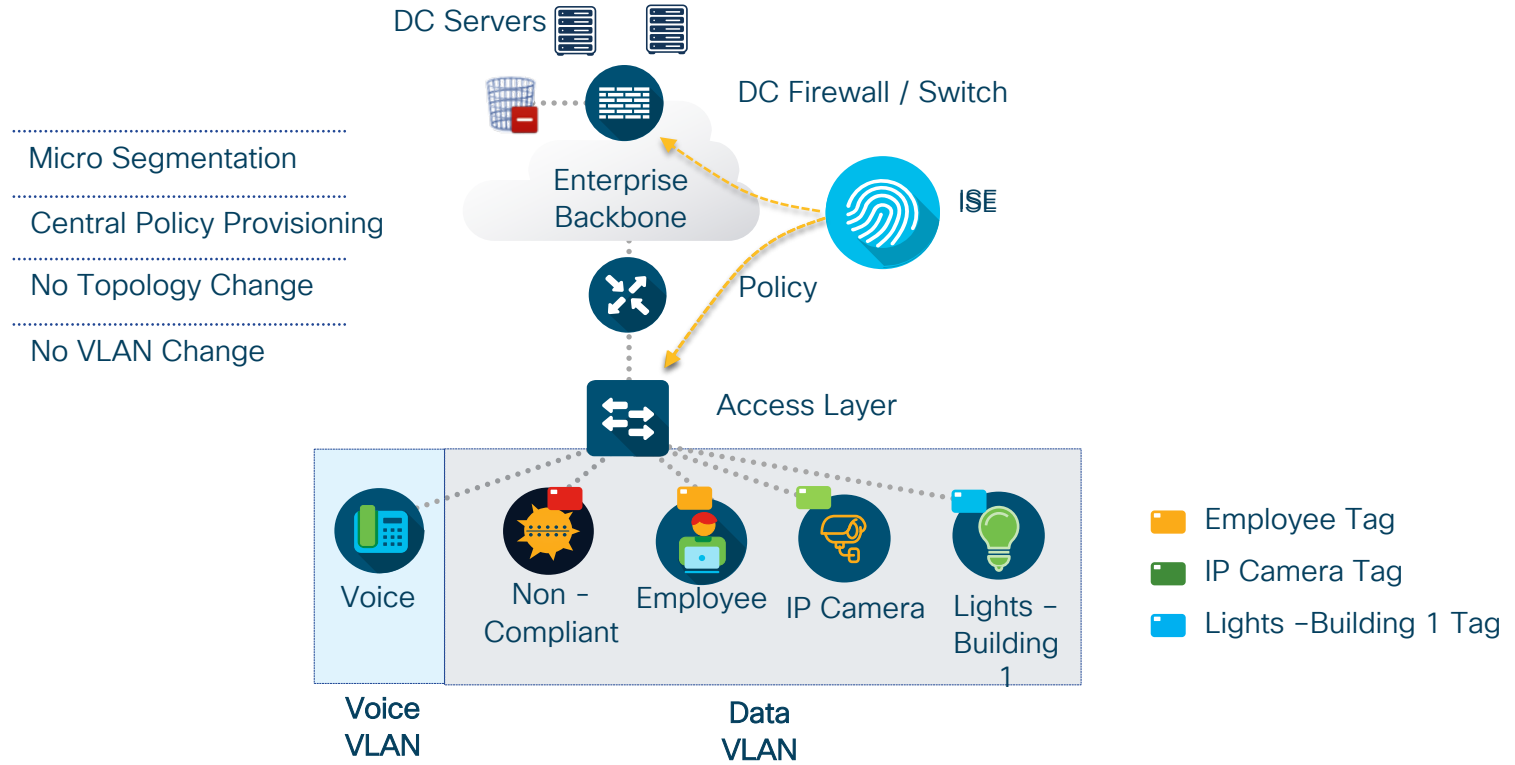
Segmentation constructs for IoT in Fabric



Traditional segmentation



Software micro-segmentation (Group based policy)



