Implementing Segmentation in Industrial Networks

Andrew McPhee - IIoT Security Solution Manager

BRKIOT-2882

Webex App

Questions?

Use the Webex app to chat with the speaker after the session

How

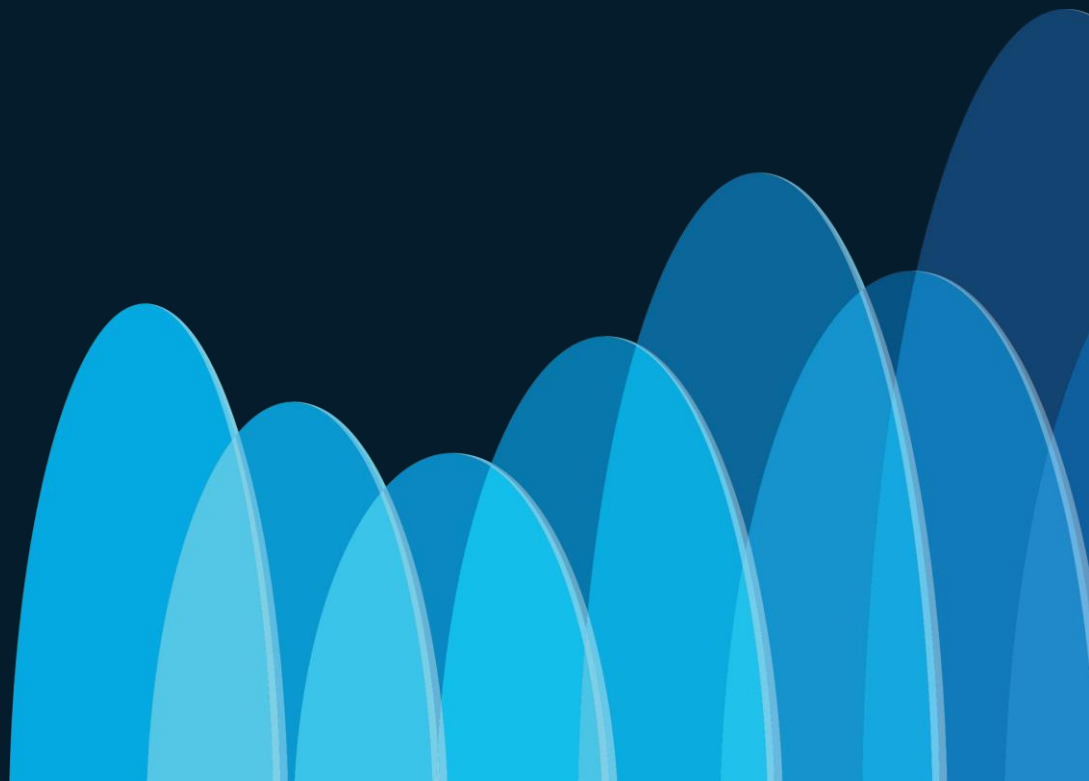
1. Find this session in the Cisco Events mobile app
2. Click “Join the Discussion”
3. Install the Webex app or go directly to the Webex space
4. Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until February 28, 2025.

Agenda

- Introduction
- Identifying the Assets
  - Virtual Segmentation
- The role of Firewalls in OT
- Network as an Enforcer
- Segmenting the Users
- Q&A

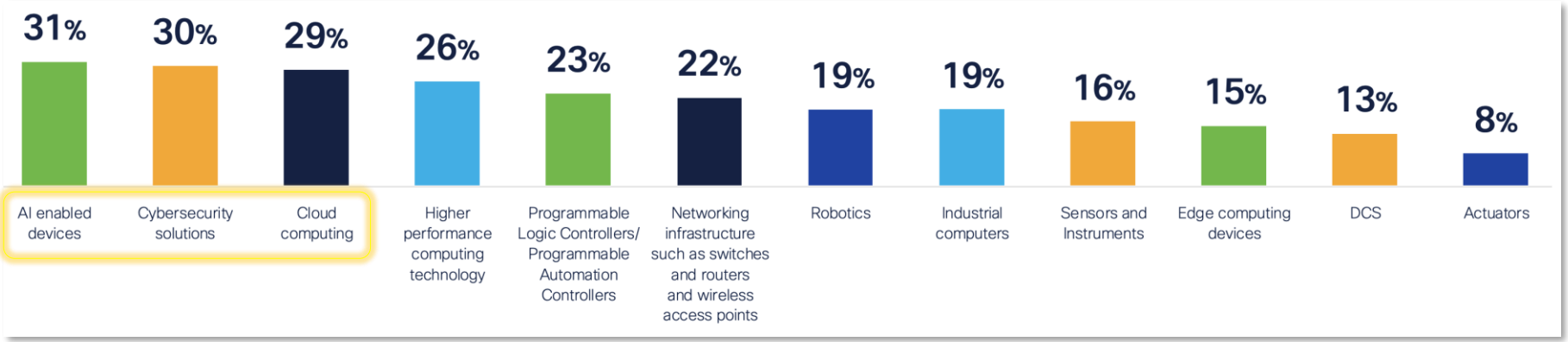
Introduction



State of Industrial Networking 2024

Insights from over 1000 operational leaders, across 17 countries and 20 industries

Which types of industrial/OT infrastructure are receiving the most investment in your organization currently? Select up to three.



Attackers are taking advantage of poor connectivity

Clorox says sales and profit took a big hit from cyberattack

Johnson Controls Ransomware Attack: Data Theft Confirmed,

World's Critical Infrastructure Suffered 13 Cyber Attacks Every Second in 2023

Jan 29, 2024

Cyberattacks on CNI surge by 30% in 2024, study reveals

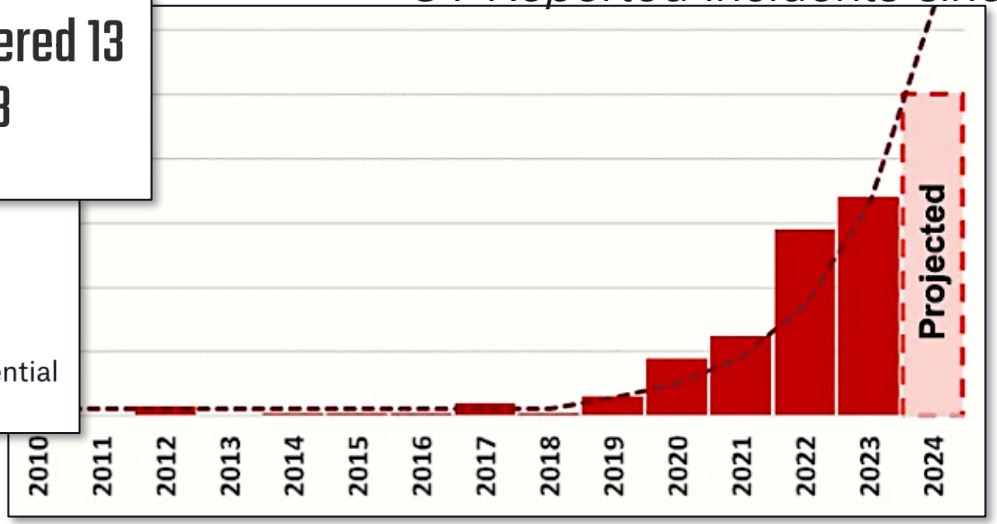
The report by KnowBe4 details the significant rise in attacks on essential sectors - with the US power grid providing especially vulnerable.

Suzuki Motorcycle India breach forces plant shutdown

Simpson Manufacturing Takes Systems Offline Following Cyberattack

Simpson Manufacturing is experiencing disruptions after taking IT systems offline following a cyberattack.

OT Reported Incidents sinc



Over 50% of incidents occurred in process and discrete manufacturing in 2023

Security guidelines can often make cybersecurity seem complex

NIS2

- 46 Articles
- 144 Recitals
- 3 Annexes
- 40000+ words

Can I follow IEC 62443?

IEC 62443

- 14 documents
- Product Compliance
- System Compliance
- Zones & Conduits or Zero Trust?

And yet, industry is still asking *what do I need to comply?*

What about NIST?

NIST SP 800-82

- 300+ Pages
- 1 of 200+ special publications

Current OT security themes from our customers

Scalable Visibility

"High cost of SPAN networks, as there are an order of more assets in OT than in IT"

Adaptive Segmentation

"Avoiding downtime when enforcing segmentation policy for IEC-62443 zones & conduits"

Cross-Domain SOC

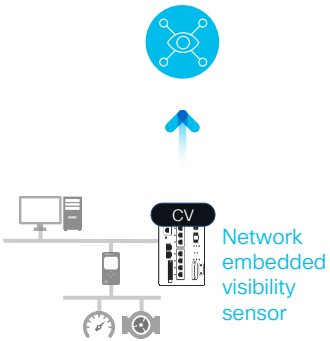
"Difficulty in tracking lateral movement of threats propagating between IT and OT"

Cisco Industrial Threat Defense

Visibility

OT Asset Visibility and Security Posture

Cisco Cyber Vision

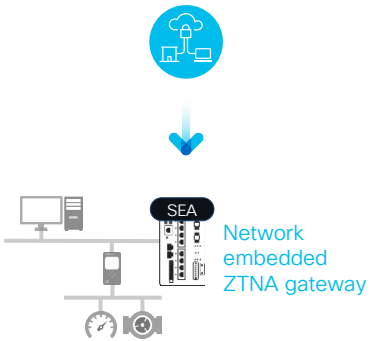


Protection

Zero Trust Security for OT

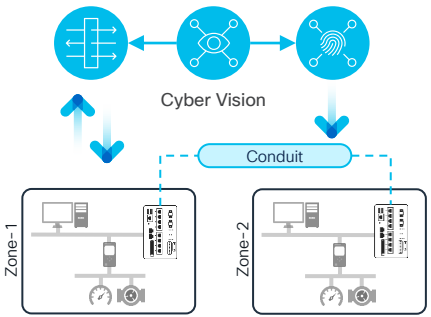
Secure remote access (ZTNA)

Cisco Secure Equipment Access



IEC 62443 zone segmentation

Cisco Secure Firewall **Cisco ISE**

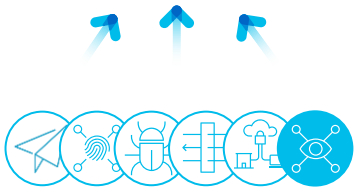


Network enforced segmentation

Response

Cross-Domain Detection, Investigation & Response

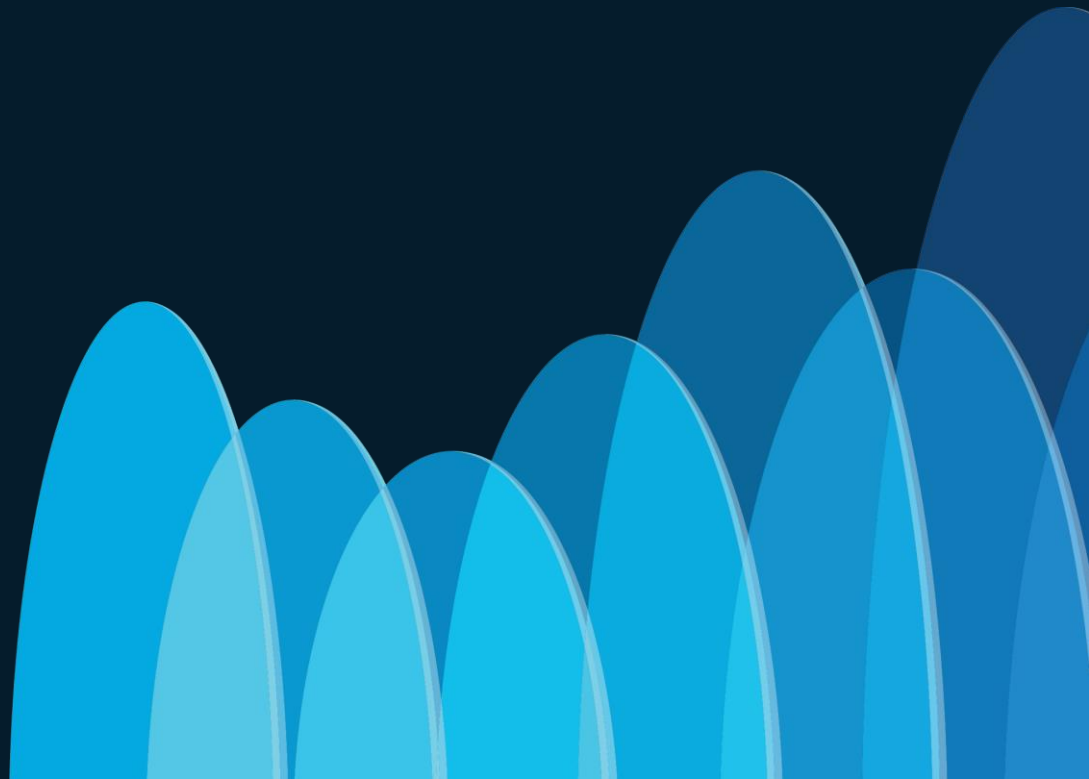
splunk> a cisco company



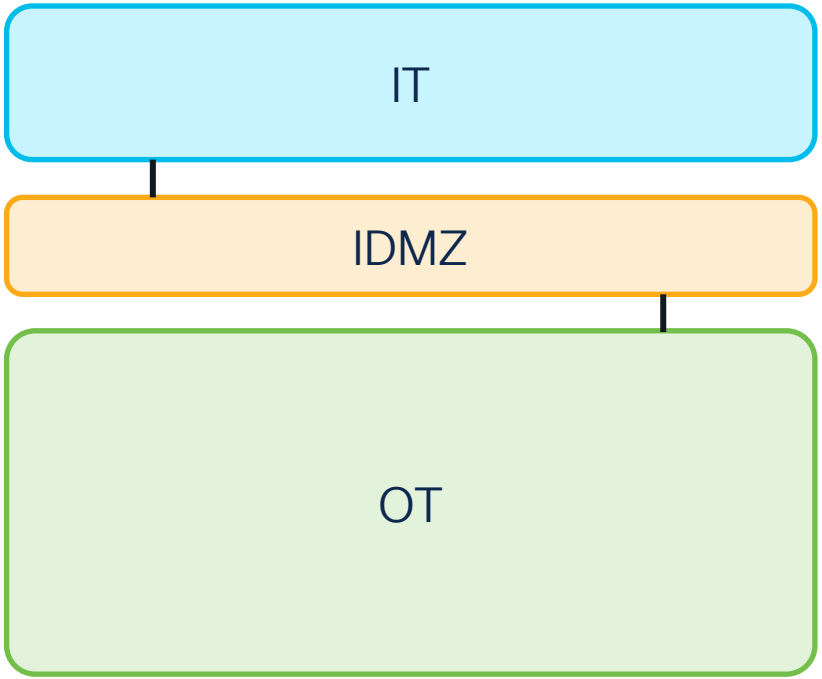
Visibility across the entire attack chain

Network as a fabric to secure OT at scale

What Industry says about Segmentation



The Purdue Model



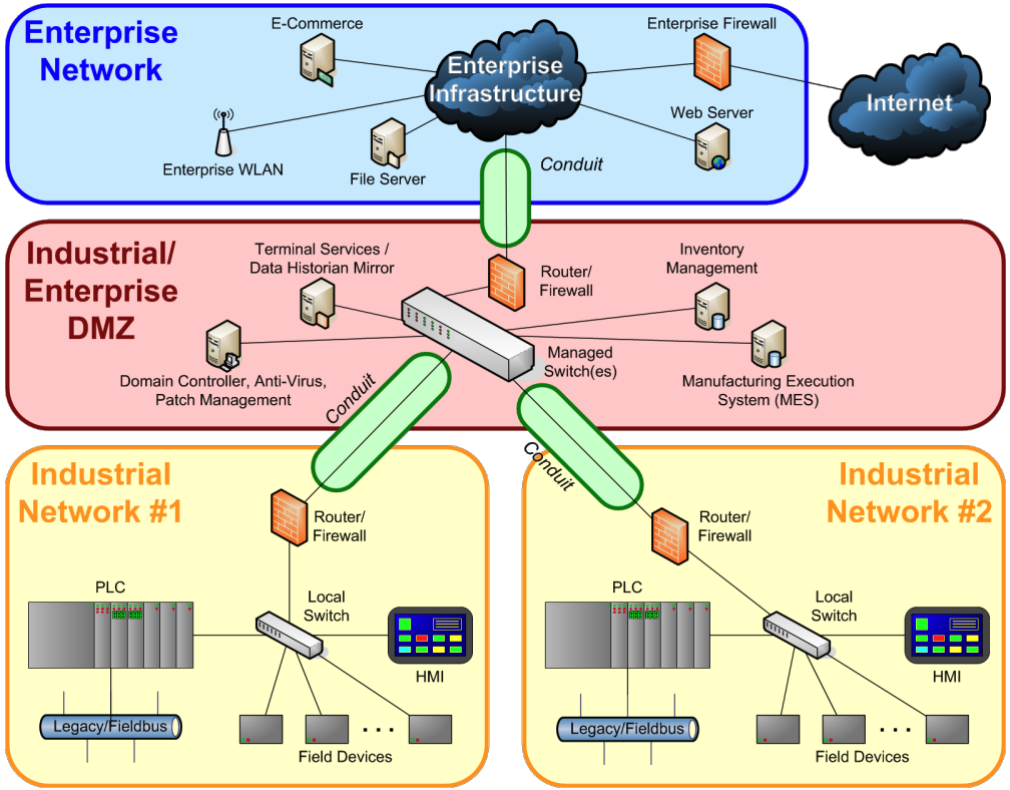
- No direct communication between IT (level 4 & 5) & OT (level 0 – 3)
- IDMZ services (level 3.5) are recommended to be segmented from each other
  - i.e. each service in its own VLAN and terminates at the firewall
- OT consists of site operations zone (level 3) and Cell/Area zone (level 0-2)

TSA definition of a Critical Cyber System

“Critical Cyber System means any Information or Operational Technology system or data that, if compromised or exploited, could result in operational disruption. Critical Cyber Systems include those business services that, if compromised or exploited, could result in operational disruption.”

– TSA Security Directive 1580/82-2022-01A

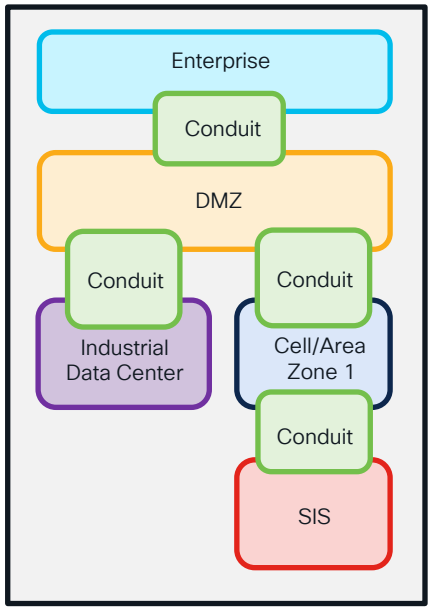
IEC 62443 Zones & Conduits



- **Zone**: Collection of entities that represent a partitioning of a System under Consideration (SUC) based on their functional, logical and physical (including location) relationship that share common security requirements
- **Conduit**: Physical or logical grouping of communication channels, intermittent or permanent, between connecting a zone with another zone or with the outside that share common security requirements
- The intent is to identify those assets which share common security characteristics in order to establish a set of common security requirements that reduce cybersecurity risk

NIST Zero Trust Guidance is practically the same

ISA/IEC 62443



NIST Zero Trust Guidance

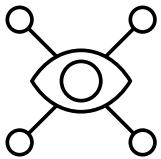
3.1.2 ZTA Using Micro-Segmentation

An enterprise may choose to implement a ZTA based on placing individual or groups of resources on a unique network segment protected by a gateway security component. In this approach, the enterprise places infrastructure devices such as intelligent switches (or routers) or next generation firewalls (NGFWs) or special purpose gateway devices to act as PEPs protecting each resource or small group of related resources. Alternatively (or additionally), the enterprise may choose to implement host-based micro-segmentation using software agents (see Section 3.2.1) or firewalls on the endpoint asset(s), These gateway devices dynamically grant access to individual requests from a client, asset or service. Depending on the model, the gateway may be the sole PEP component or part of a multipart PEP consisting of the gateway and client-side agent (see Section 3.2.1).

This approach applies to a variety of use cases and deployment models as the protecting device acts as the PEP, with management of said devices acting as the PE/PA component. This approach requires an identity governance program (IGP) to fully function but relies on the gateway components to act as the PEP that shields resources from unauthorized access and/or discovery.

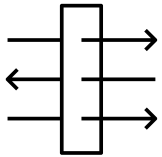
The key necessity to this approach is that the PEP components are managed and should be able to react and reconfigure as needed to respond to threats or change in the workflow. It is possible to implement some features of a micro-segmented enterprise by using less advanced gateway devices and even stateless firewalls, but the administration cost and difficulty to quickly adapt to changes make this a very poor choice.