Use existing topology and automate security policy to reduce OpEx

Group based policy building blocks

Scalable Groups (SGT)



Group based Policy

Destination

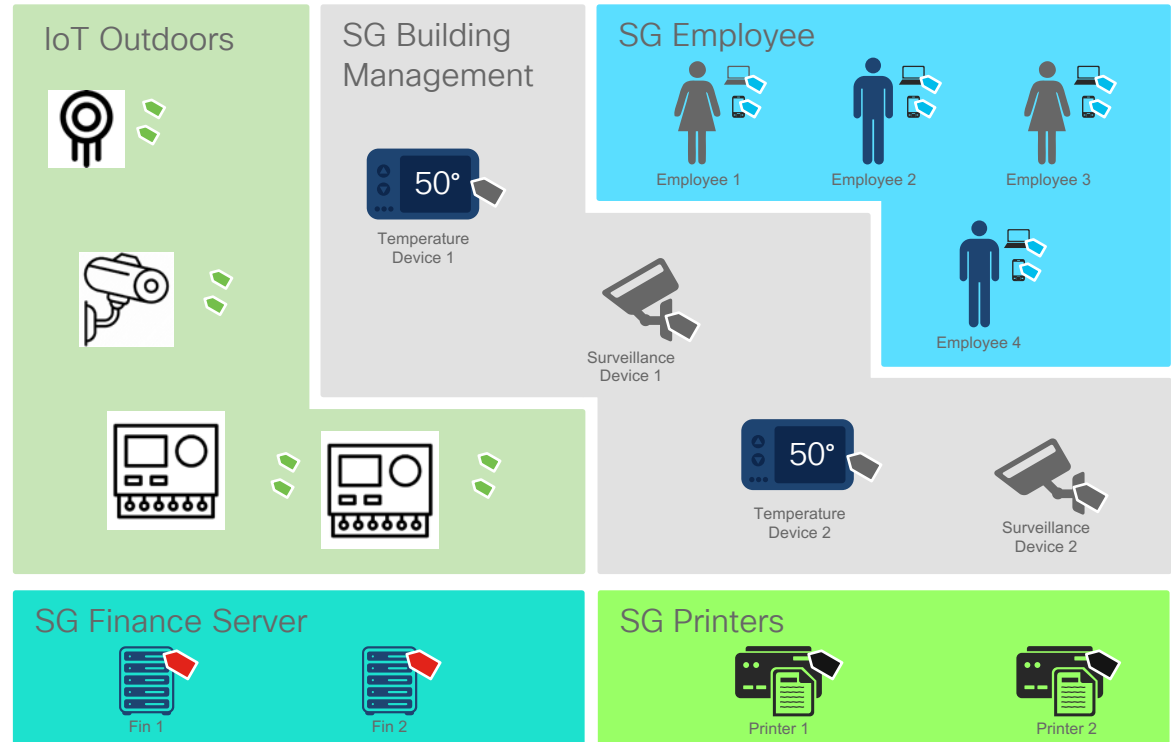
	Admins	Lights	Cameras	Employees
Admins	-	✓	✓	✓
Lights	-	-	-	-
Cameras	-	-	-	-
Employees	-	-	-	-

Source

Secure segmentation based on contextual visibility

- Intent based groupings to provide consistent policy and access independent of network topology
- Leverage attributes such as location and device type to define group assignments

SG → Scalable Group aka Security Group



Group based policy

Identity Services Engine Home ▶ Context Visibility ▶ Operations ▶ Policy ▶ Administration ▼ Work Centers

▶ Network Access ▶ Guest Access ▼ TrustSec ▶ BYOD ▶ Profiler ▶ Posture ▶ Passiveld

▶ Overview ▶ Components ▼ TrustSec Policy Authentication Policy Authorization Policy ▶ SXP ▶ Troubleshoot Reports ▶ Settings

[Security Groups ACLs List](#) > **MalwareBlock**

Security Group ACLs

* Name

Description

IP Version ☐ IPv4 ☐ IPv6 ☒ Agnostic

* Security Group ACL content

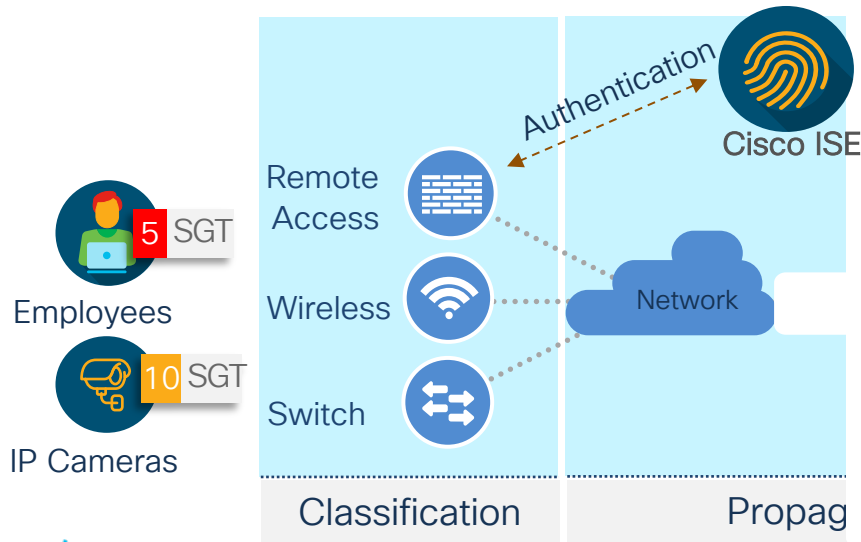
```
deny icmp
deny udp src dst eq domain
deny tcp src dst eq 3389
deny tcp src dst eq 1433
deny tcp src dst eq 1521
deny tcp src dst eq 445
deny tcp src dst eq 137
deny tcp src dst eq 138
deny tcp src dst eq 139
deny udp src dst eq snmp
deny tcp src dst eq telnet
deny tcp src dst eq www
deny tcp src dst eq 443
deny tcp src dst eq 22
deny tcp src dst eq pop3
deny tcp src dst eq 123
permit ip
```

Populated cells: 69

Clear ▼	Deploy	Monitor All - Off	Import	Export	View ▼	Show	CorpPolicy ▼
Employees 4/0004	Contractors 5/0005	Development_Ser... 12/000C	PCI_Servers 14/000E	Point_of_Sale_S... 10/000A			
MalwareBlock	MalwareBlock	Permit IP	Deny IP	Permit			
MalwareBlock	MalwareBlock	Deny IP	Deny IP	Deny IP			

Microsegmentation overview

- Identify endpoints and assign Scalable Groups
- Propagate SGT's across the desired path
- Enforce policy on the right device