Segmentation Phases



Virtual Segmentation

- Visualizing the zones and conduits model and reacting to data observed between zones



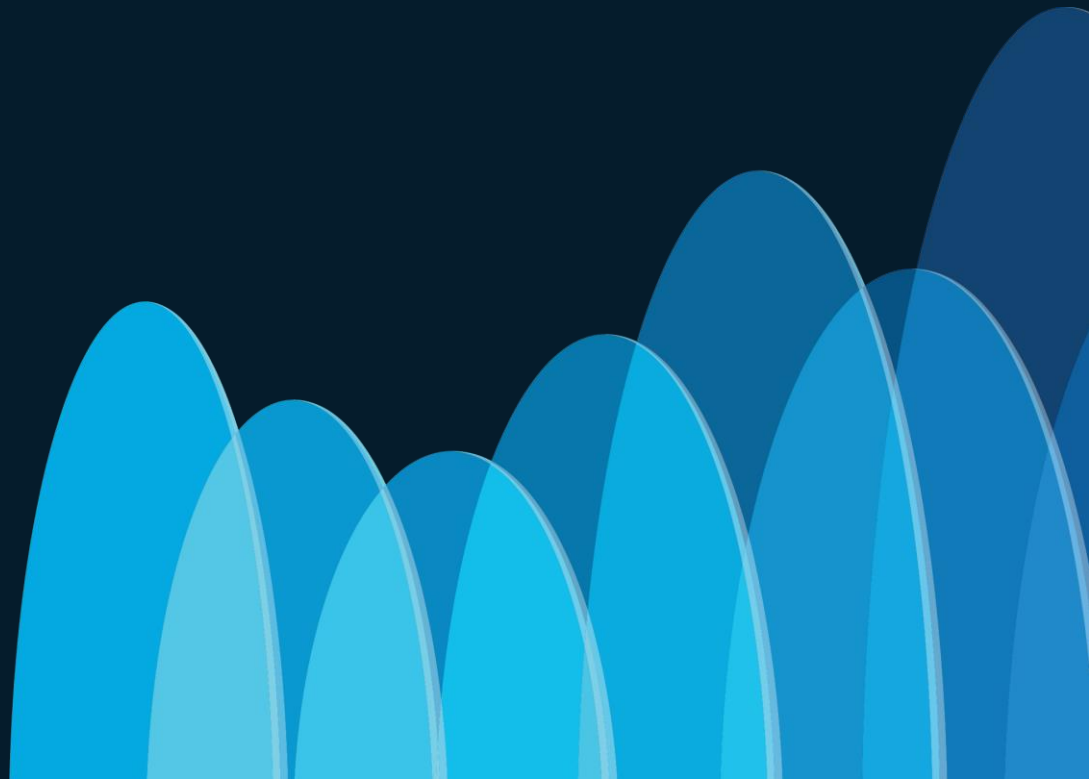
Macro Segmentation

- Pushing policy across ”large” zones (production lines or cell/area zones)
- IDF is typically point of VLAN termination and is a conditioned space

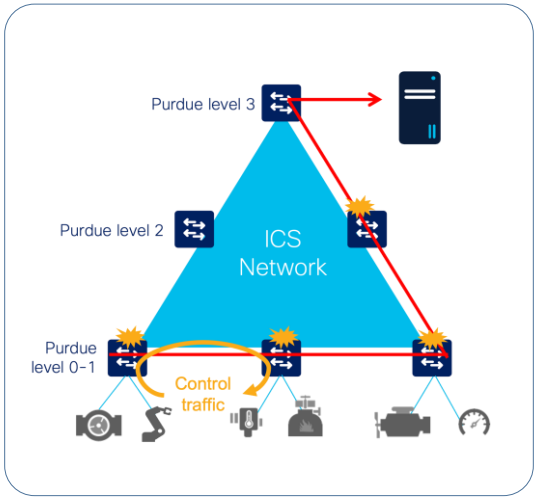
Micro Segmentation

- Pushing policy across “small” zones
- Segmentation within Cell/Area Zone

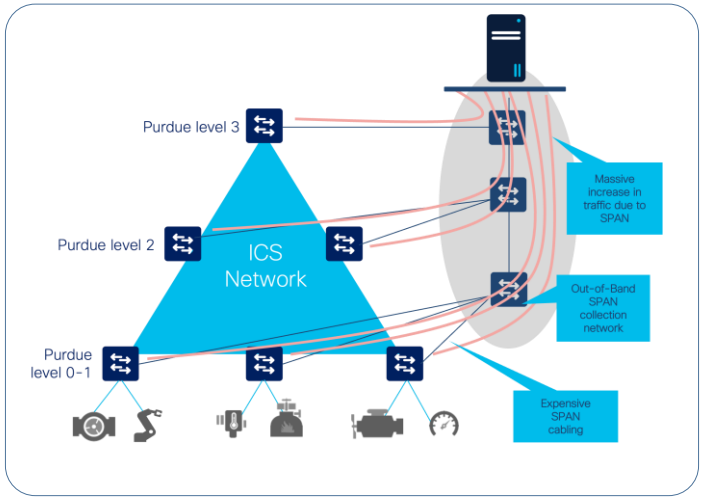
Identifying the Assets



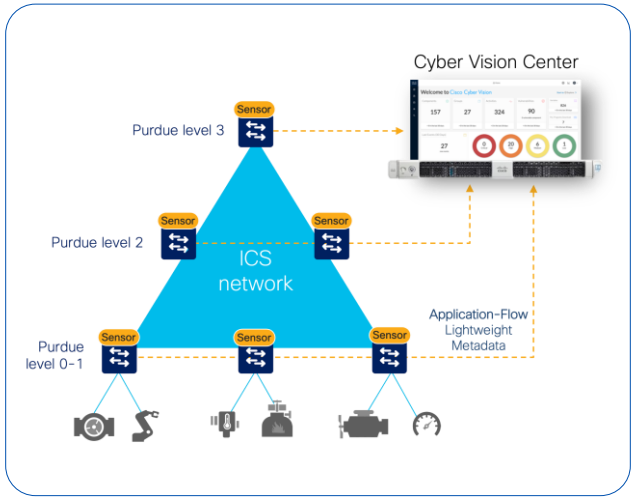
Leverage the network as a sensor to lower cost and complexity



RSPAN introduces Jitter



Out-of-Band SPAN is expensive

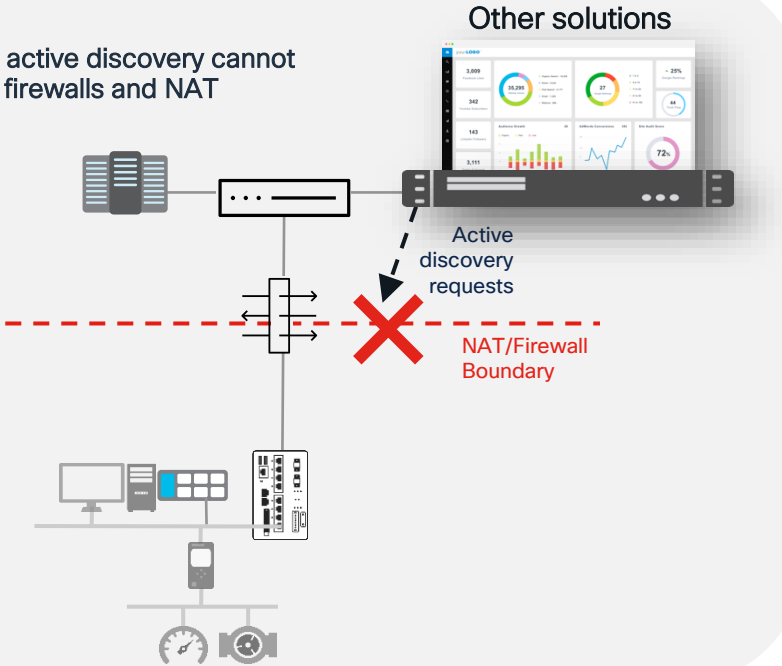


Network sensors scale without SPAN

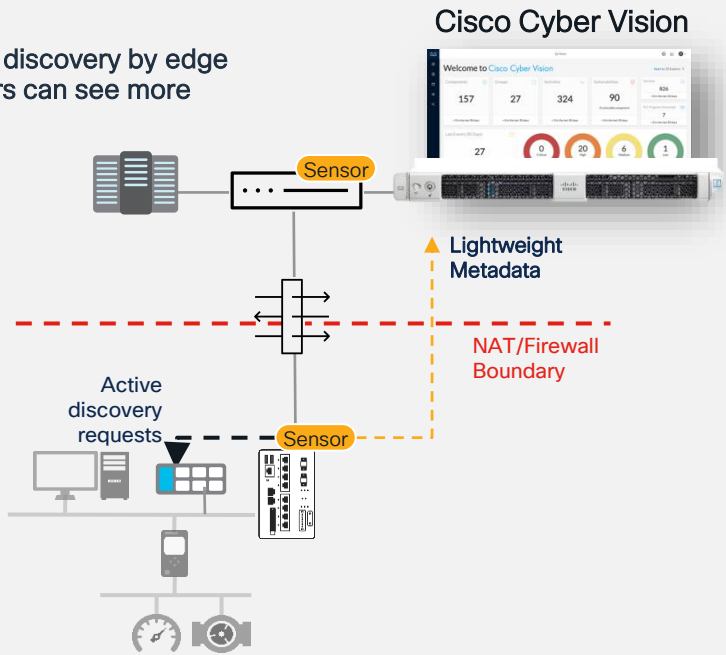
Why is a network-sensor important?

Distributed edge active discovery gives you 100% visibility

Centralized active discovery cannot see behind firewalls and NAT boundaries



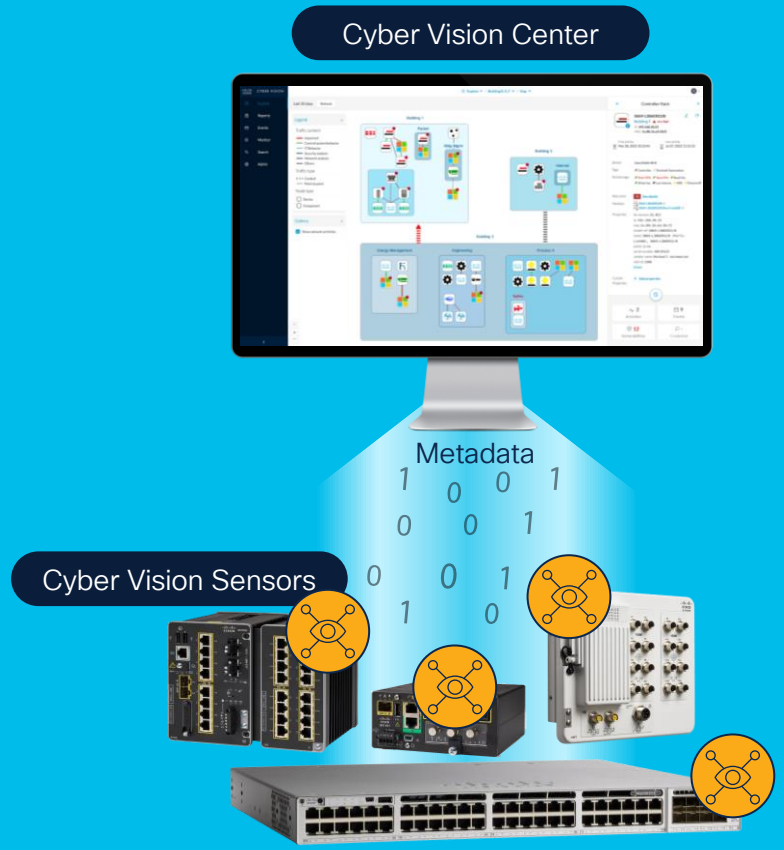
Active discovery by edge sensors can see more



Cyber Vision

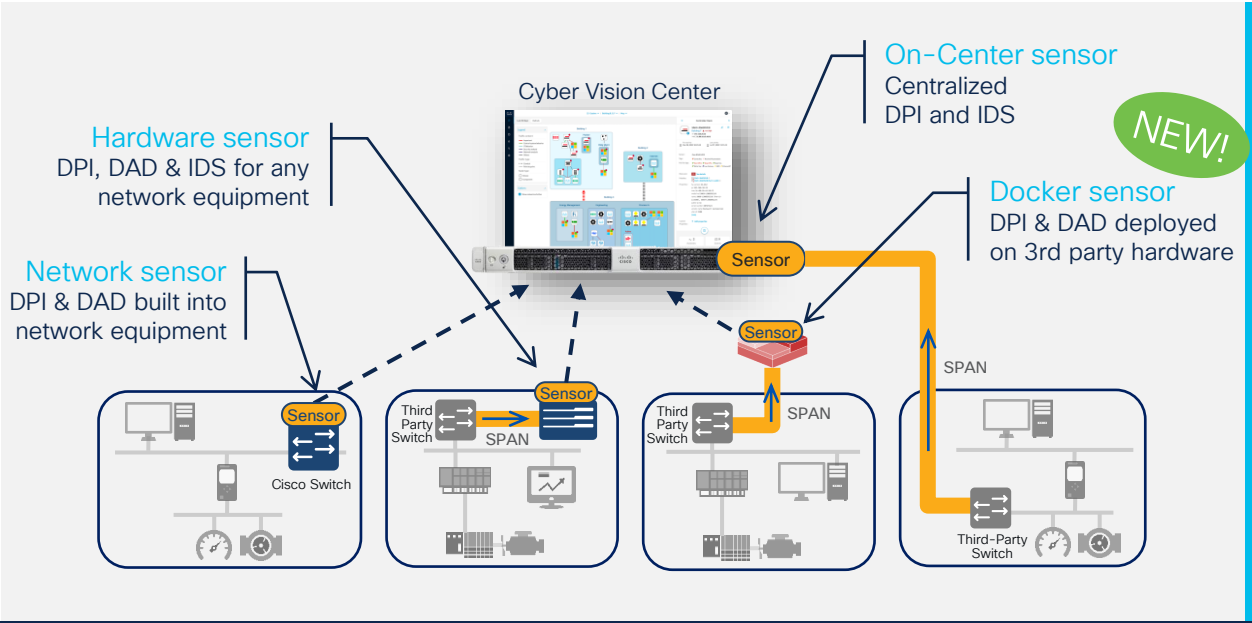
Manage risks from OT assets with full visibility on your OT security posture

- Asset Inventory & Profiling
- Asset Communications
- Asset Vulnerabilities
- Asset Risk Scores
- Behavior Baselining
- Snort Threat Detection
- Talos Threat Intelligence



Deep Packet Inspection & Active Discovery
built into your network infrastructure

Easy to deploy in Brownfield and Greenfield environments



- **Network-sensors** embedded in Cisco networking for simple and highly scalable deployments
- **Hardware or Virtual sensors** capturing traffic on any switch with a single hop SPAN to support brownfield deployments
- **On-Center sensor** to leverage existing SPAN infrastructures, or collect traffic within the datacenter

Cyber Vision offers flexible deployment options

DPI = Deep Packet inspection
DAD = Distributed Active Discovery
IDS = Intrusion Detection System

Cisco Cyber Vision portfolio

Center

Hardware Appliance
UCS based servers with Hardware RAID

CV-CNTR-M6N
- 24 core CPU
- 128 GB RAM
- 3.2TB drives

Software Appliance
Virtual Machines

VMWare ESXi OVA

HyperV VHD

Minimum requirements
x386 server CPU, 10 cores
32GB RAM and 1TB SSD
1 or 2 network interfaces

aws

Amazon Web Services

Microsoft Azure

Minimum requirements
x386 server CPU, 10 cores
32GB RAM and 1TB SSD
1 or 2 network interfaces

Sensors

Catalyst IE3300 and IE3400 Switches

Catalyst IE3400HD IP67 Switch

Catalyst IR1101 Cellular Router

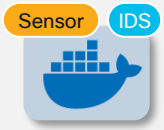
Catalyst IR1800 Cellular Router

Catalyst IR8300 Multiservice Router

Catalyst IE9300 Rugged Switches

Catalyst 9300/9400 Aggregation Switches

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



x86 or ARM64 Compute

IC3000 Industrial Compute

Docker Sensor
Hardware-Sensor
DPI and active discovery via SPAN to support brownfield

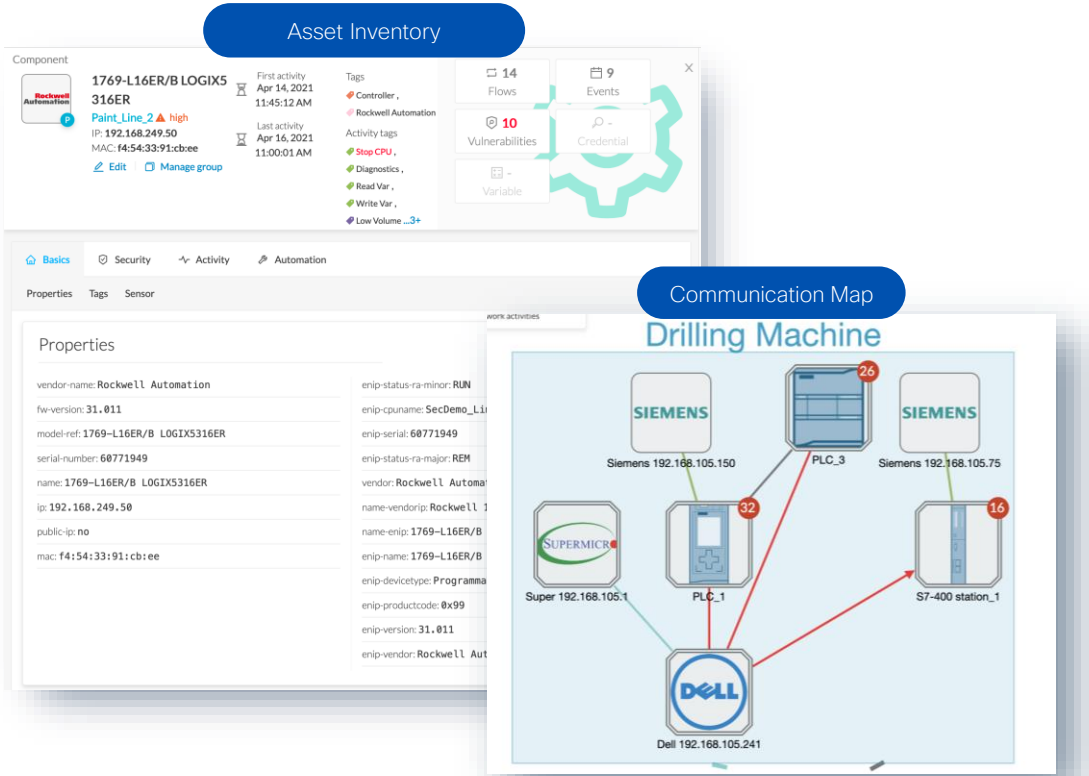
Visibility into connected industrial assets

Asset Inventory

Automated inventory of all assets in your environment with detailed and up to date profile information

Communication Patterns

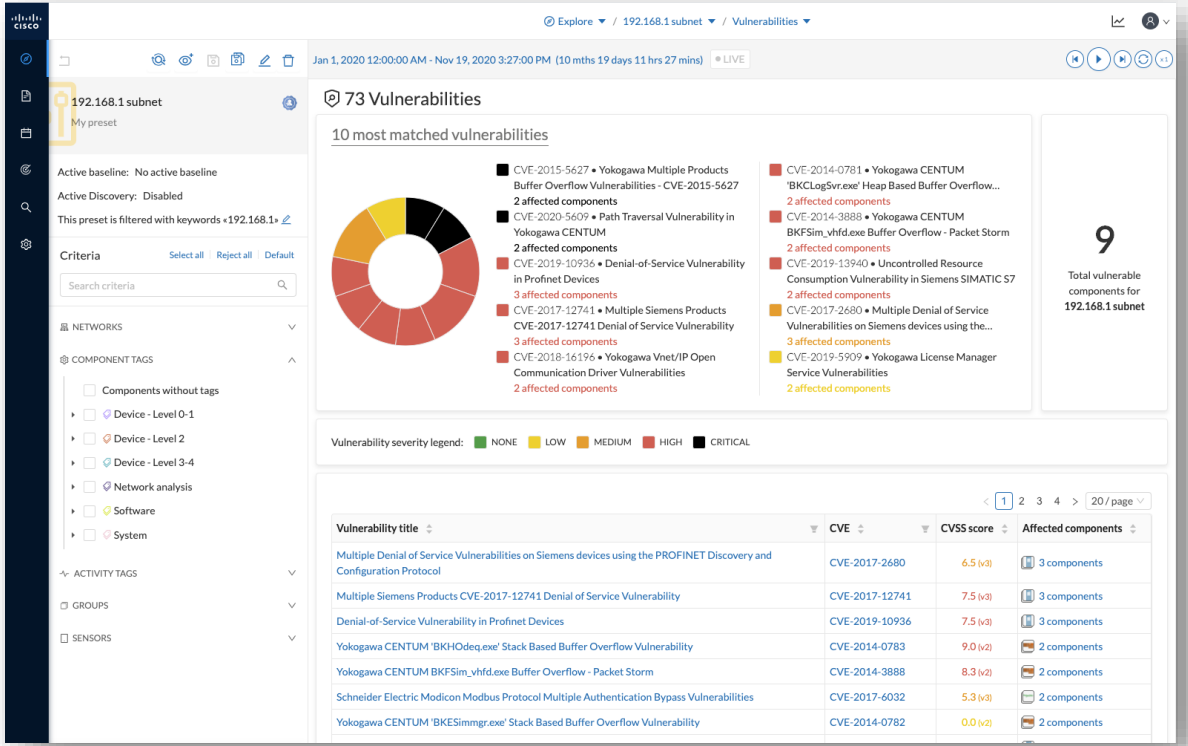
Dynamic map of all communication activities with detailed application flow level information



Identify & Track Vulnerabilities

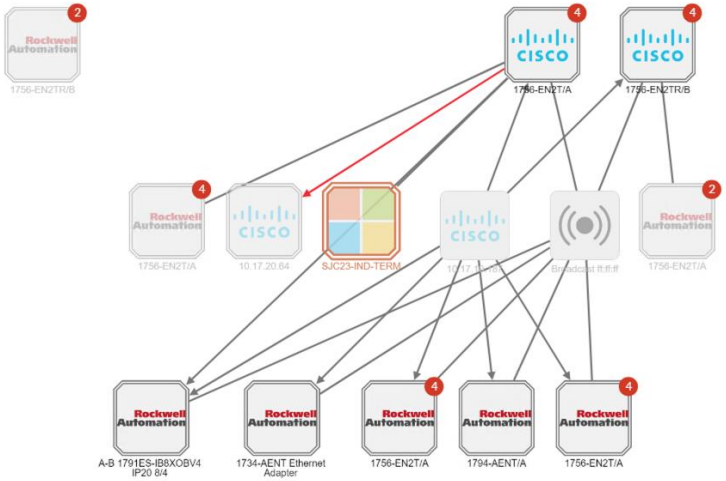
Vulnerability Detection

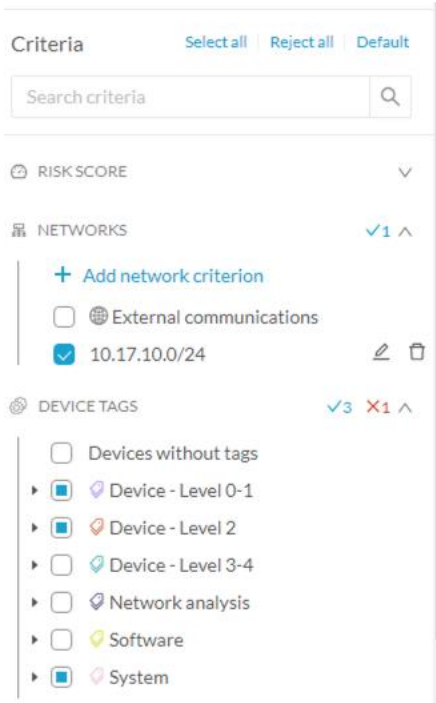
Identify known asset vulnerabilities so you can patch or protect them before they are exploited



Filtering and Grouping

Filters allow the user to customize how assets are displayed and grouped



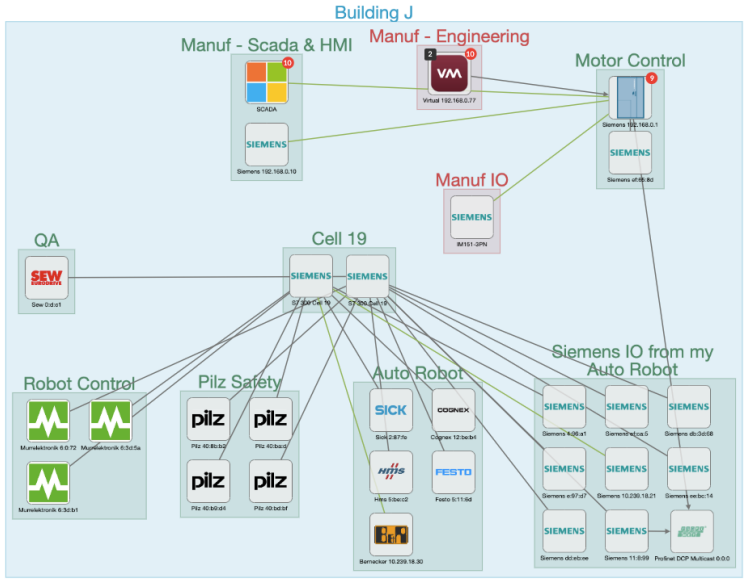


Filter Criteria

	Filter Category	Function	Examples
1	Risk Score	Filters components by risk score range	Risk Score > 70
2	Networks	Filters components by VLAN and/or subnet	10.17.90.0/24
3	Device Tags	Filter devices using device tags such as Purdue level, device type, system manufacturer	Device – Level 2, Controller, Rockwell Automation, Device with Public IP, Windows device
4	Activity Tags	Filter by tags assigned to observed flows such as control system behavior or industrial protocols	Start/Stop CPU, RDP, Multicast, Encrypted traffic, CIP, PTP
5	Groups	Filter by user created tags	Group: Assembly
6	Sensors	Filter by Cisco Cyber Vision sensor	Select sensor(s) on a production line

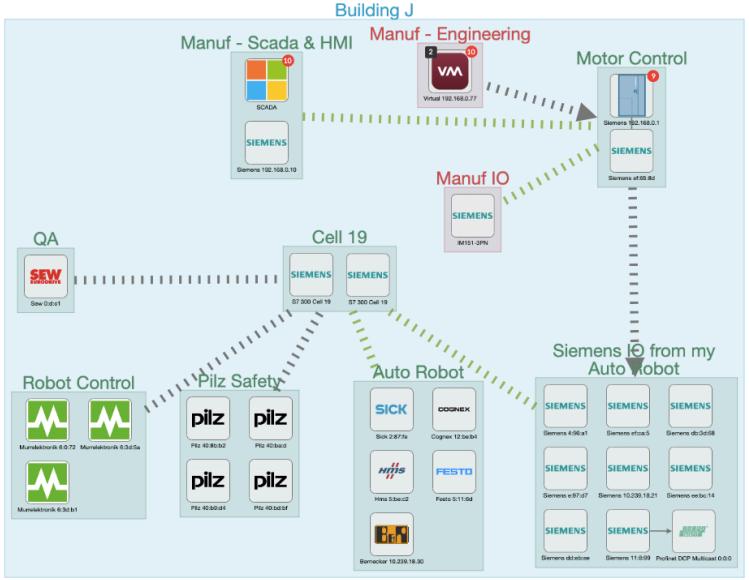
Aggregated activities match IEC62443 conduits