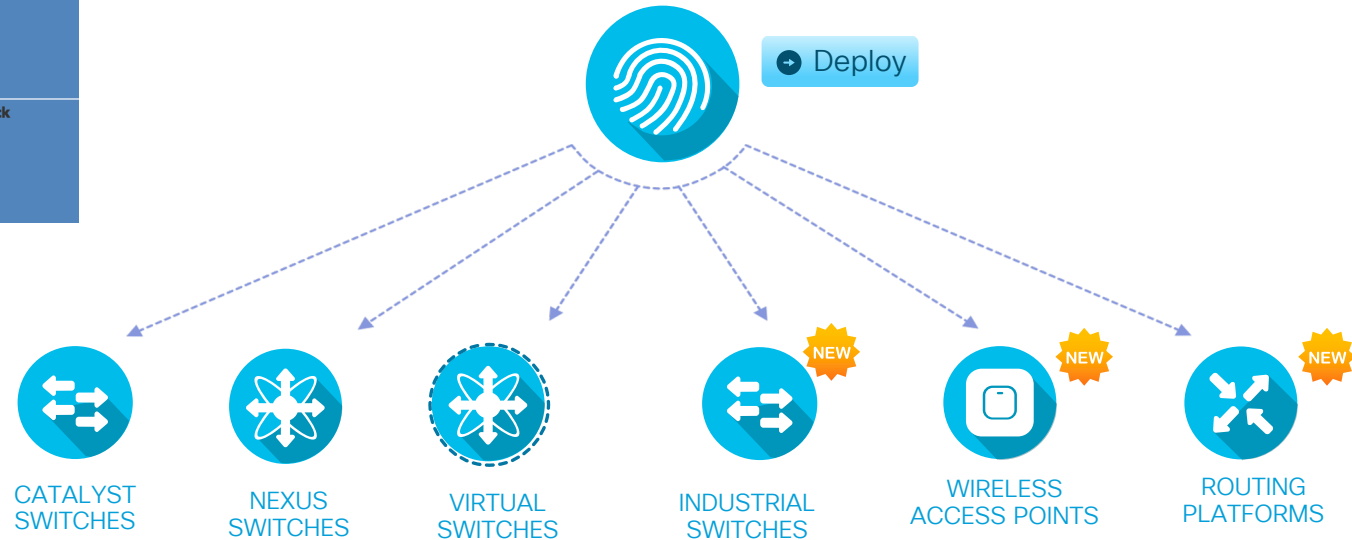


Source	Destination	
	App Server	HR Server
	Employees	
	IP cameras	
	HR Server	
	App Server	

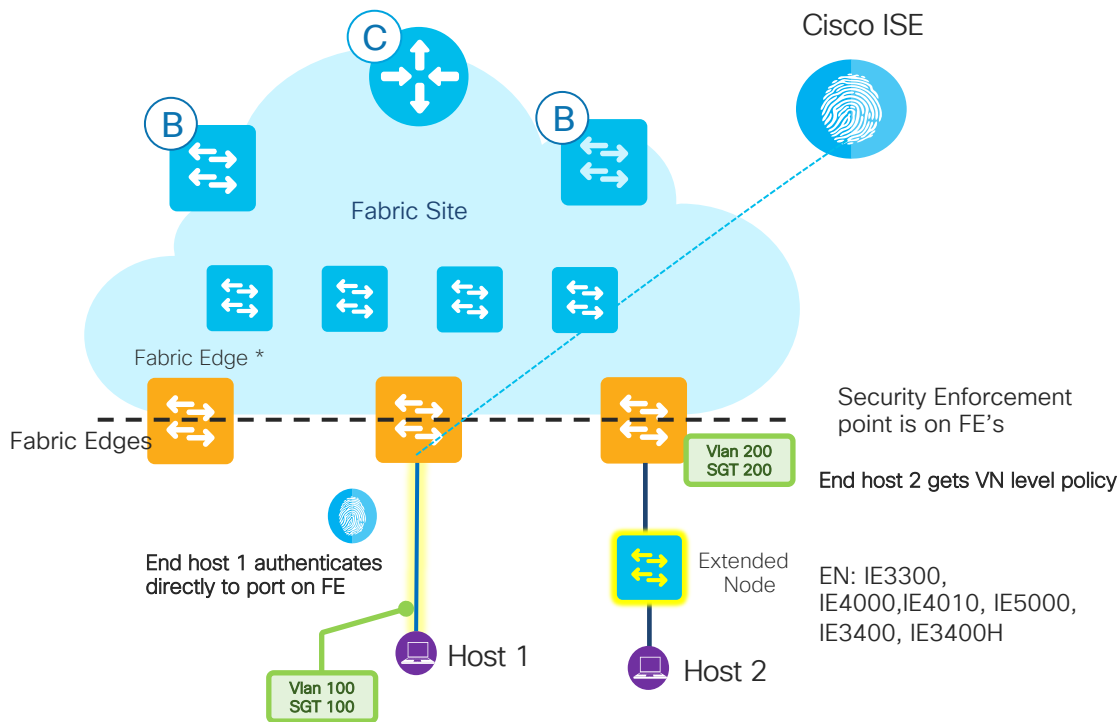
Click and deploy

Production Matrix			Populated cells: 69
Edit Add Clear Deploy Monitor All - Off Import			
Destination ▶	Employees 4/0004	Contractors 5/0005	
Source ▼			
Employees 4/0004	MalwareBlock	MalwareBlock	
Contractors 5/0005	MalwareBlock	MalwareBlock	

Push and deploy
Segmentation policies
consistently across
switching, wireless and
routing infrastructure

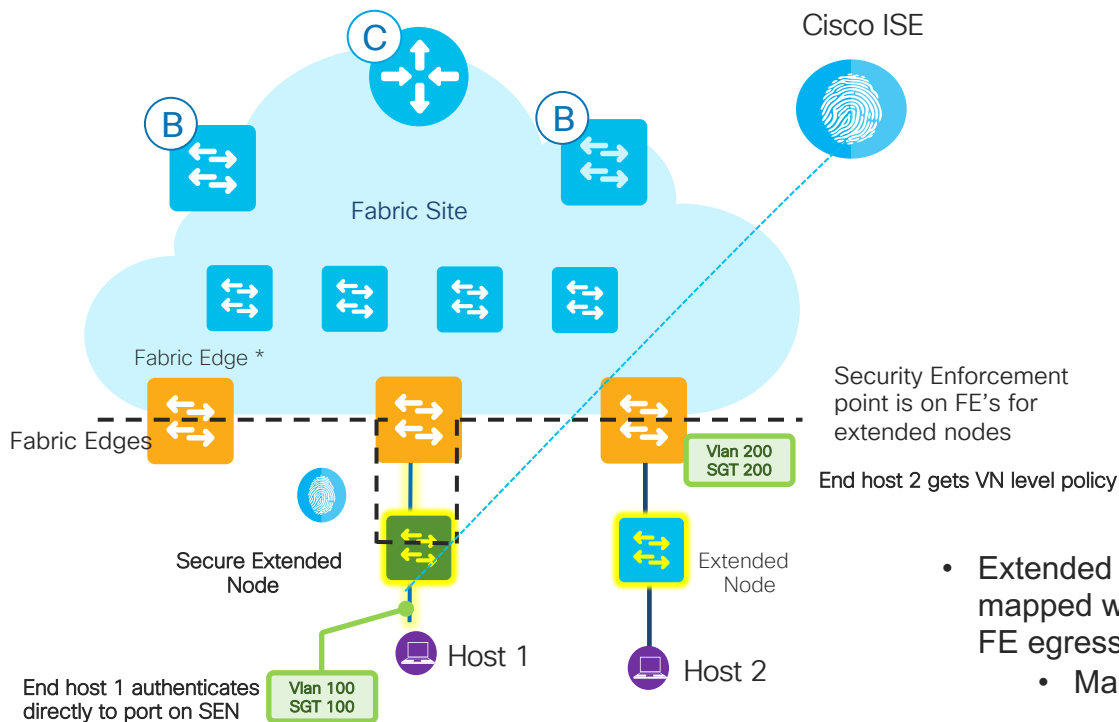


IoT Security with Extended Node



- The **Fabric Edge** 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
- Fabric Edge is LISP and ISIS with VXLAN
 - Not in Extended Node
 - Extended Node is Layer 2 only
- Fabric Edge performs security (SGACL) enforcement on egress interface
- End devices connected to Extended Node are put in default SGT / SGACL group for the Virtual Network/VLAN

IoT Security with Policy Extended Node



- 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
- Policy Extended node performs security (SGACL) enforcement on egress interface.
 - Micro Segmentation
- Extended Node puts end devices in default SGT group mapped with VLAN at the FE port. Enforcement for Host 2 on FE egress port.
 - Macro Segmentation

With Cisco DNA-C 1.3.3 or above

Take Away from this section



- Cisco SDA allows auto segmentation of IoT assets.
- Extended Nodes with PEN allows to extend the same Intent based networking for IoT use-cases.
- Scaling and onboarding needs are automated using Cisco SDA

Thank you



Possibilities

#CiscoLive