Unaggregated



View all asset relationships

Aggregated



Easily browse through conduits

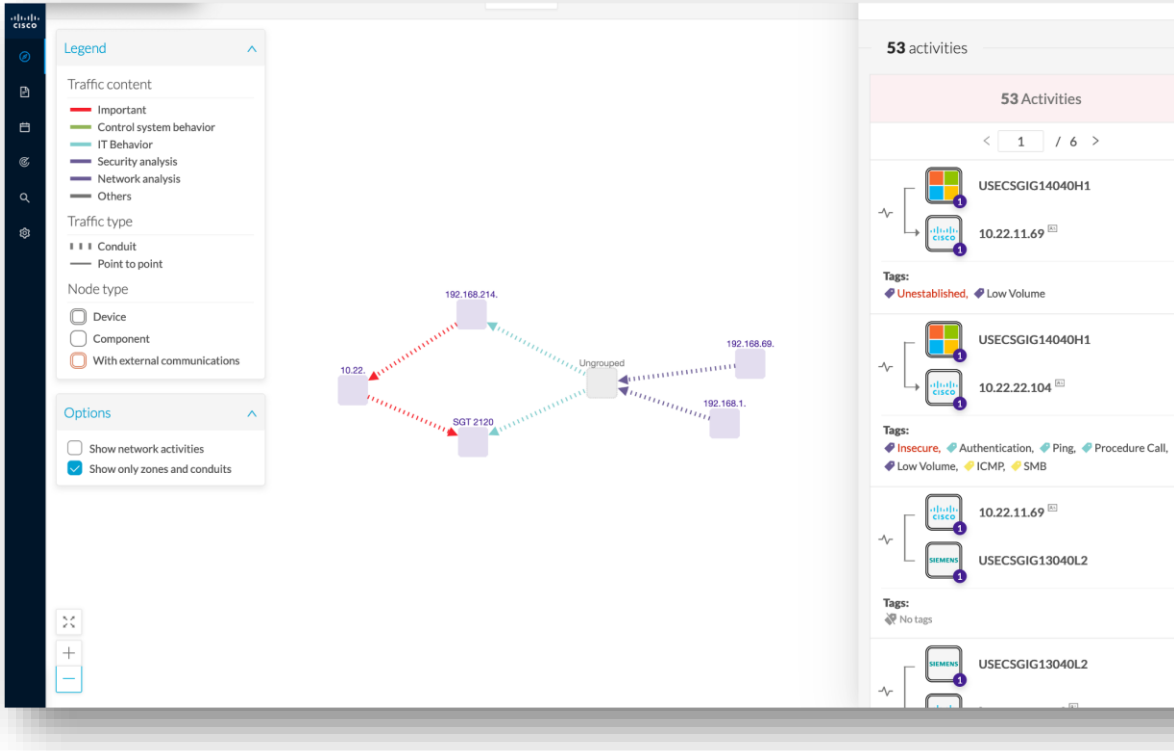
Visualize Zones & Conduits

Zones

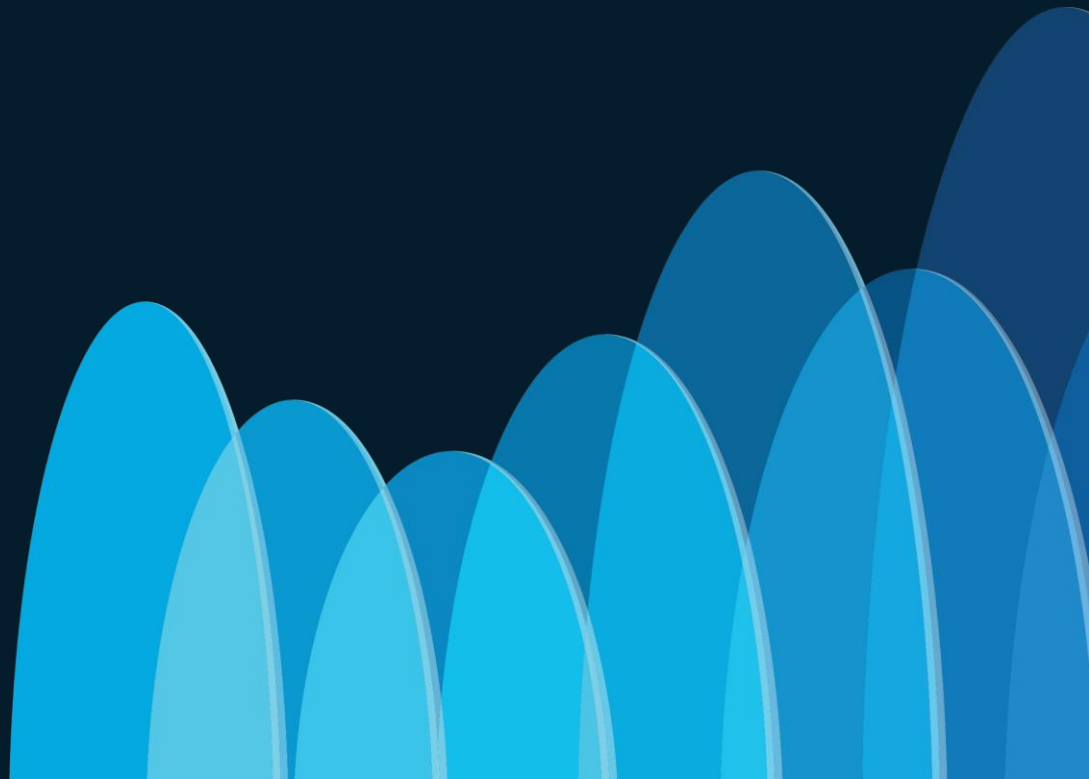
View simplified maps of grouped assets as zones

Conduits

Identify communications across zones to ensure valid flows don't get blocked when implementing segmentation



The role of Firewalls in OT

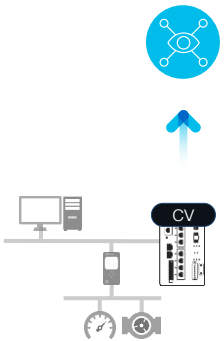


cisco Live!

Cisco Industrial Threat Defense

Asset Visibility & Security Posture

Cisco Cyber Vision

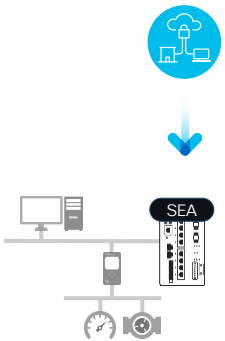


Network embedded CV Sensor

Zero Trust for OT

Zero Trust Network Access

Cisco Secure Equipment Access

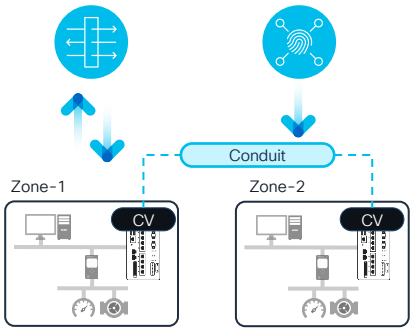


Network embedded ZTNA Gateway

IEC 62443 Zones & Conduits

Cisco Secure Firewall

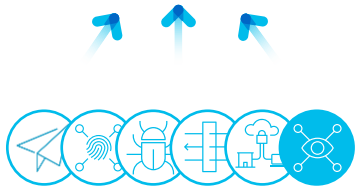
Cisco ISE



Network enforced segmentation

Cross-Domain Detection, Investigation & Response

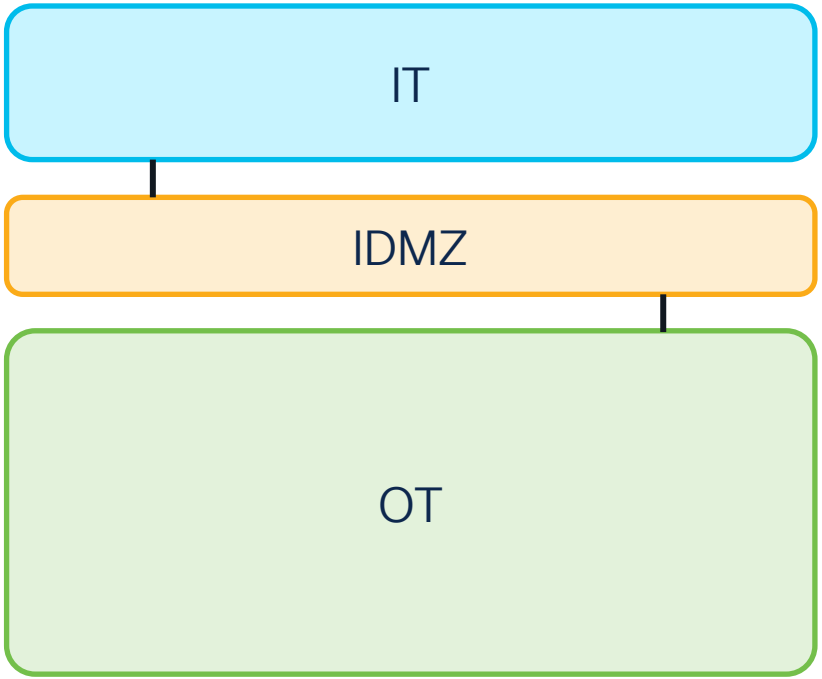
splunk> a cisco company



Visibility across the entire attack chain

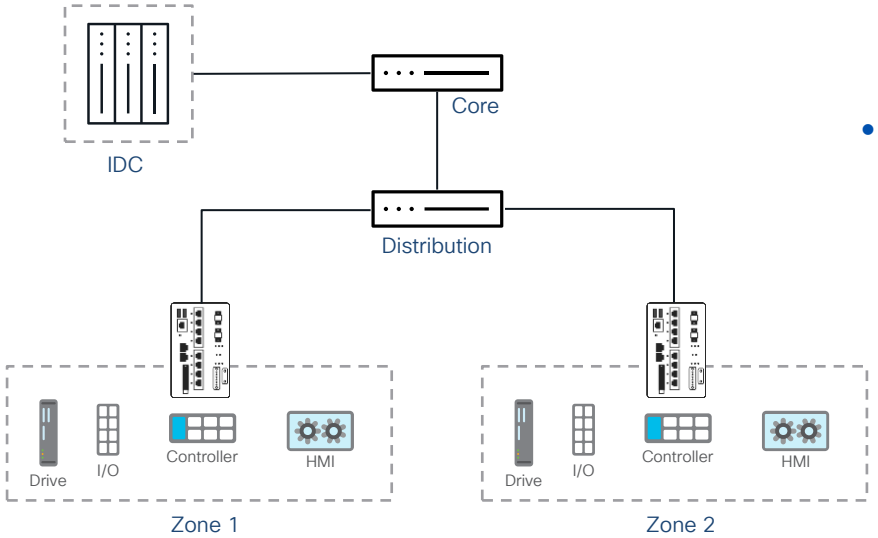
Network as a fabric to secure OT at scale

Re-visiting the Purdue Model



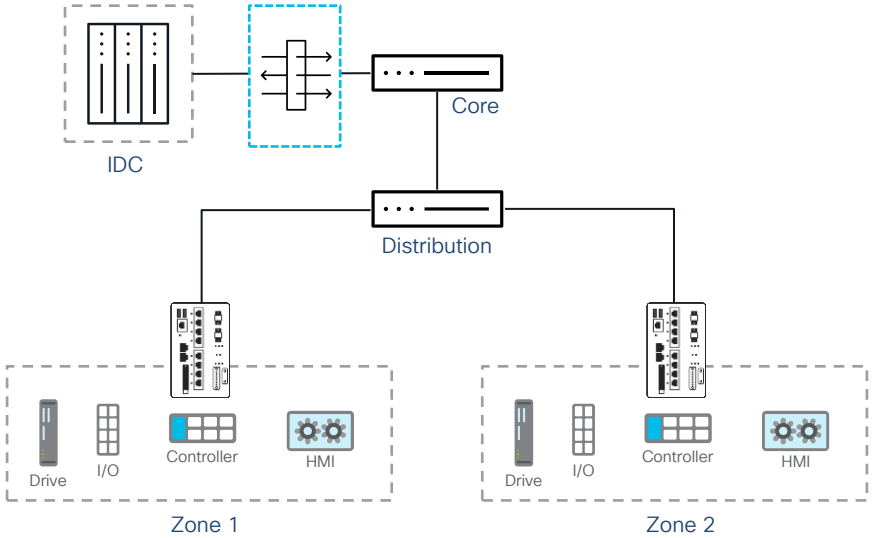
- Firewalls are usually the first point of contact between IT and OT domains
- Firewalls are used to segment DMZ applications from each other
- Deny by Default policy, only allow trusted communication through

Going beyond the IDMZ



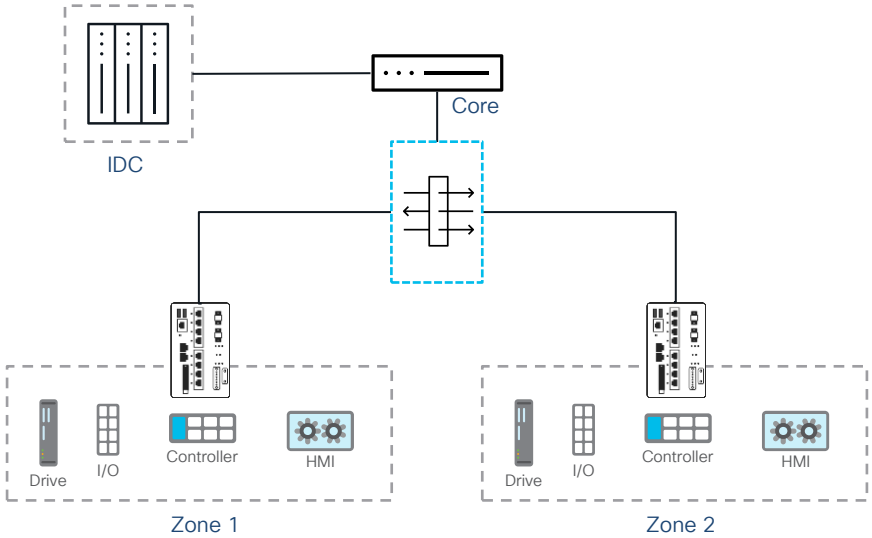
- Most manufacturing networks have a distribution network (IDF) in a conditioned space
- VLANs terminate at the IDF to go east/west across Cell/Area Zones

Where to place a firewall?



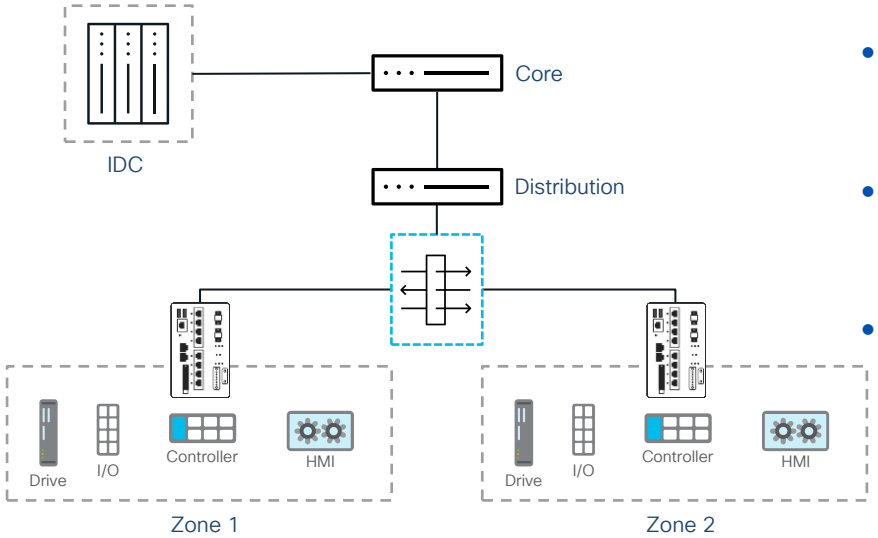
- In front of the Industrial Data Center
  - Protects critical infrastructure from applications in the IDC
  - IDC servers are typically the candidates for cloud / IT access to subject to a wider attack surface
  - Limits the impact a vulnerability in the IDC can have on the critical infrastructure

Where to place a firewall?



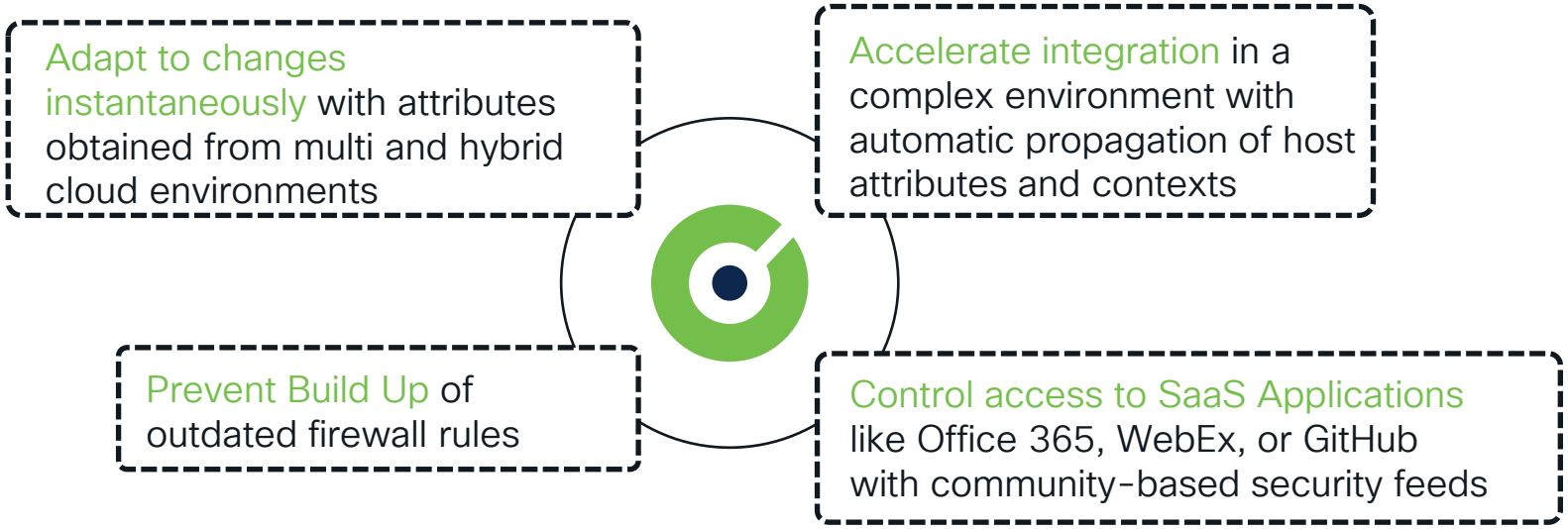
- Terminate OT VLANS
  - All VLANs in the OT network will terminate at the firewall
  - Traffic that crosses VLAN boundaries will be subject to firewall rules
  - Great choice for well architected networks

Where to place a firewall?

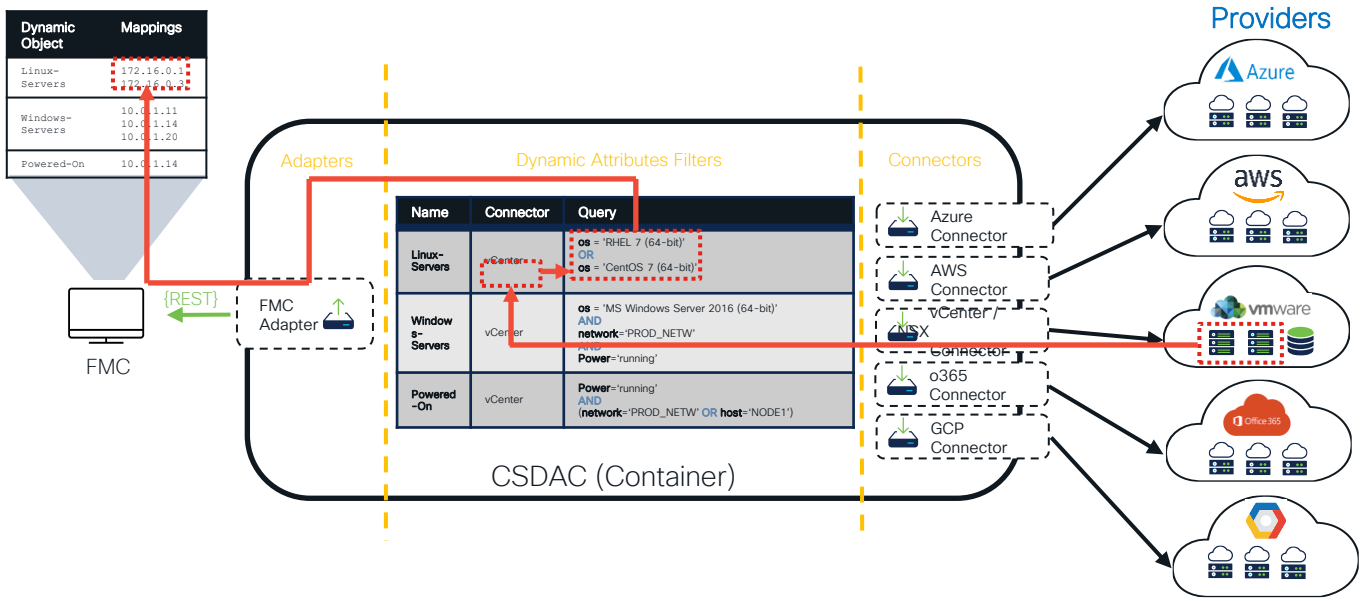


- Transparent Firewall before distribution layer
- Catalyst switching continues to terminate VLANs
- Transparent firewalls will also capture inter-VLAN connection
- Great for existing environments to bolt security on

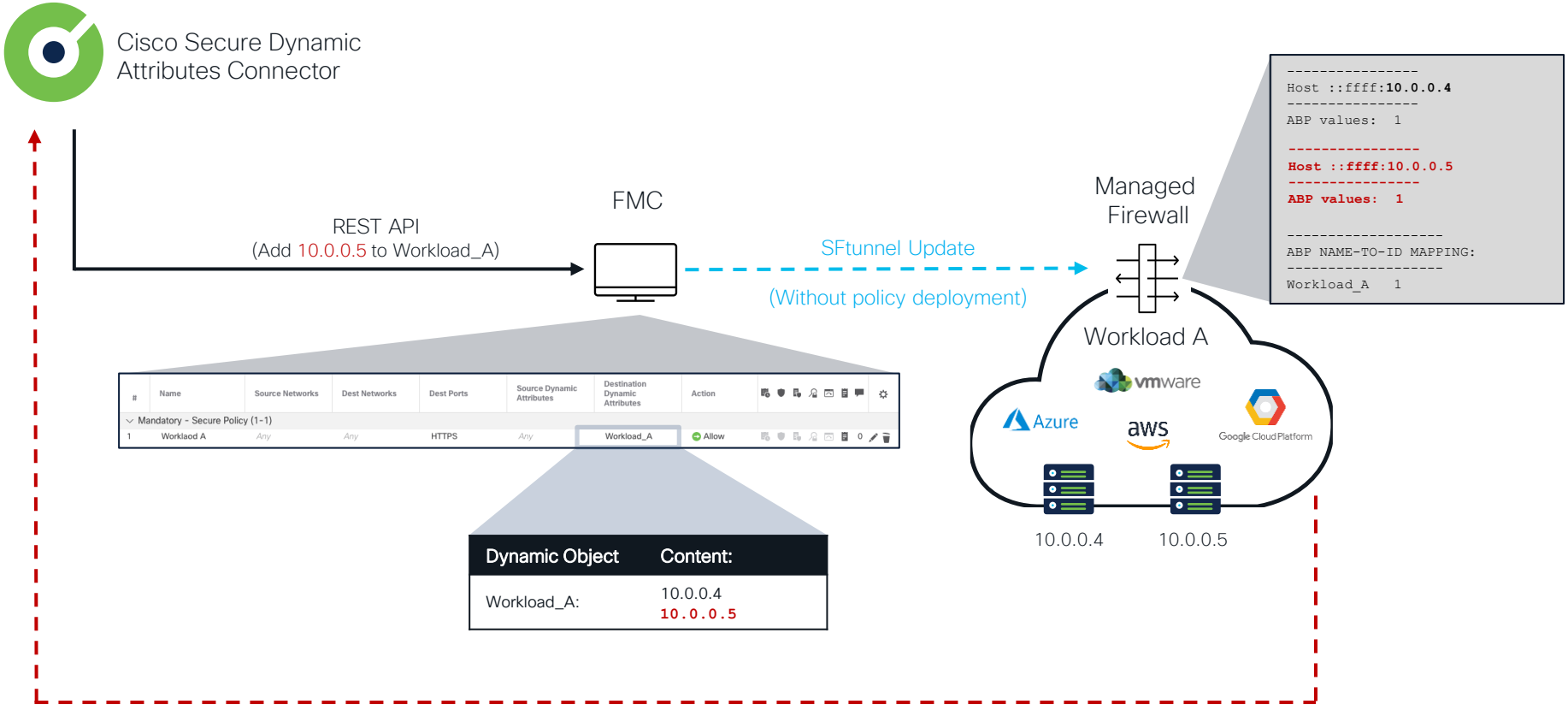
Dynamic Attributes in Cisco Secure Firewall



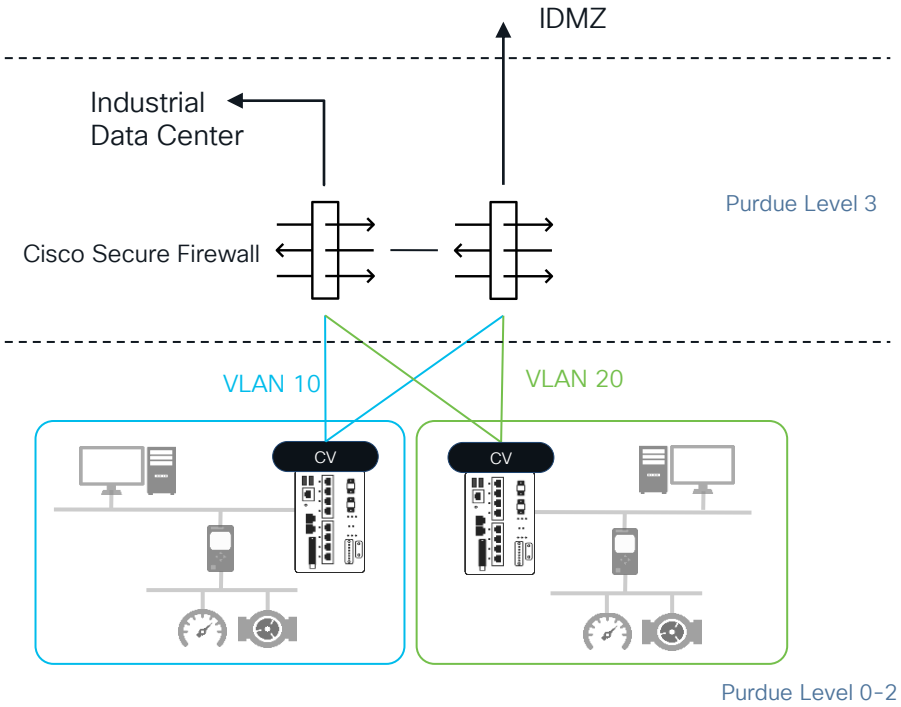
Cisco Secure Dynamic Attributes Connector (CSDAC)



Dynamic Objects in Action

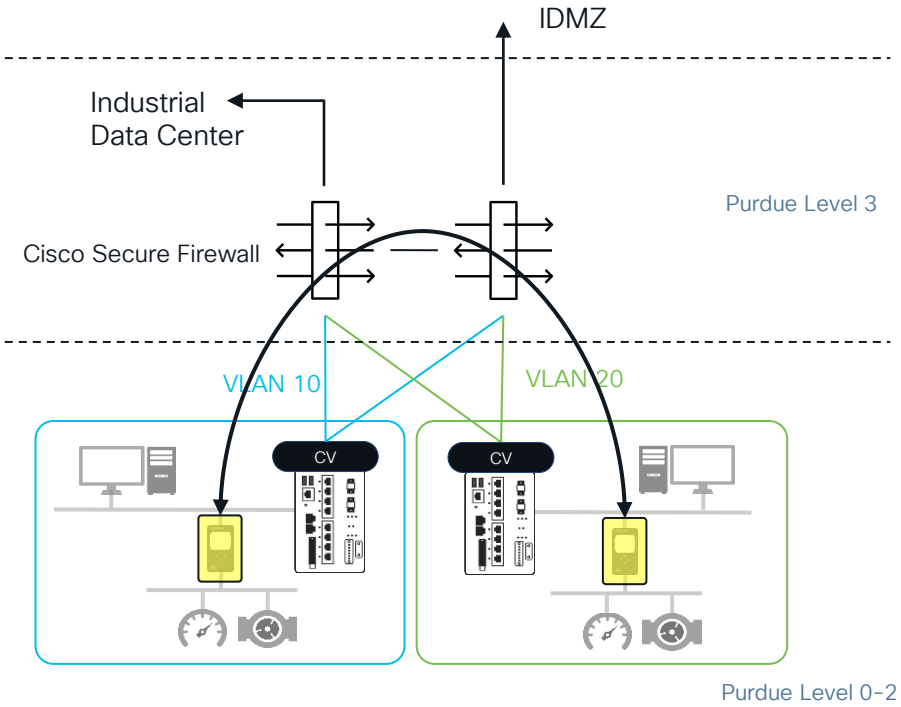


Firewalls in Industrial Networks



Name	Action	Source	Destination	App
Cell1-Cell2	Deny	VLAN10	VLAN20	any
Cell2-Cell1	Deny	VLAN20	VLAN10	any

Dynamic Attribute Example: Interlocking PLC

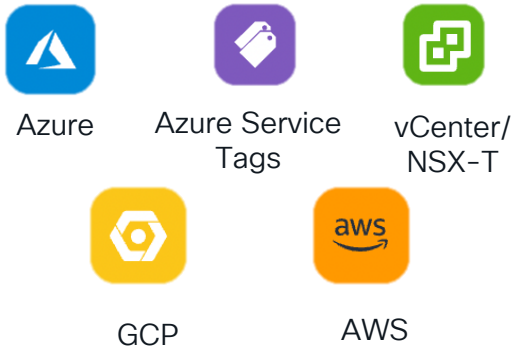


Name	Action	Source	Destination	App
PLC-PLC	Allow	C1_PLC	C2_PLC	CIP
Cell1-Cell2	Deny	VLAN10	VLAN20	any
Cell2-Cell1	Deny	VLAN20	VLAN10	any

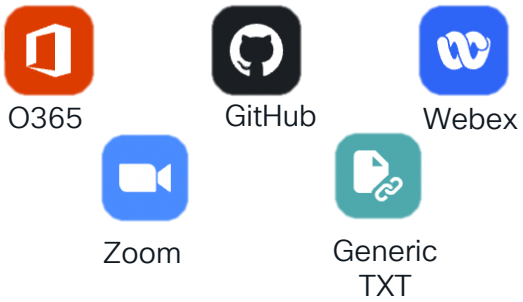
Supported Connectors

CSDAC 3.0.0 release adds Cyber Vision

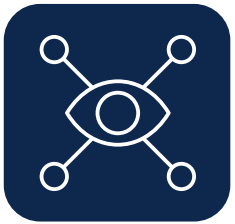
Cloud Connectors



Public Feeds Connectors

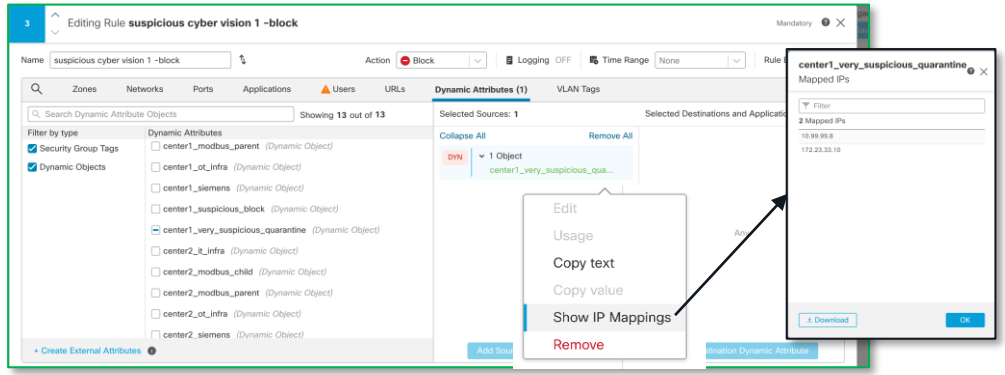


Cisco IIoT Connector



Cyber Vision

Cisco Secure Dynamic Attributes Connector Cyber Vision Integration

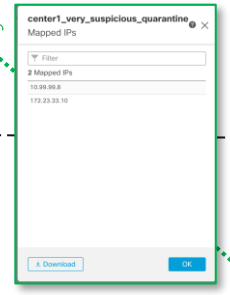


Cloud

On-Prem

CDO FMCe

Dynamic objects (REST)



Policy change

FMC

Dynamic objects (REST)

Policy change

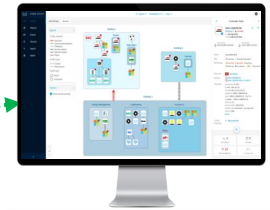
FTD

FTD

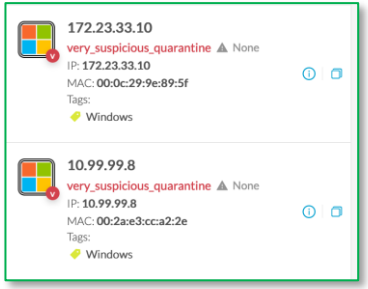
Standalone CSDAC instance

API calls

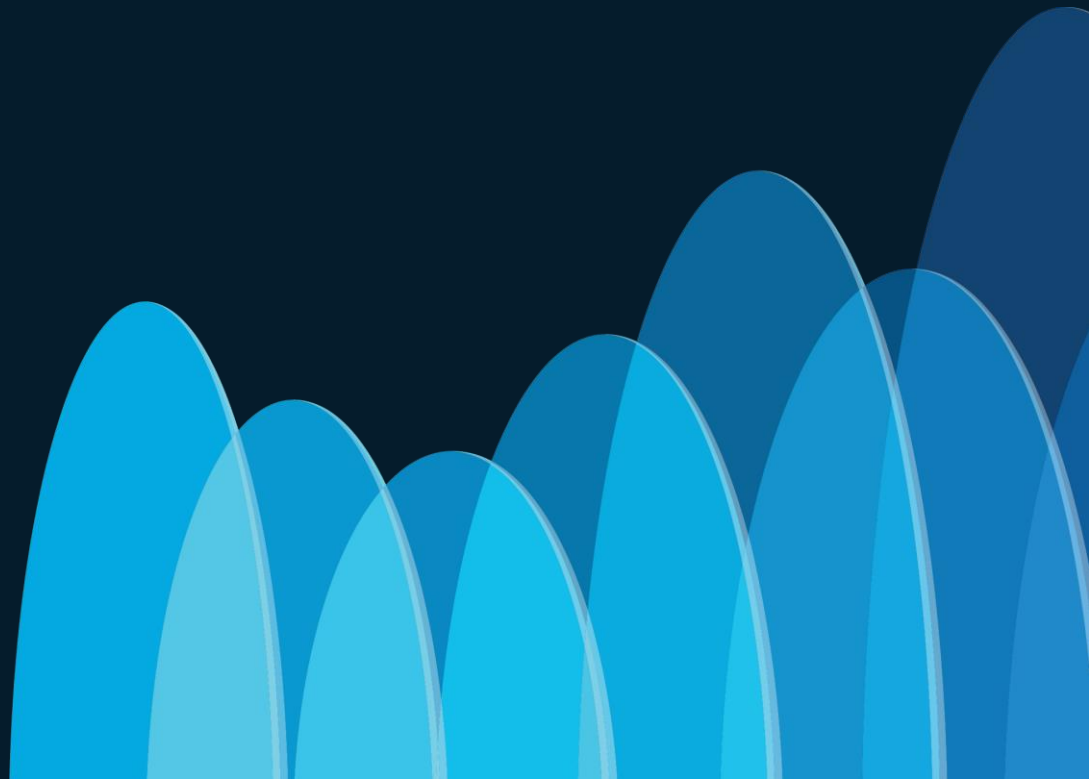
Groups and associated IPs



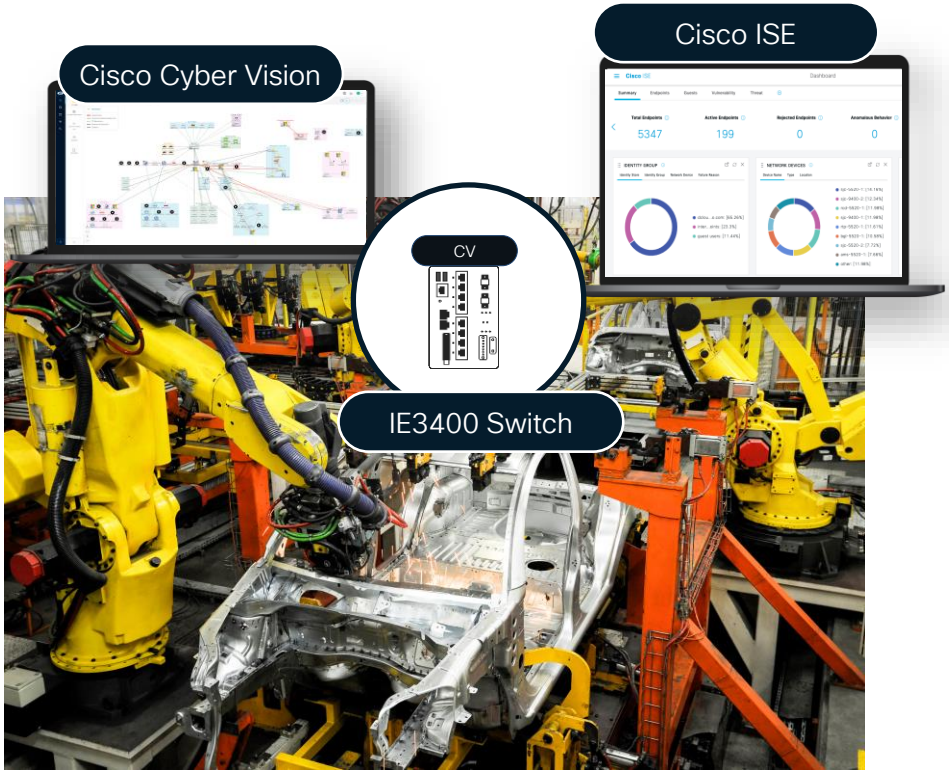
Center 1



Network as an Enforcer



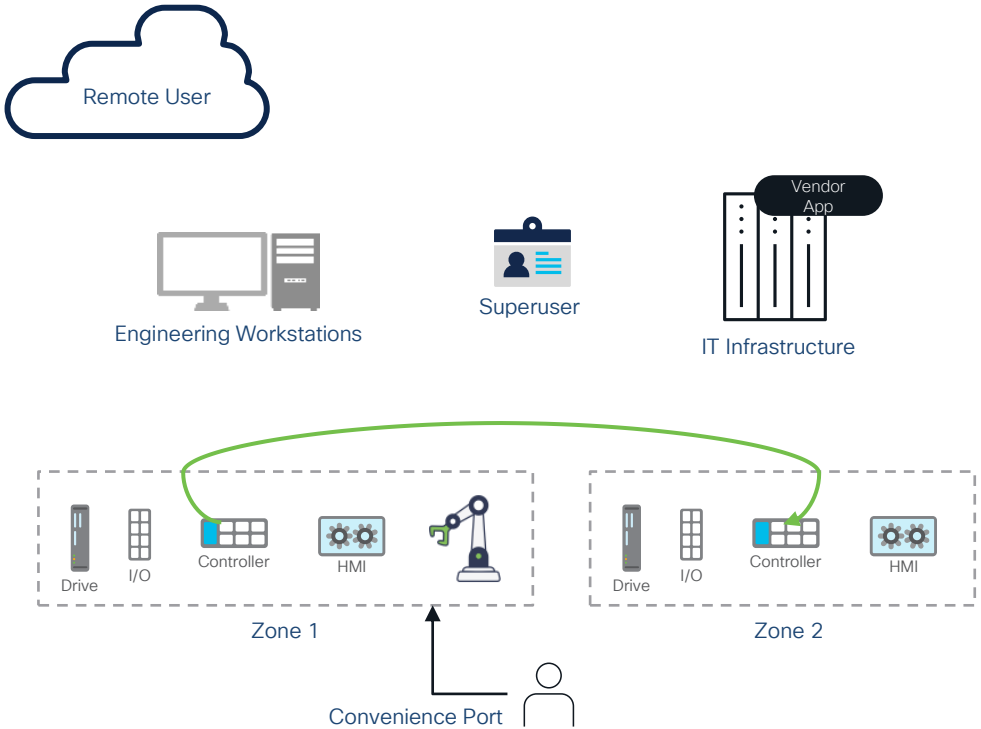
TrustSec Case Study: Car Manufacturer



Cisco Proposed Solution

- Network designed based on C9300 distribution layer and IE3400 switches on the plant floor
- Cyber Vision deployed on C9300 & IE3400 switches for visibility to the security posture of OT assets
- Cyber Vision visibility used to drive zone level segmentation on IE3400 switches in the OT network using Cisco ISE and TrustSec

9 Use Cases for Securing Industrial Networks

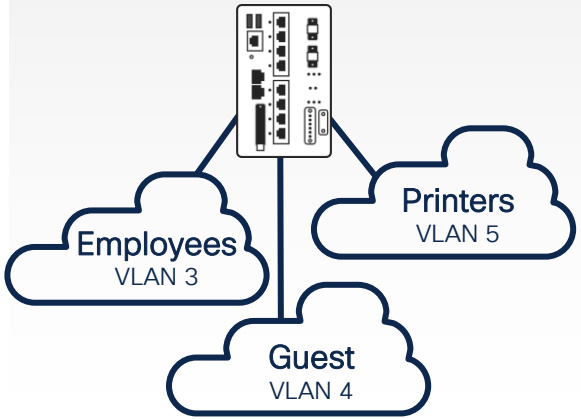


1. All devices within a zone can communicate freely
2. Deny by default across zone
3. Convenience Port within a zone
4. Engineering workstations to all devices within designated zones
5. Superusers – named employees to all devices
6. IT applications have restricted access to all zones
7. Vendor applications to specified machines
8. Communication of named devices between zones (e.g. Interlocking PLC)
9. Remote Access to single application temporarily

ISE Segmentation Technologies

VLANs

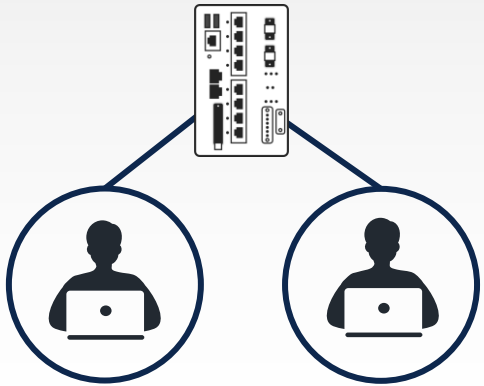
Dynamic VLAN Assignments



Per port / Per Domain / Per MAC

ACLs: DL, Named, DNS

Downloadable ACL (Wired) or
Named ACL (Wired + Wireless)

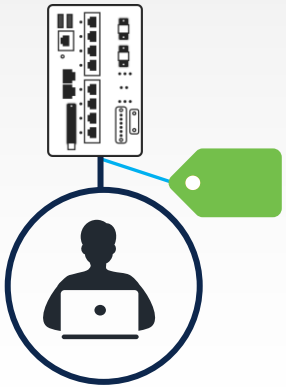


Employee
permit ip any any

Contractor
deny ip host <critical>
permit ip any any

Scalable Group Tags

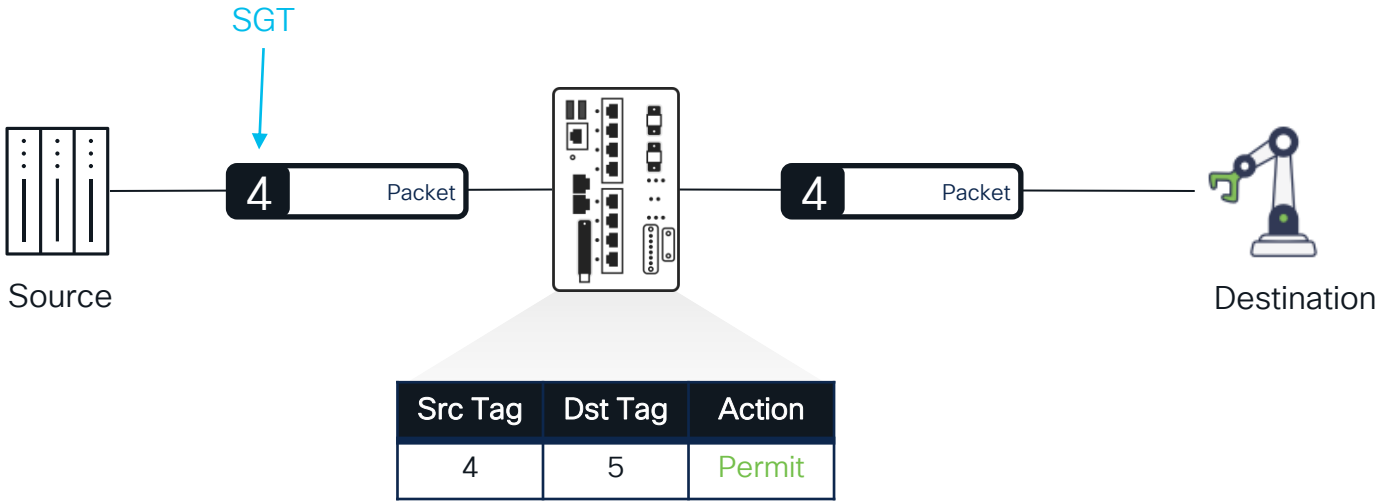
Cisco Group-Based Policy



16-bit SGT assignment and
SGT based Access Control

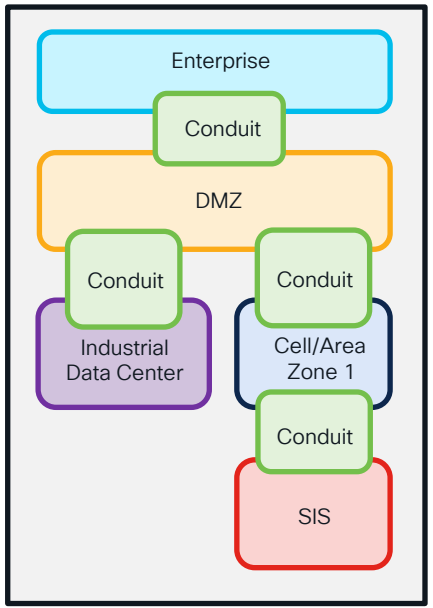
What are Security Group Tags (SGTs)?

Role Based Access Control embedded in the network



Zones & Conduits with SGTs

ISA/IEC 62443

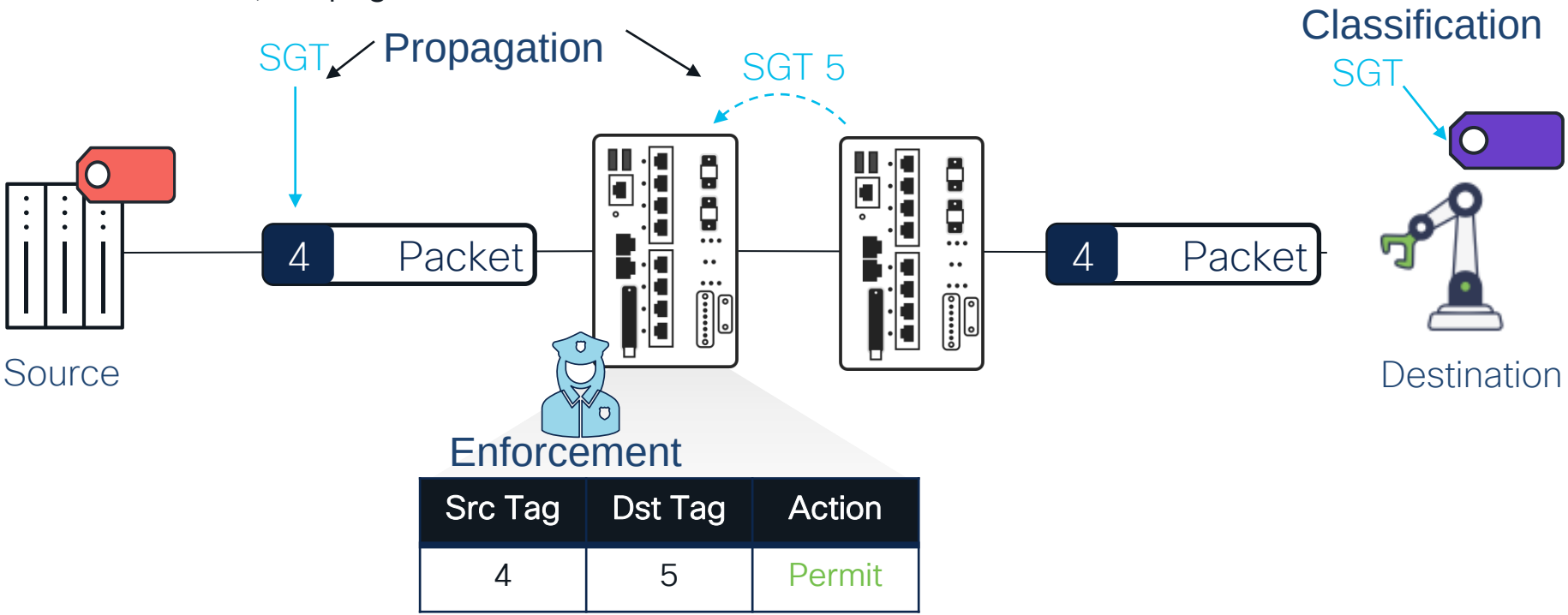


TrustSec Matrix

	Enterprise	DMZ	IDC	Cell 1	SIS
Enterprise	✓	✗	✓	✗	✗
DMZ	✗	✓	✓	✗	✗
IDC	✓	✓	✓	✓	✗
Cell 1	✗	✗	✓	✓	✗
SIS	✗	✗	✗	✗	✓

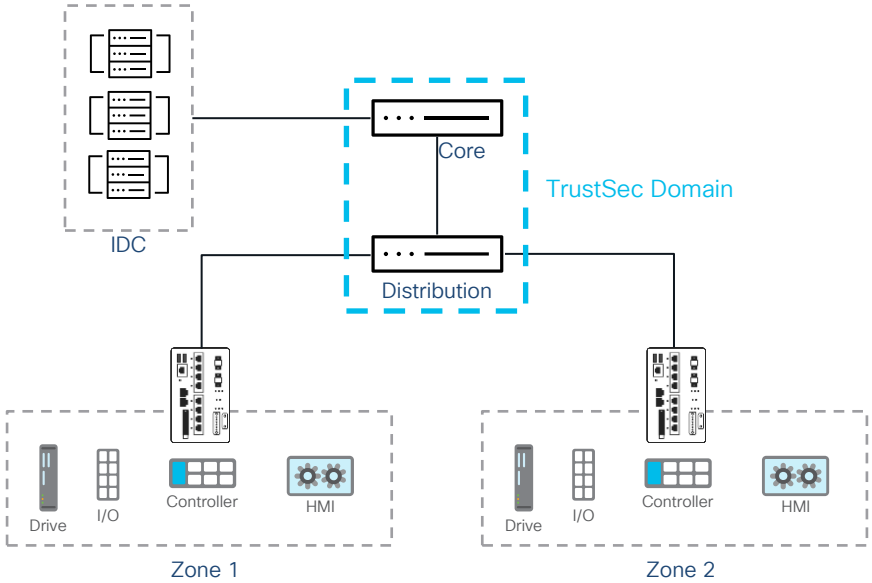
Cisco TrustSec – Key Concepts Review

Classification, Propagation and Enforcement



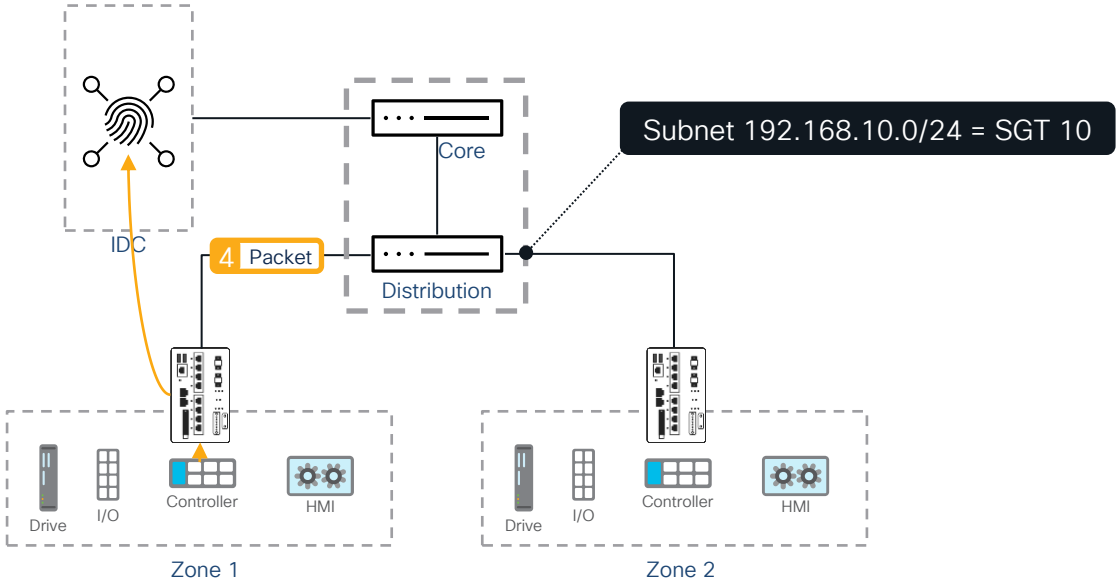
Case Study Takeaway

Define TrustSec Domain based on requirements
Use case #1: All devices within a Zone should be able to communicate freely



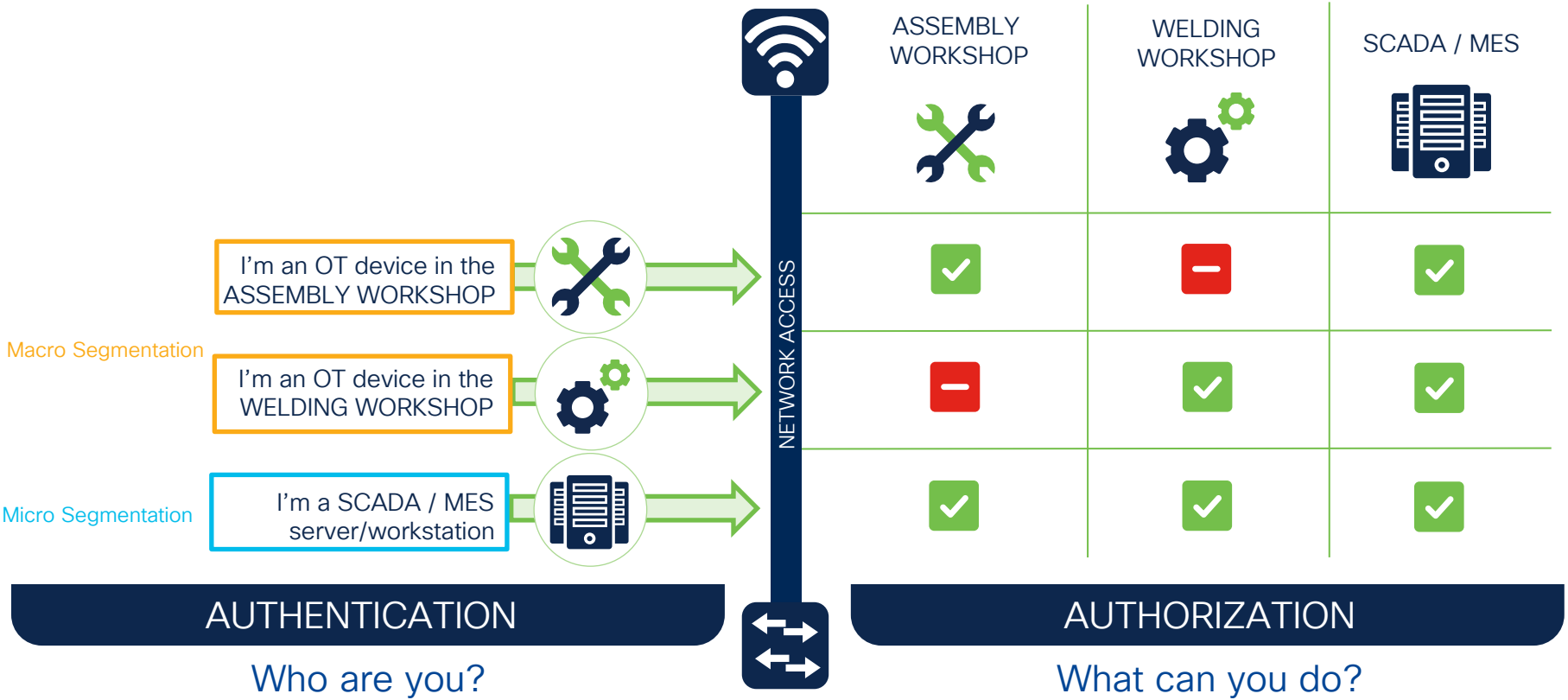
- If my TrustSec domain resides within a Cell/Area Zone, I must create policy to allow communication through the switches
  - More on this later!

How do we classify an SGT?



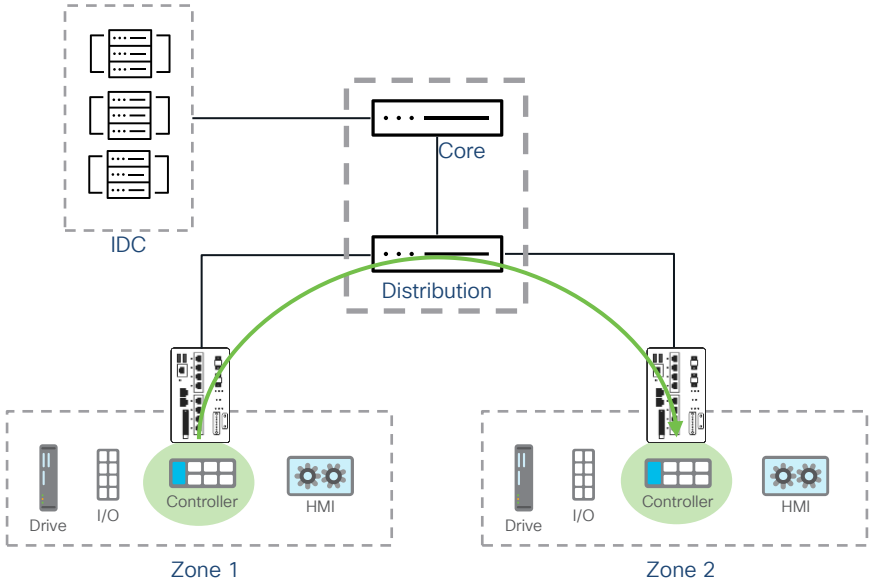
- Static Classification options:
  - VLAN to SGT
  - Subnet to SGT
  - IP to SGT
  - Interface to SGT
- Static classification can be done directly on a switch, or centrally in ISE
- Dynamic Classification is done via Authentication to ISE

Cisco TrustSec – Hybrid Macro / Micro Segmentation



Use Case #8:

Communication of named devices between zones is allowed



- Zone 1 -> Zone 2 is denied
- Zone 1 PLC -> Zone 2 PLC is allowed

Dynamic Classification of SGTs in ISE

Endpoint Request Access

- Endpoint is identified and trust is established
- Posture of endpoint verified to meet compliance

Endpoint classified, and profiled into groups

- Endpoints are tagged x/SGTs
- Policy applied to profiled groups based on least privilege

Trust continually verified

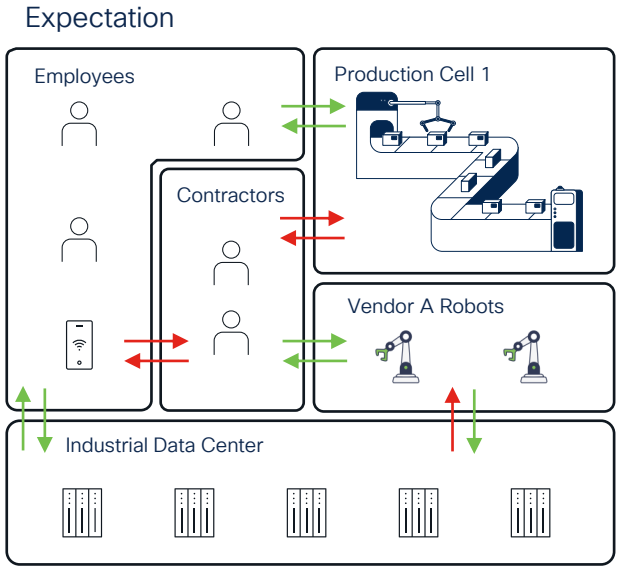
- Continually monitors and verifies endpoint trust level
- Vulnerability assessments to identify indicators of compromise
- Automatically Updates access policy

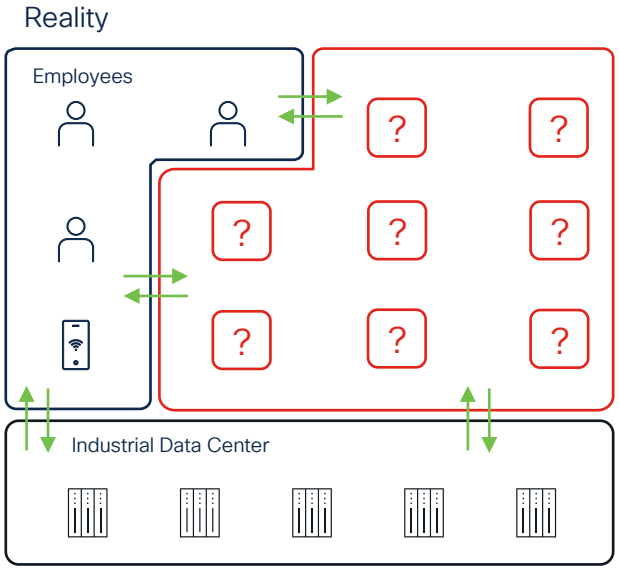
Endpoint authorized access based on least privilege

- Access granted
- Network segmentation achieved

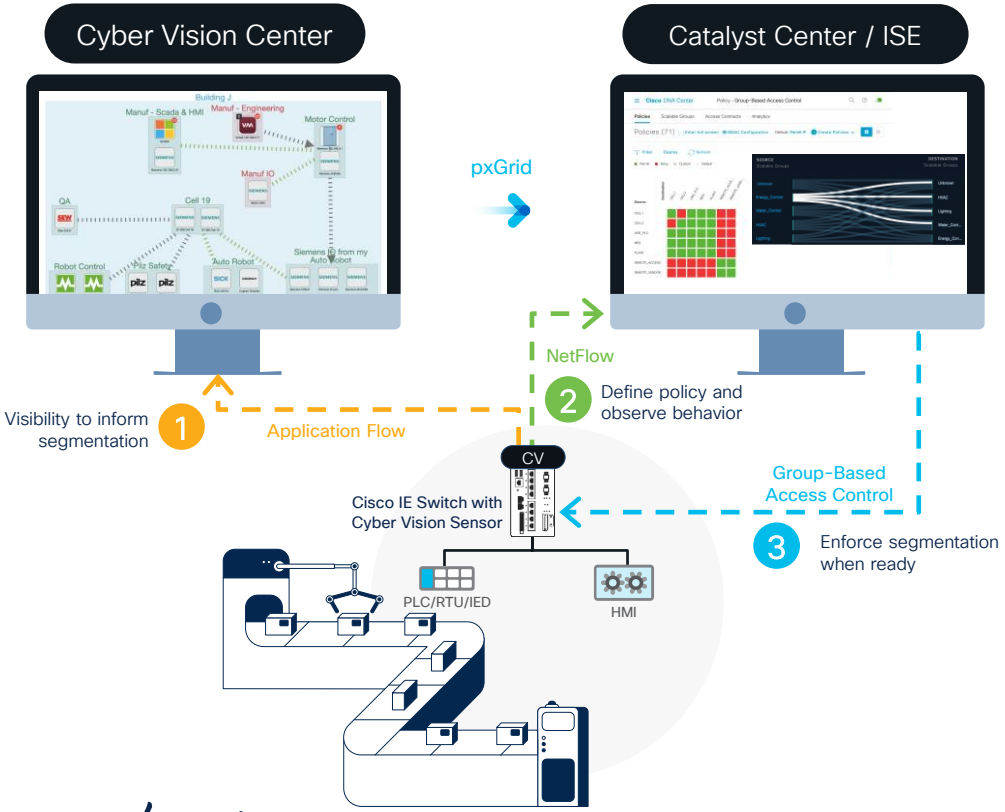
Least Privilege Access:

Expectation vs. Reality





Use Visibility to Influence Segmentation



Visualize Zones & Conduits

Group endpoints into zones to visualize aggregated flows as conduits to inform segmentation policy

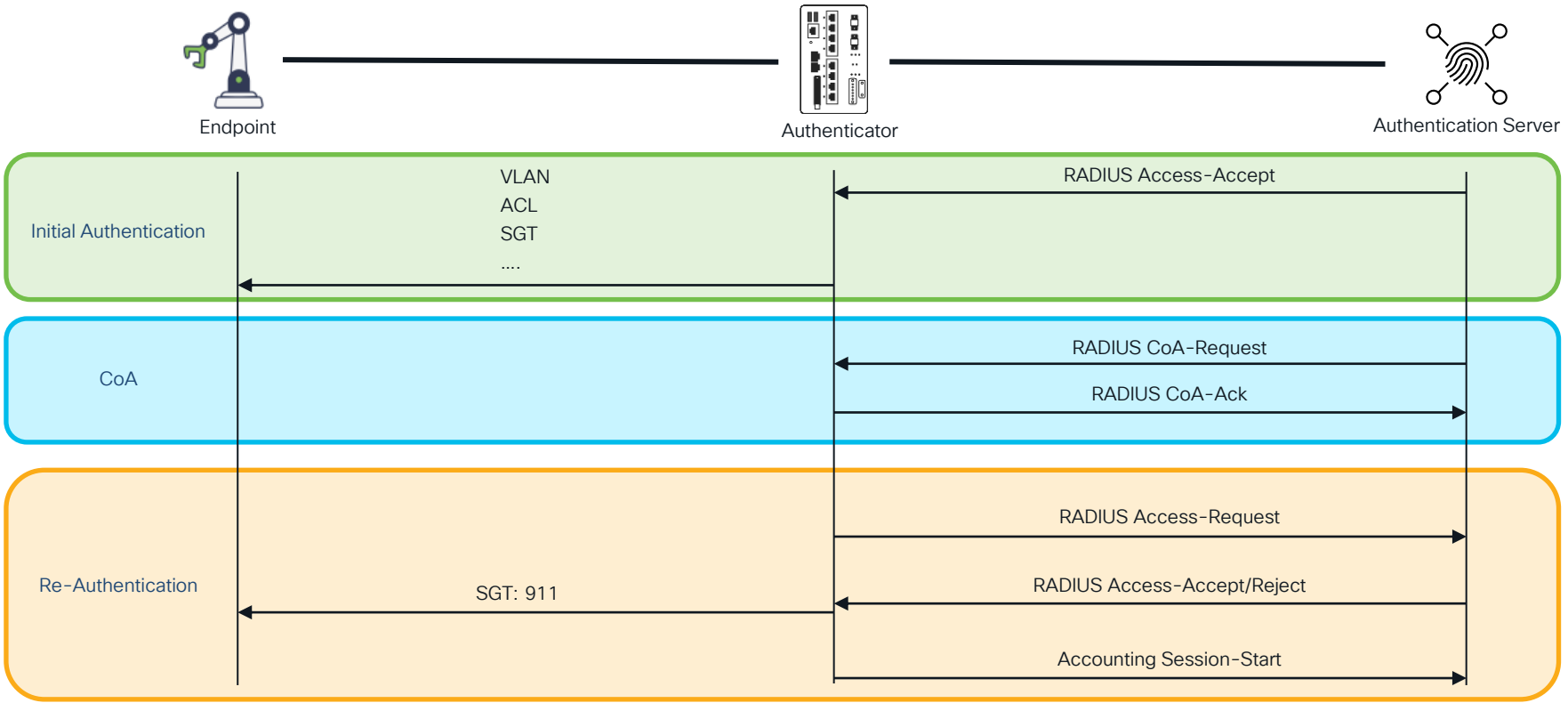
Dynamic SGT Mapping

Cyber Vision grouping results in dynamic Group-based policy assignment to endpoints through ISE

Monitor Before Enforcement

Visualize Group-based network behavior in Catalyst Center and enable enforcement when confident after monitoring

Change of Authorization (CoA)



Case Study Takeaway

Reduce complexity by creating SGTs based on Privileges instead of device type

Device Type	SGT
Vision Cameras, Barcode Scanners, Controllers, Convenience port, Drive, HMI, Industrial Printer, Laser Systems, Inverters, Leak Tester, PLC Interlock, IO, Private IO, Press controllers, Process Serves, RFID modules, Security Cameras, Torque Tools, Robots, Andon, Process PC, …	Cell/Area Zone devices Interlock Workstation

Case Study Takeaway

Classification depends on asset capabilities and “role”

Static assignment based on location

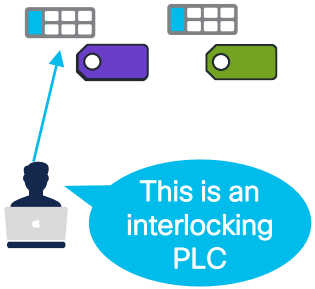
OT device in body area

OT device in painting area

Use the network to answer: “Where are you?” (VLAN or Subnet)

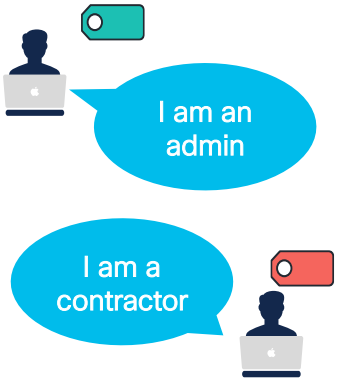
Assignment for "named" devices

OT device in body area



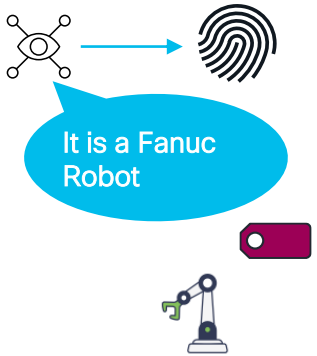
Use Cyber Vision to “promote”/change device tag

Dynamic assignment for users



Use credentials to confirm identity (802.1x)

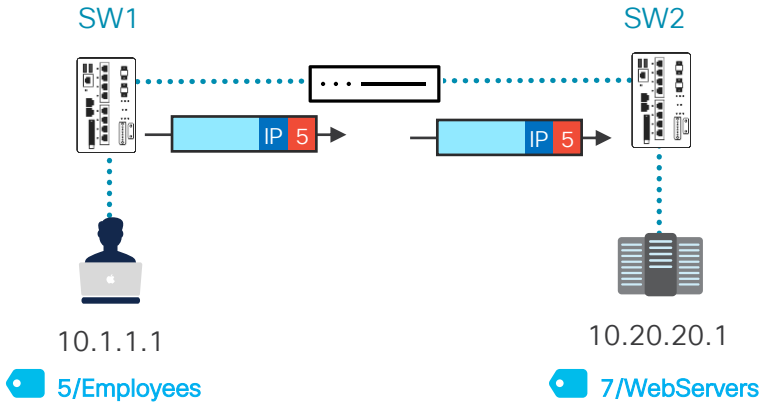
Dynamic assignment for OT devices



Use device attributes (ISE) and communication patters (Cyber Vision) to profile device

TrustSec Propagation

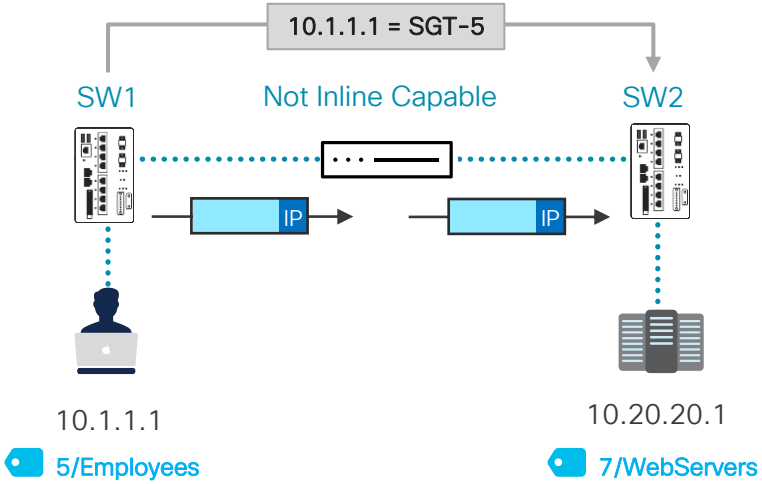
DATA PLANE PROPOGATION (INLINE TAGGING)



SGT carried inline in the data traffic. Methods include, SGT over:

Ethernet | MACSec | LISP/VxLAN | IPSec | DMVPN | GETVPN

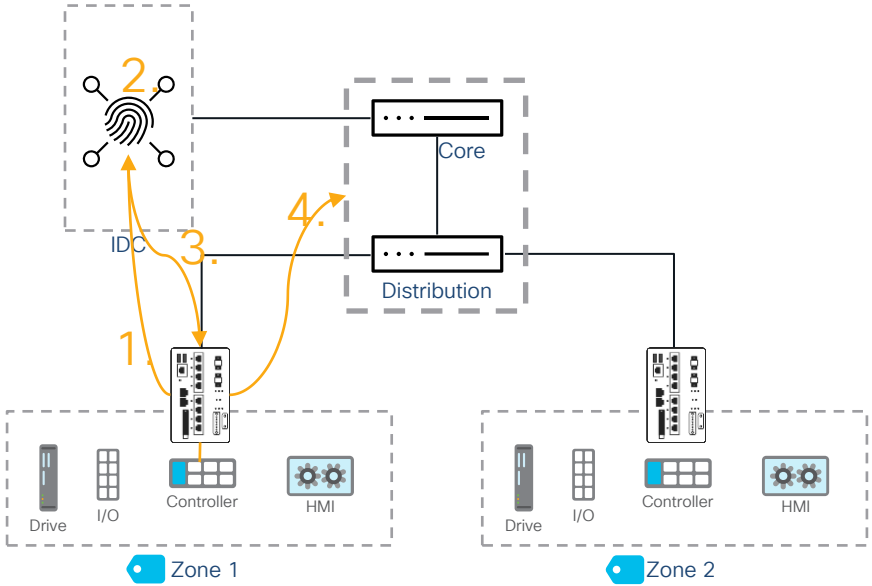
CONTROL PLANE PROPOGATION (SXP)



IP-to-SGT data shared over control protocol. No SGT in the data plane. Methods include, IP-to-SGT exchange over:

SXP | pxGrid

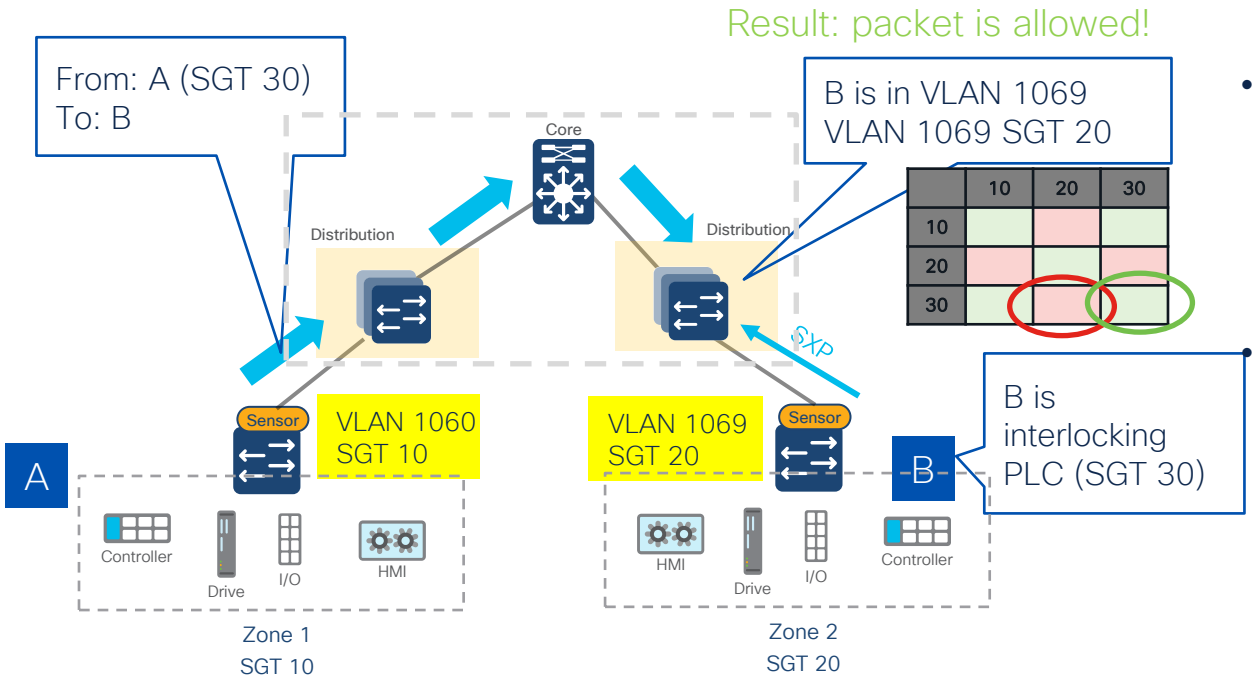
SXP in Action



1. PLC connects to Cisco IE Switch and authenticates to ISE via MAB
2. Device is profiled as Interlocking PLC and ISE assigns the device with the SGT for interlocking PLCs
3. IE Switch receives the SGT assignment, and creates a binding for the PLC IP address and the newly assigned SGT
4. IE switch shares the IP to SGT mapping to the TrustSec domain

Case Study Takeaway

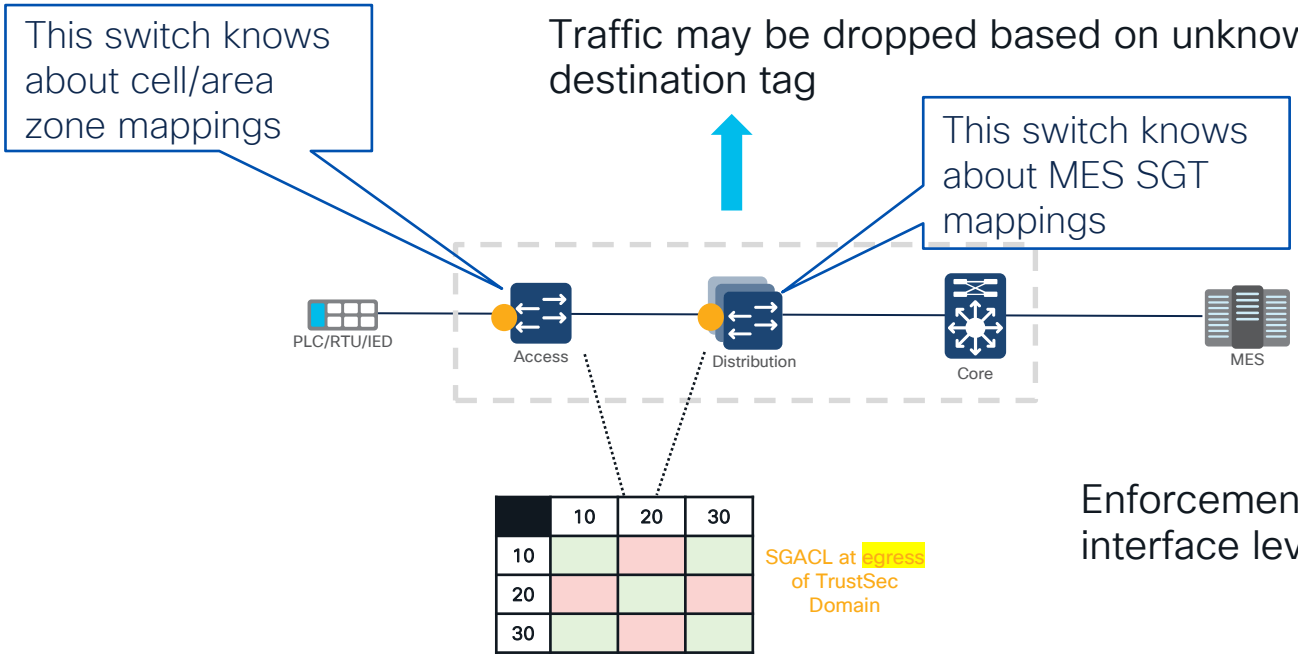
SXP propagation is required when enforcement is not at the access & dynamic authentication is used. Needed for enforcement device to learn about destination tag



- SXP can be from ISE to Distribution Switch (centralized) or from access switch to Distribution Switch (distributed)
- SXP is configured via templates

Case Study Takeaway

What happens with MES to PLC traffic when we enforce twice on the packet path?

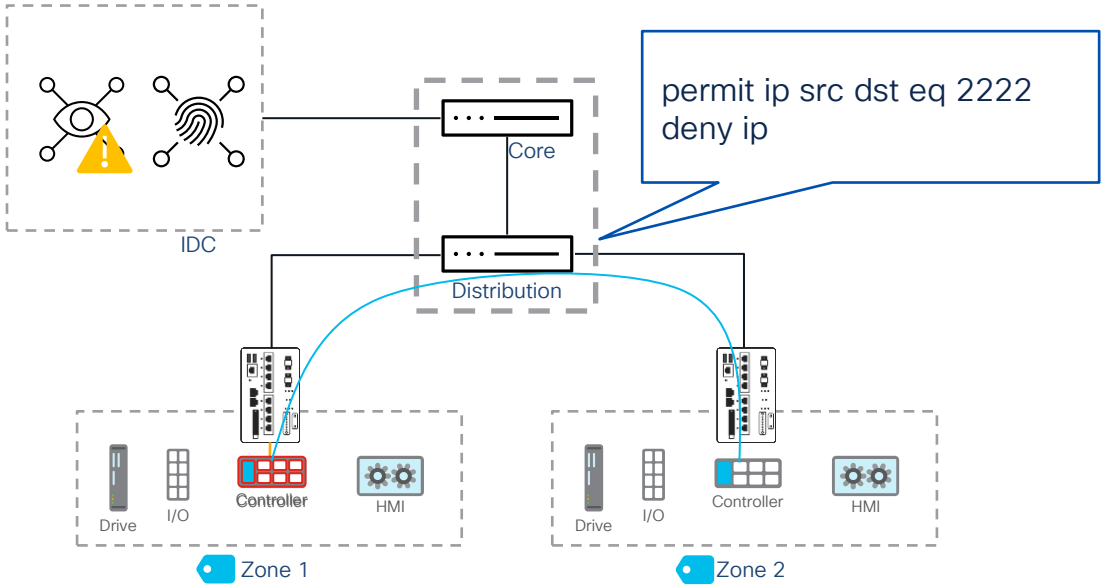


Enforcement can be disabled at the interface level

Enforcement

Case Study Takeaway

What happens when a device is replaced at midnight?



1. Controller in Zone 1 fails
2. Operator replaces PLC with new hardware
3. Evaluate worse case scenario and define workflow

Example:

PLC in zone 1 needs to talk PLC in zone 2

Default policy allows only port 2222 by default between zone 1 and zone 2

OT admin gets alert form CV about device and updates the tag to “promote” or “restrict” permissions

The TrustSec Matrix

	ASSEMBLY WORKSHOP	WELDING WORKSHOP	PAINTING WORKSHOP	INFRASTRUCTURE SERVICES
ASSEMBLY WORKSHOP	✓	−	−	✓
WELDING WORKSHOP	−	✓	−	✓
PAINTING WORKSHOP	−	−	✓	✓
INFRASTRUCTURE SERVICES	✓	✓	✓	✓

Defining Security Group Access Control Lists (SGACL)

	ASSEMBLY WORKSHOP	WELDING WORKSHOP	PAINTING WORKSHOP	INFRASTRUCTURE SERVICES
ASSEMBLY WORKSHOP	✓	–	–	✓
WELDING WORKSHOP	–	✓	–	✓
PAINTING WORKSHOP	–	–	✓	✓
INFRASTRUCTURE SERVICES	✓	✓	✓	✓

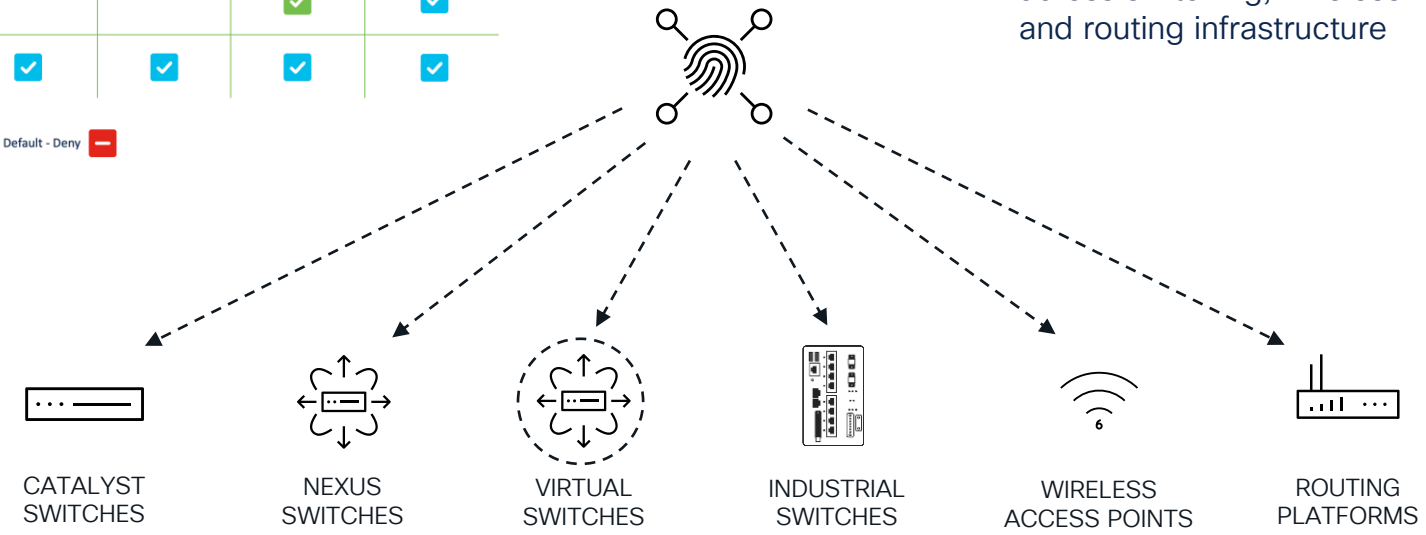
permit ip src dst eq 123
permit ip src dst eq 67
permit ip src dst eq 68
permit ip src dst eq 53
permit ip src dst eq 1812
permit ip src dst eq 1813
deny ip

Centralized Management, Distributed Enforcement

	ASSEMBLY WORKSHOP	WELDING WORKSHOP	PAINTING WORKSHOP	INFRASTRUCTURE SERVICES
ASSEMBLY WORKSHOP	✓			✓
WELDING WORKSHOP		✓		✓
PAINTING WORKSHOP			✓	✓
INFRASTRUCTURE SERVICES	✓	✓	✓	✓

Default - Deny

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



Making use of the default policy

	ASSEMBLY WORKSHOP	WELDING WORKSHOP	PAINTING WORKSHOP	INFRASTRUCTURE SERVICES
ASSEMBLY WORKSHOP	✓			✓
WELDING WORKSHOP		✓		✓
PAINTING WORKSHOP			✓	✓
INFRASTRUCTURE SERVICES	✓	✓	✓	✓

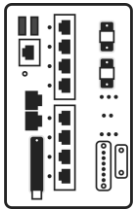
Default – Deny ⛔

What Devices Support SGT Enforcement?

Enforcement Nodes: Can actively block traffic

Catalyst Switches

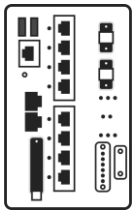
Typically used at the distribution & core



IE3400, IE9300

Typically used at access & aggregation

SXP Speakers: Can share IP to SGT information over SXP but cannot enforce traffic

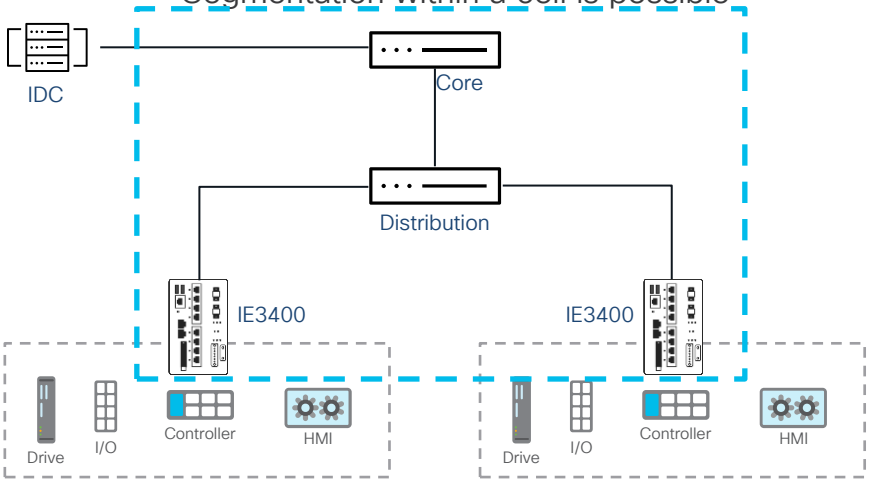


- IE3300
- IE3200
- IE3100
- IE2000

How device support effects the TrustSec domain

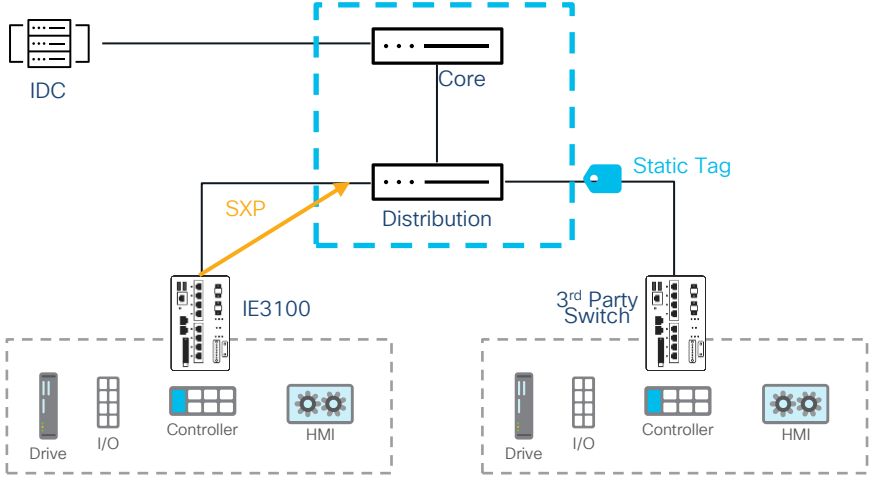
If all switches are capable of enforcement, my TrustSec domain can be everywhere

- Segmentation within a cell is possible

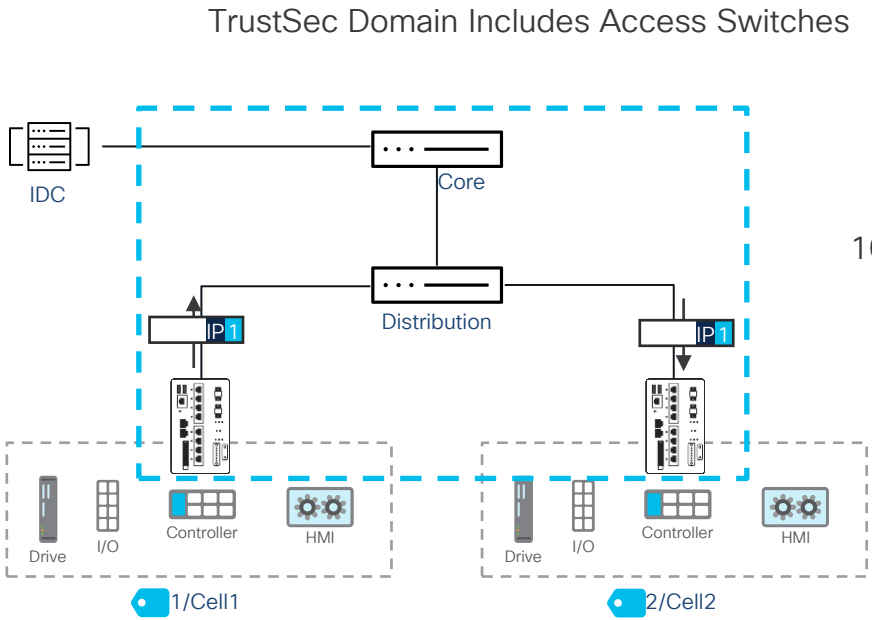


Not all switches need to be enforcement nodes to do TrustSec

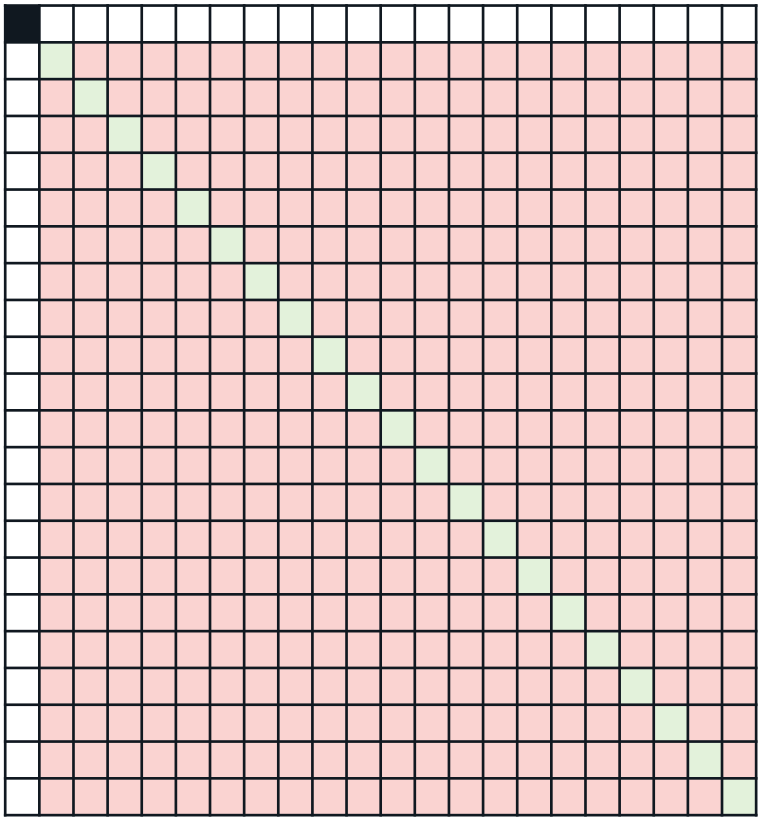
- Segmentation between cells still possible



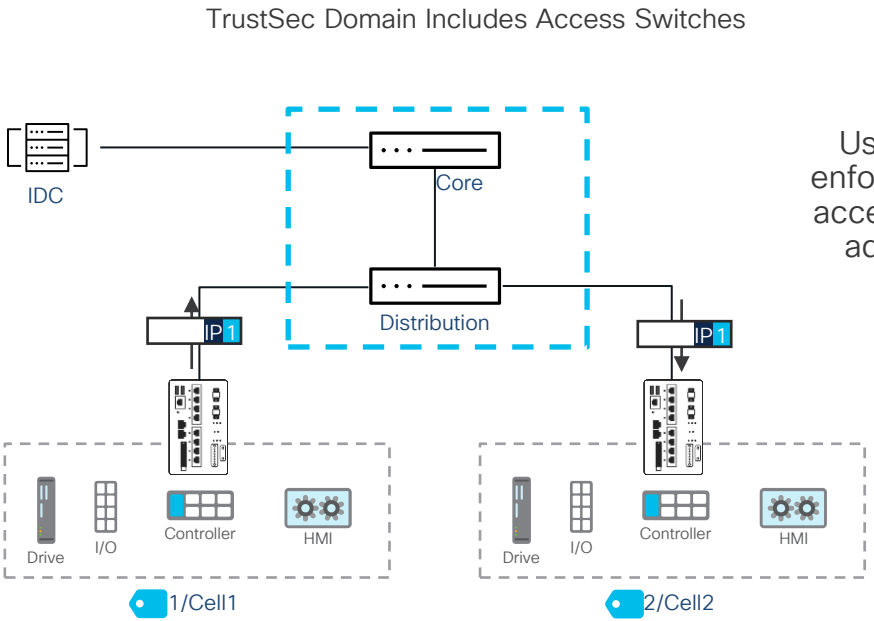
How the TrustSec domain enables you to reduce the number of policies in your network



100s of Cells



How the TrustSec domain enables you to reduce the number of policies in your network

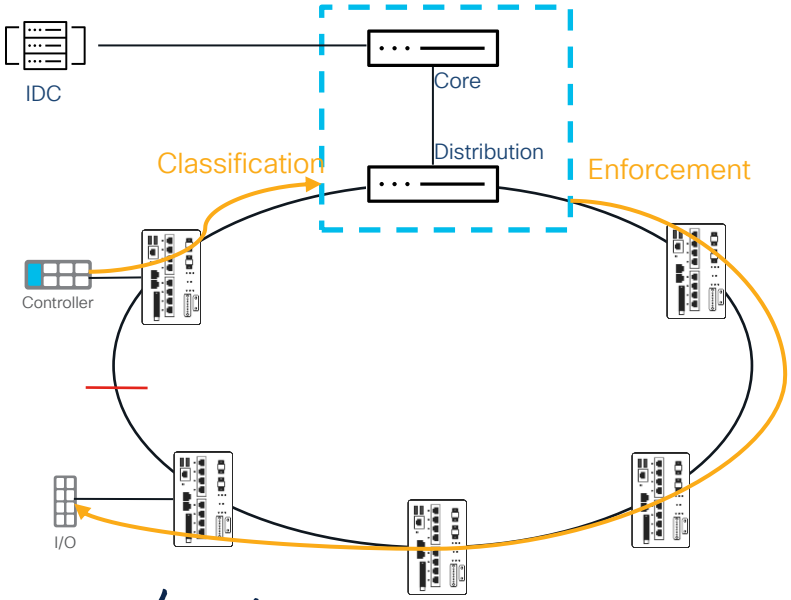


Use lack of enforcement in access to your advantage

- Every Cell/Area Zone has the same SGT
  - Deny by default
- We are only focused on the policy for traffic that leaves the zone

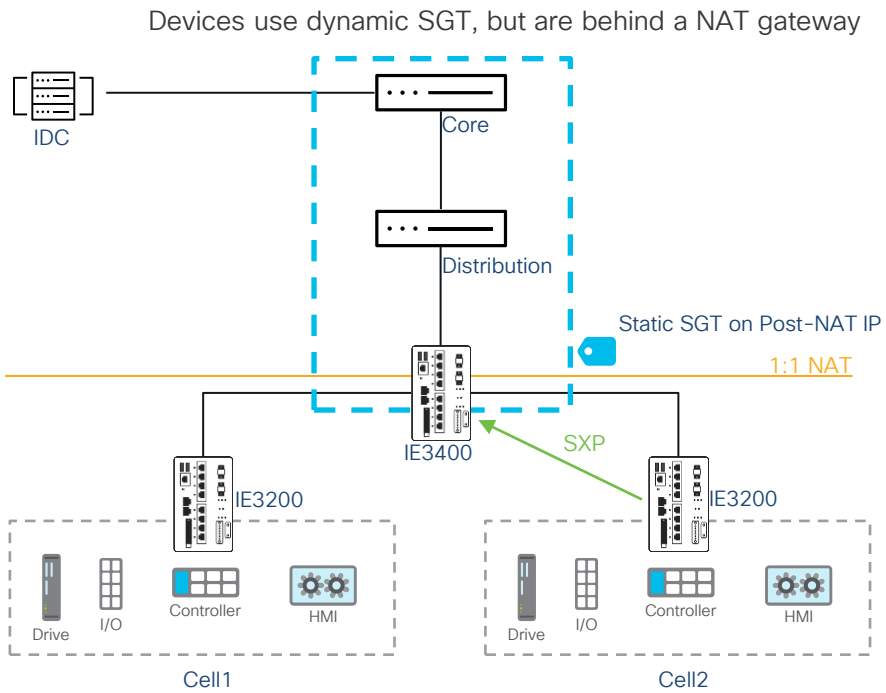
	Cell/Area Zones	Infrastructure Services
Cell/Area Zones		
Infrastructure Services		

How a ring topology effects your enforcement strategy



- In this case, aggregation of the SGT does NOT work
- TrustSec domain is part of the ring
- Each ring must have its own SGT so traffic can be permitted through

How L2NAT effects your enforcement strategy



- **Problem Statement**: IP to SGT mapping will be on private IP address. This address does not exist in the TrustSec domain
- **Solution**: L2NAT Gateway is added to TrustSec Domain
  - Static SGT on Post-NAT IP
  - Dynamic SGT is shared to L2NAT device via SXP
  - L2NAT device does inline tagging on Post-NAT IP for transporting through TrustSec Domain
  - L2NAT device understands private IP address for enforcement

Segmentation Design Principles

It is all about the use case

Classification

Group assets based on privileges

Classification may be based on endpoint location (i.e. zone), role (i.e. interlocking), dynamic authentication (i.e. user or profiling rule)

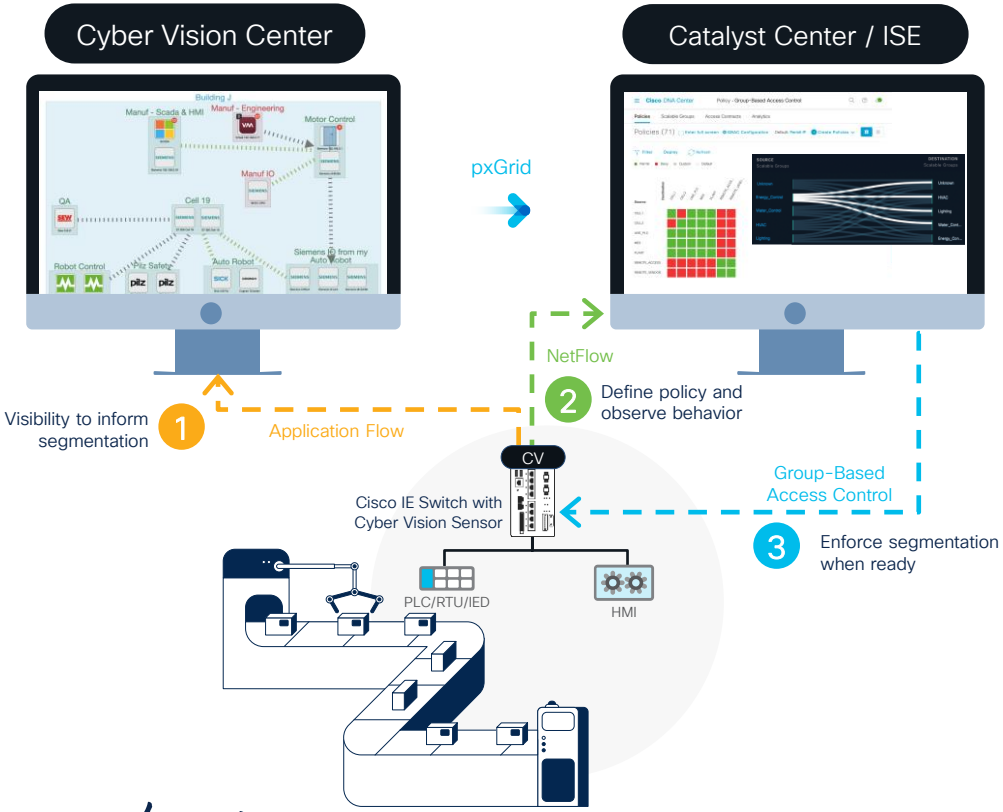
Enforcement

Segmentation needs should define enforcement points

Propagation

Remember: enforcement points needs to know source and destination tag, propagate if required

Recap: Use visibility to influence segmentation



Visualize Zones & Conduits

Group endpoints into zones to visualize aggregated flows as conduits to inform segmentation policy

Dynamic SGT Mapping

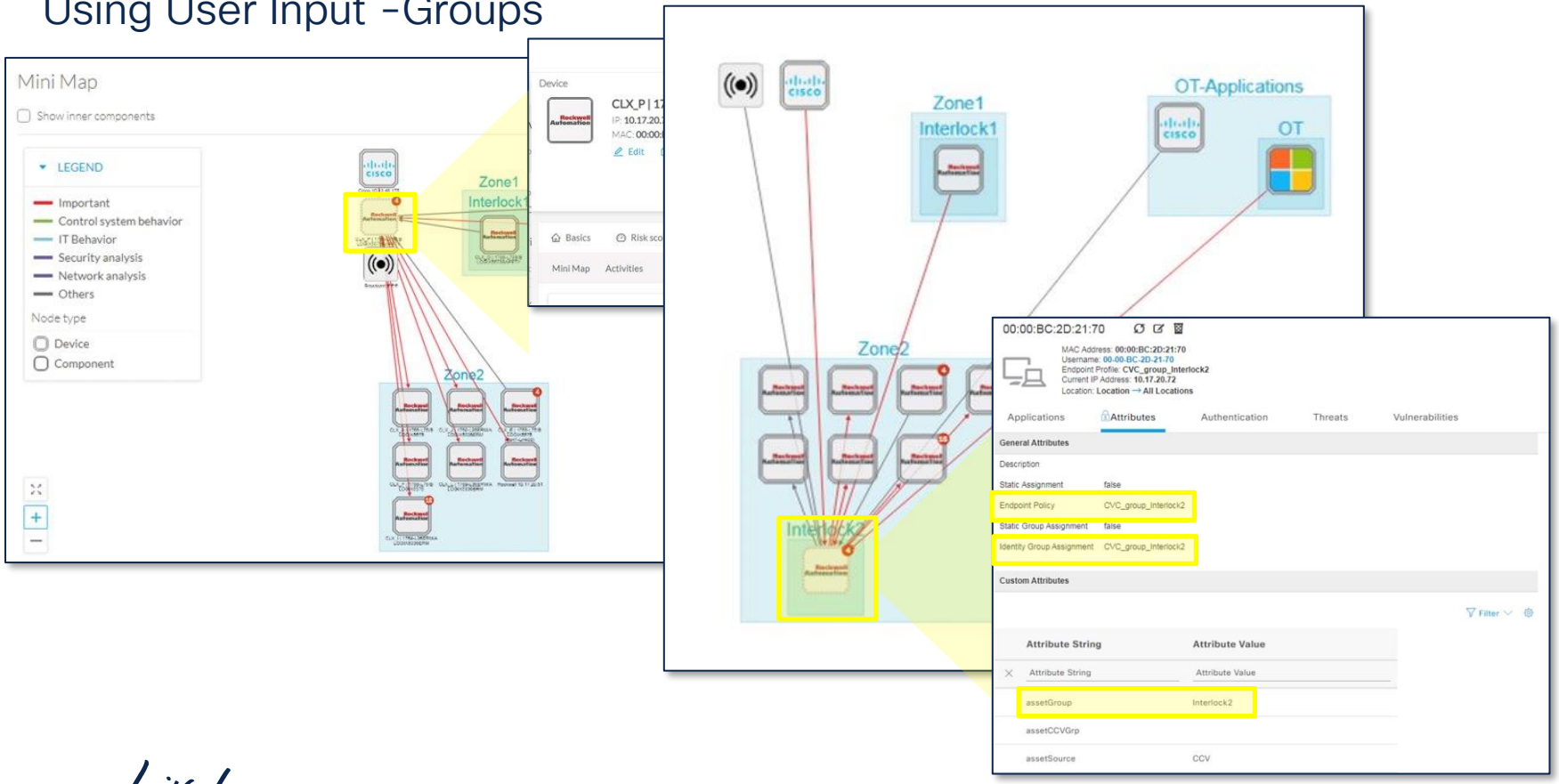
Cyber Vision grouping results in dynamic Group-based policy assignment to endpoints through ISE

Monitor Before Enforcement

Visualize Group-based network behavior in Catalyst Center and enable enforcement when confident after monitoring

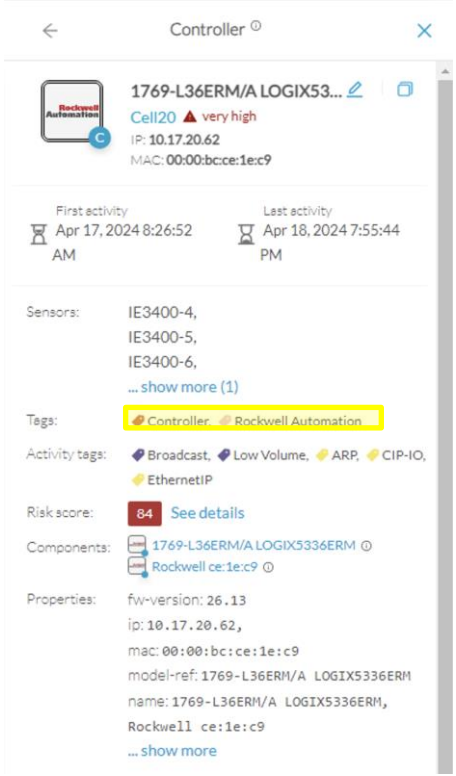
Using Cyber Vision to Initiate a CoA

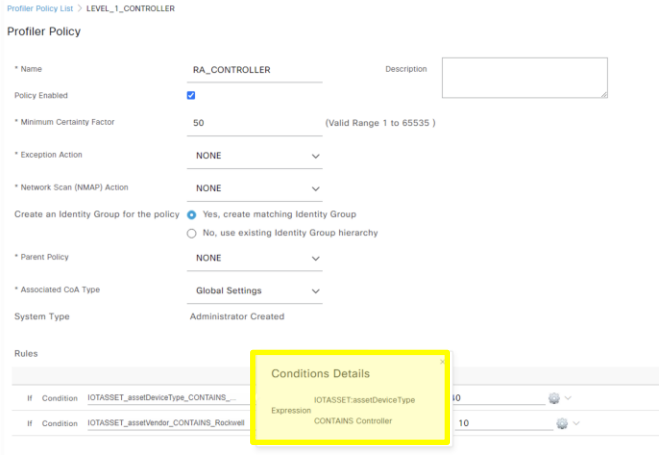
Using User Input -Groups



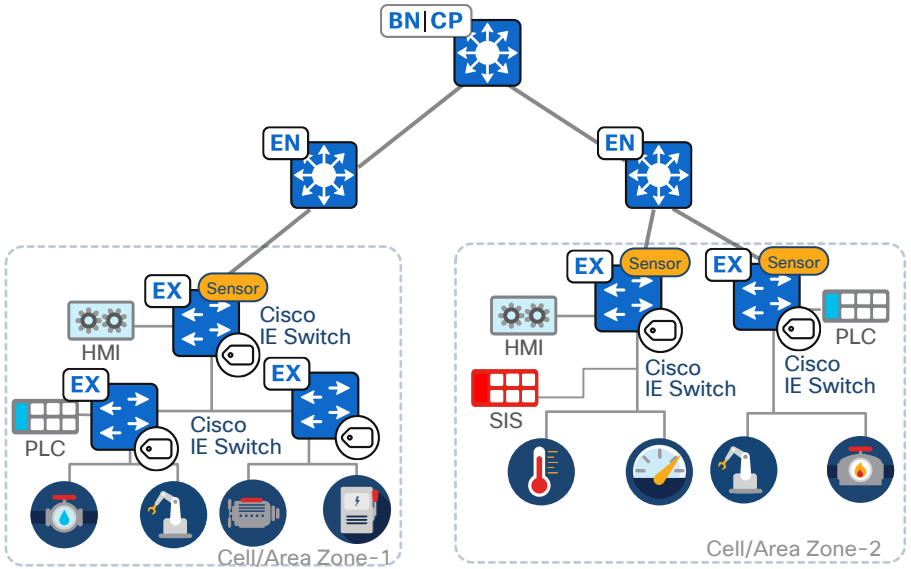
Using Cyber Vision to Initiate a CoA

Using Asset Attributes – ISE Profiling



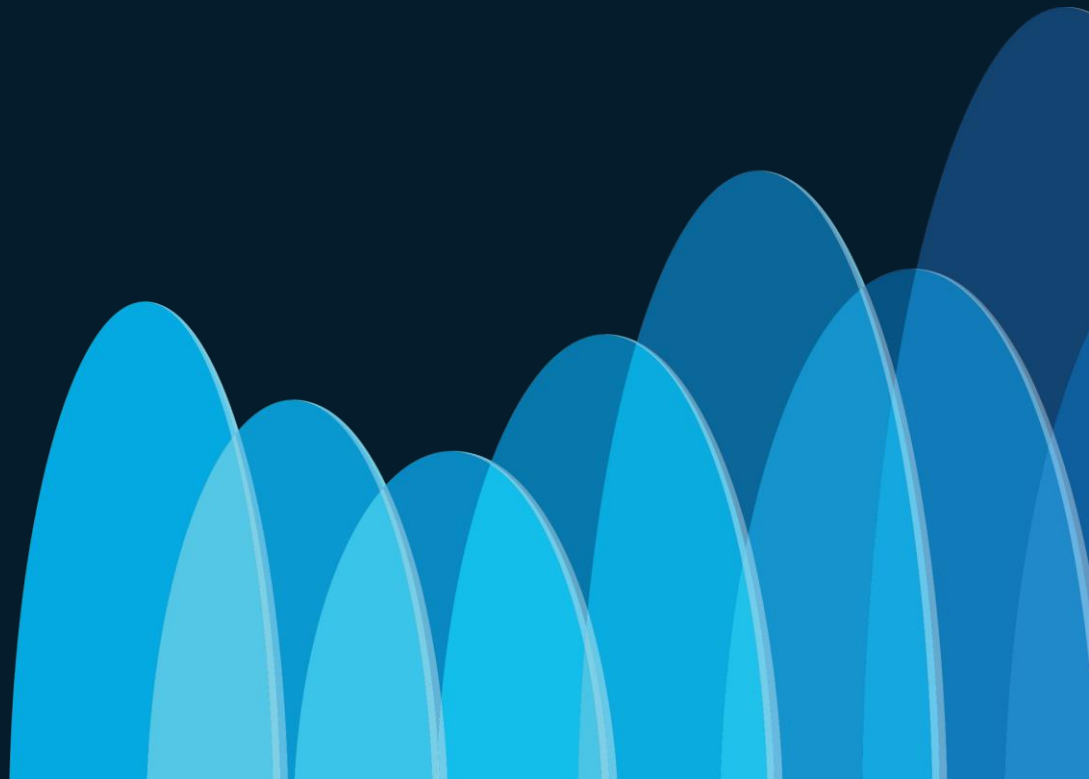


What about SDA?

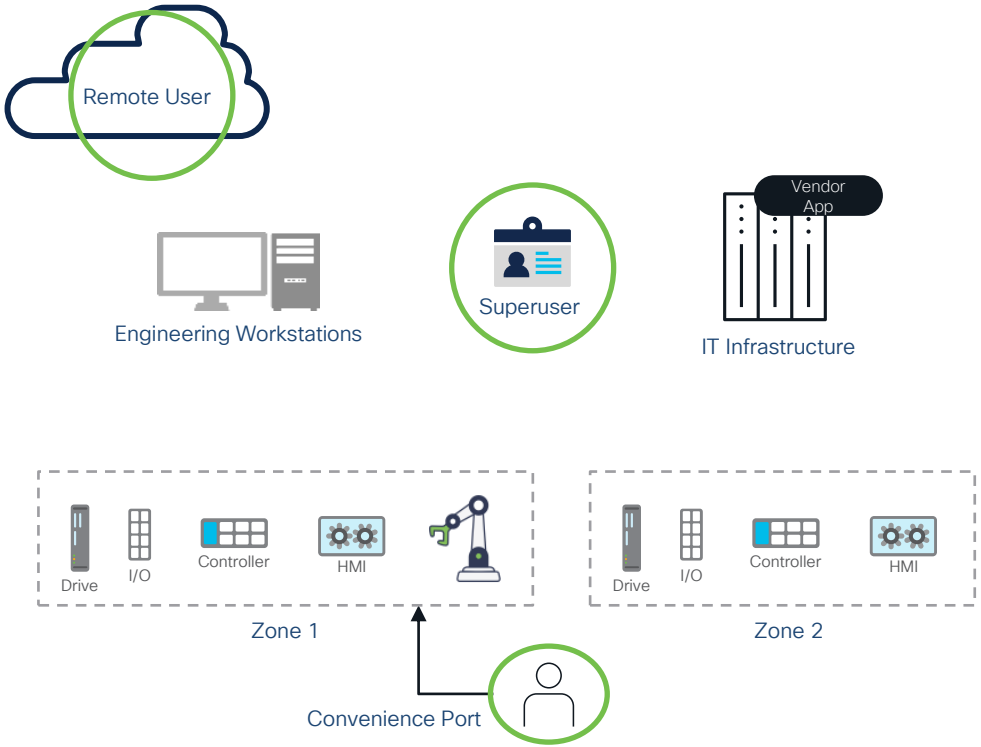


- SDA is not required to implement TrustSec
- SDA automates most TrustSec configurations
  - Enables enforcement
  - VLAN to SGT
  - Port authentication
- Design principles are the same!

Segmenting the Users

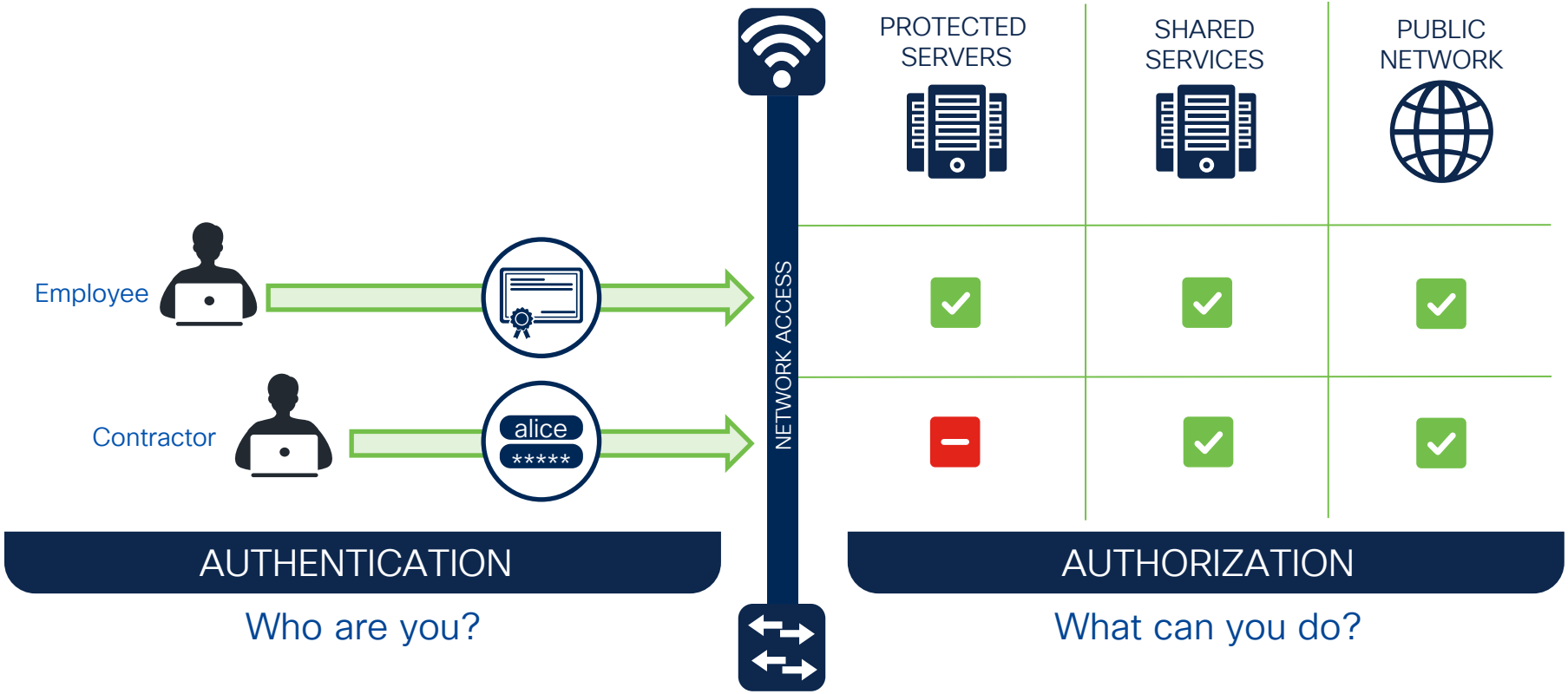


9 Use Cases for Securing Industrial Networks

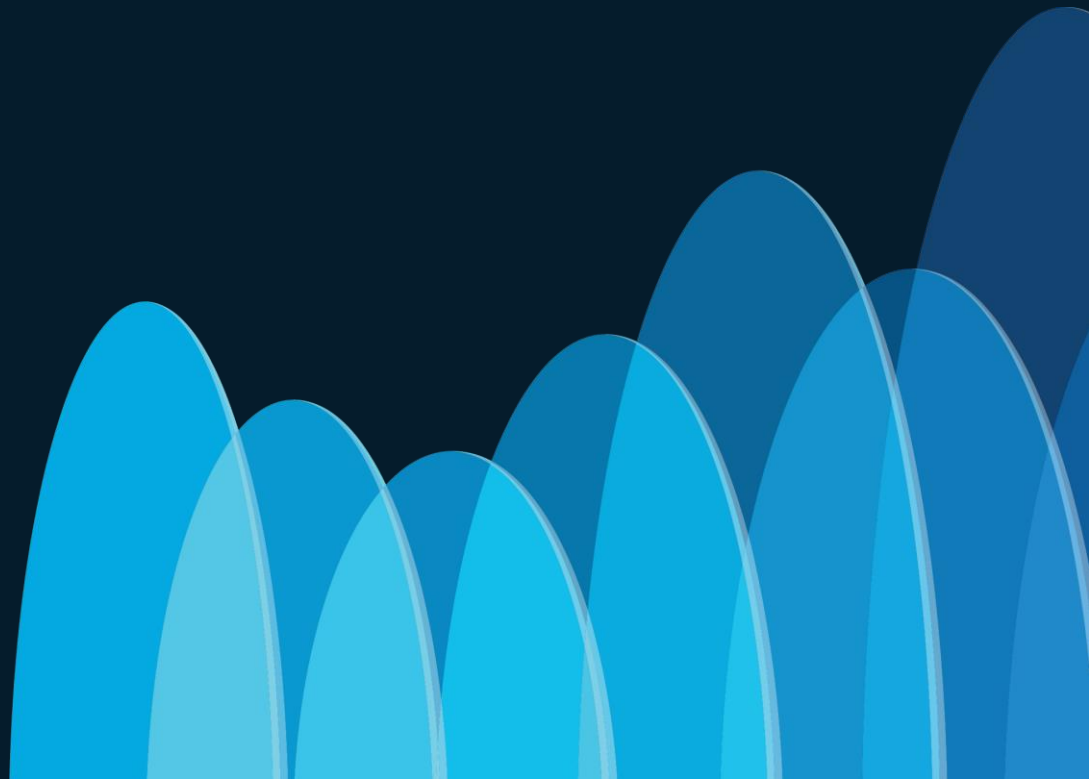


802.1X Authentication is primarily used to enable use cases associated with human interaction to the OT network

Authentication and Authorization



Remote Users are the biggest attack vector to your network



In a hybrid, multi-vendor, multi-vector universe

Risk from External Threats

83%

of breaches involved External actors

Social Engineering is on the rise

74%

of breaches include the human element

Credentials are still an issue

49%

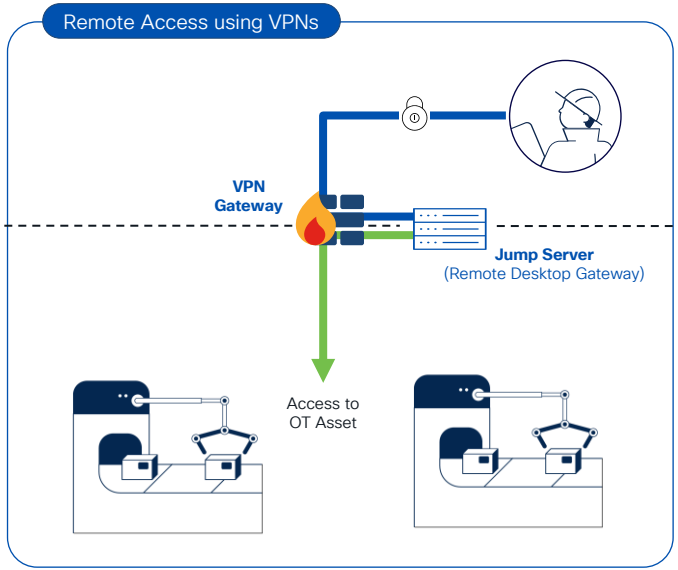
of breaches involved credentials

The risk of Vulnerabilities

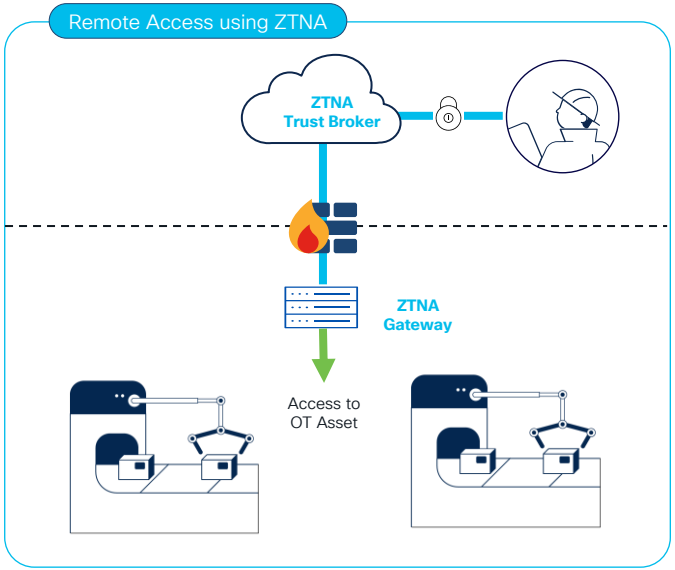
5%

of attacks exploit vulnerabilities to access an organization

Evolving from VPNs to ZTNA

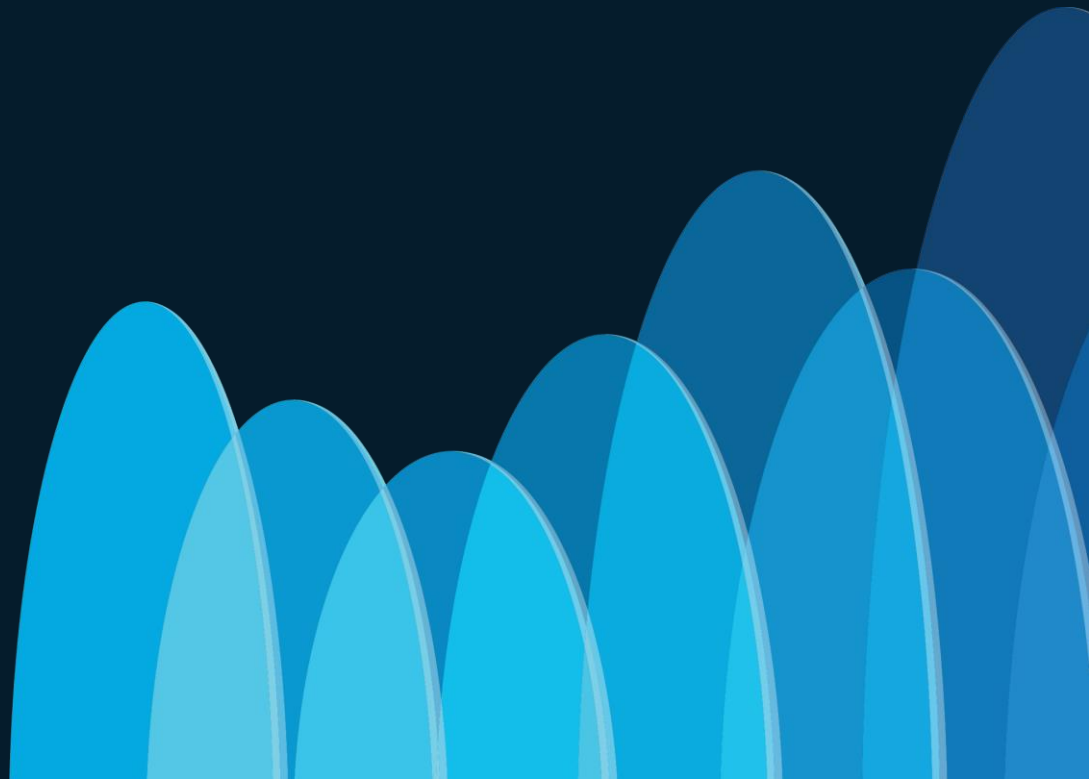


- Always-on solutions with all-or-nothing access
- Firewall rules need to be frequently updated
- Manual session management using jump servers

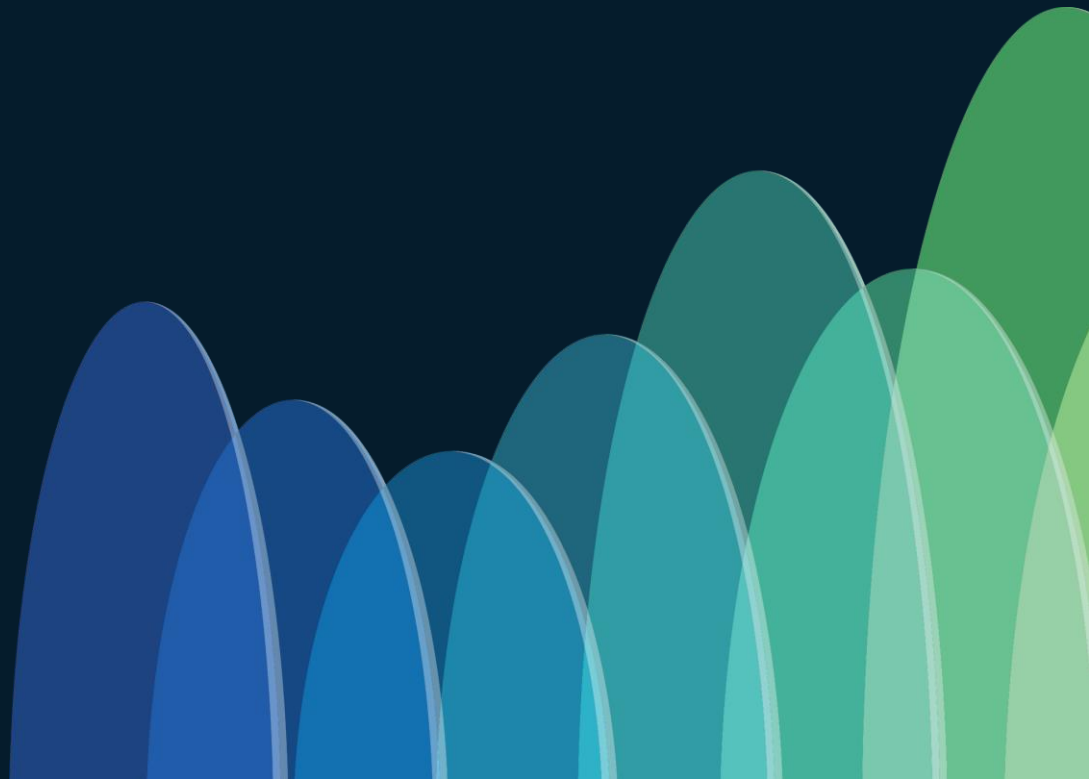


- Trust broker manages policy based on identity and context, and grants access to specific resources at specific times
- Gateway establishes an outbound connection to the trust broker eliminating complexity of firewall rules

Go to our Walk In Lab and try it!

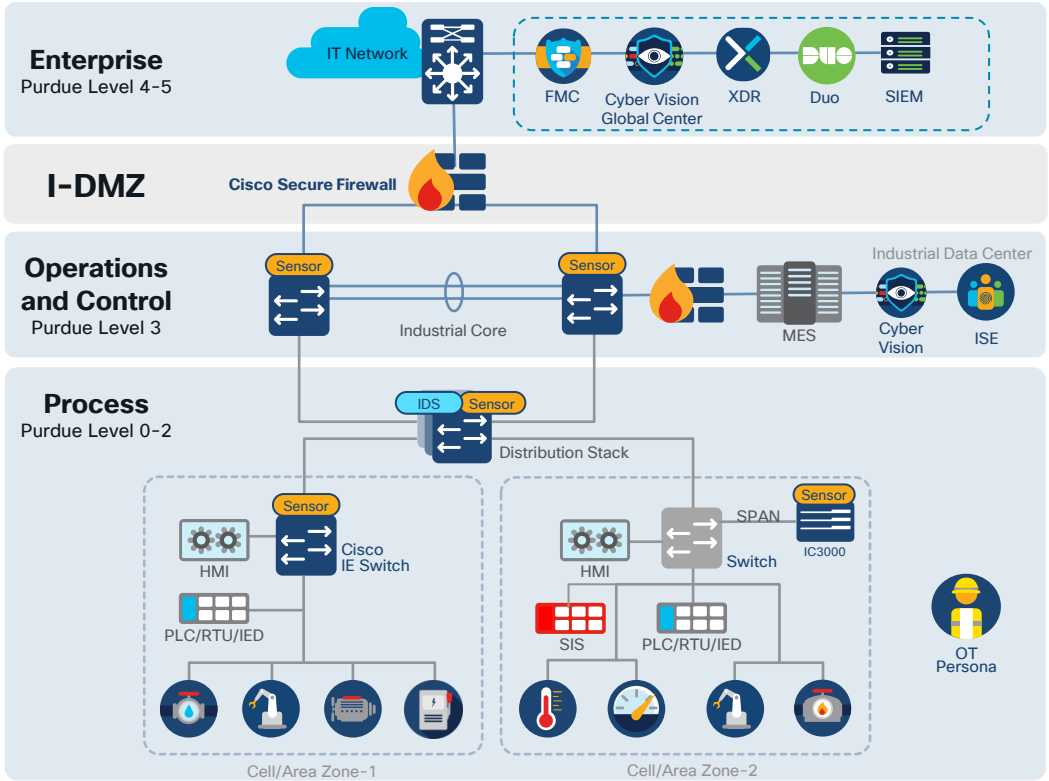


Pulling it all together



cisco Live!

Let’s put everything together

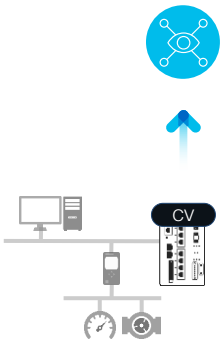


1. CyberVision discovers industrial assets and communications and groups it into Zones.
2. ISE implemented for visibility and CyberVision context is shared with ISE.
3. Components are dynamically classified in SGTs via group assignment directly from CyberVision
4. Visualize traffic activity between SGT in Catalyst Center policy analytics
5. Deploy segmentation with confidence once you are comfortable with the observed network behavior
6. CyberVision, Secure Network Analytics or other analytics tools raise alarms endpoint behavior anomalies and threat detection.
7. Investigate in Splunk and SOC tools
8. Users can trigger quarantine of offending asset.

Cisco Industrial Threat Defense

Asset Visibility & Security Posture

Cisco Cyber Vision

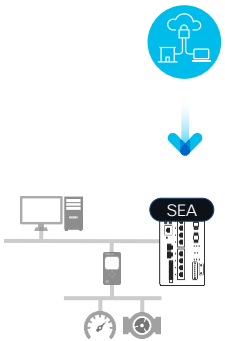


Network embedded CV Sensor

Zero Trust for OT

Zero Trust Network Access

Cisco Secure Equipment Access

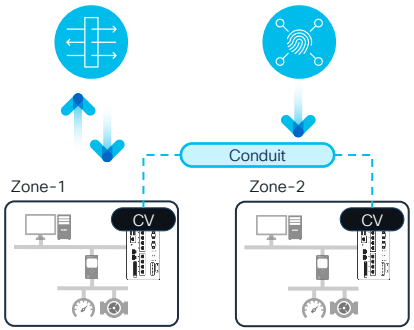


Network embedded ZTNA Gateway

IEC 62443 Zones & Conduits

Cisco Secure Firewall

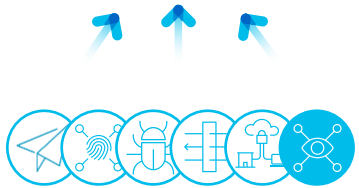
Cisco ISE



Network enforced segmentation

Cross-Domain Detection, Investigation & Response

splunk> a CISCO company



Visibility across the entire attack chain

Network as a fabric to secure OT at scale

Webex App

Questions?

Use the Webex app to chat with the speaker after the session

How

1. Find this session in the Cisco Events mobile app
2. Click “Join the Discussion”
3. Install the Webex app or go directly to the Webex space
4. Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until February 28, 2025.

Fill Out Your Session Surveys

Participants who fill out a minimum of 4 session surveys and the overall event survey will get a unique Cisco Live t-shirt.

(from 11:30 on Thursday, while supplies last)

All surveys can be taken in the Cisco Events mobile app or by logging in to the Session Catalog and clicking the ‘Participant Dashboard’

Content Catalog

Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at ciscolive.com/on-demand. Sessions from this event will be available from March 3.

Contact me at:

Contact Erika: www.linkedin.com/in/erikafranco

Contact Andrew: www.linkedin.com/in/andrew-mcphee-cisco

Take Action and Learn More

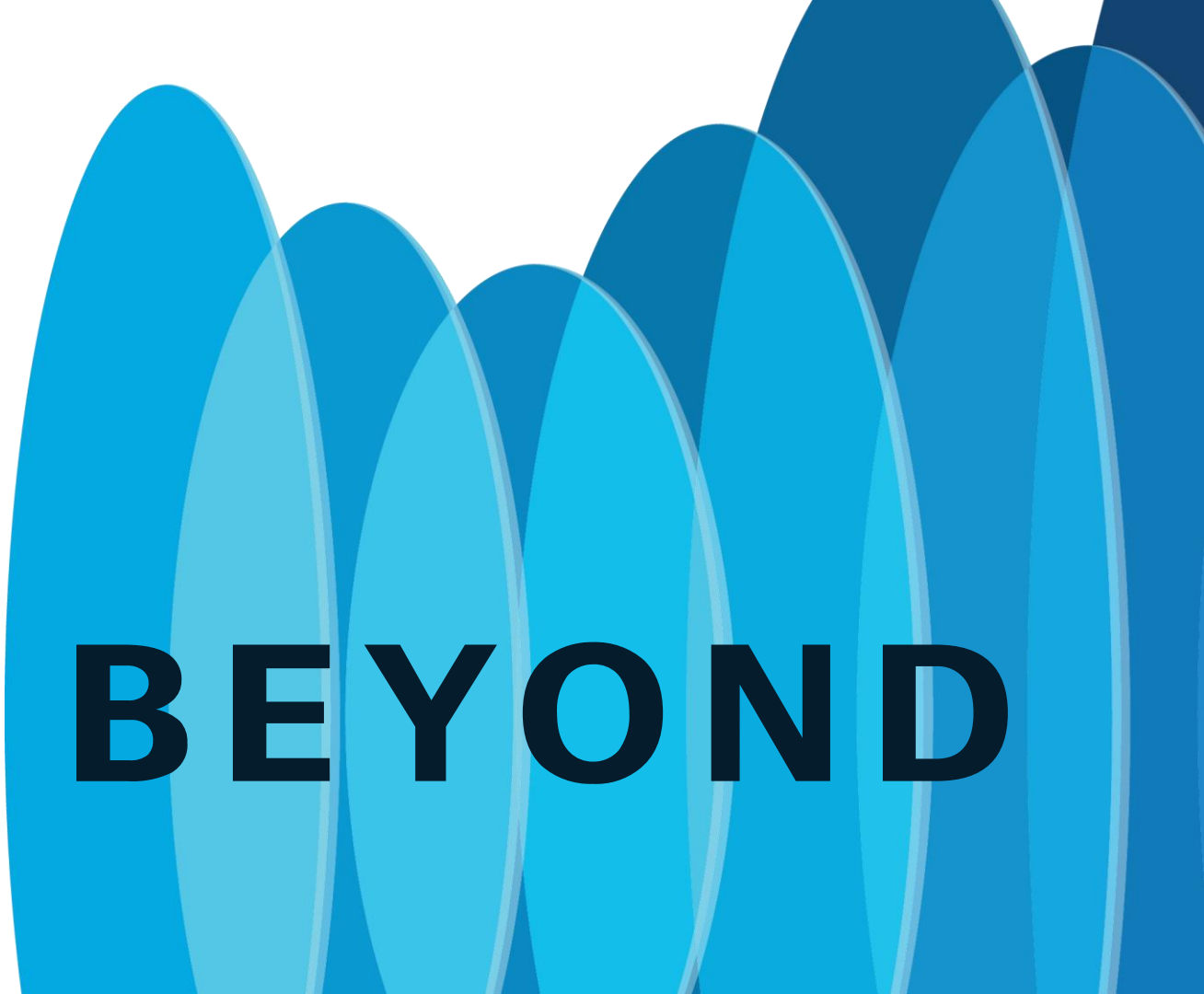
Visit us in the World of Solutions
Get a private demo

Contact us
cs.co/contactIOT

Get all the details on Cisco OT security
cisco.com/go/IoTsecurity


cisco
Thank you
cisco Live!

cisco Live!



GO BEYOND