

The Cisco Live! logo features the word "CISCO" in a dark blue, sans-serif font, followed by "Live!" in a dark blue, cursive script font.

CISCO *Live!*

The text "Let's go" is displayed in a dark blue, sans-serif font. The background behind the text is a vibrant, multi-colored geometric pattern of overlapping triangles and lines, transitioning from dark blue on the left to bright yellow and white in the center, and then to various shades of blue and green on the right.

Let's go



The bridge to possible

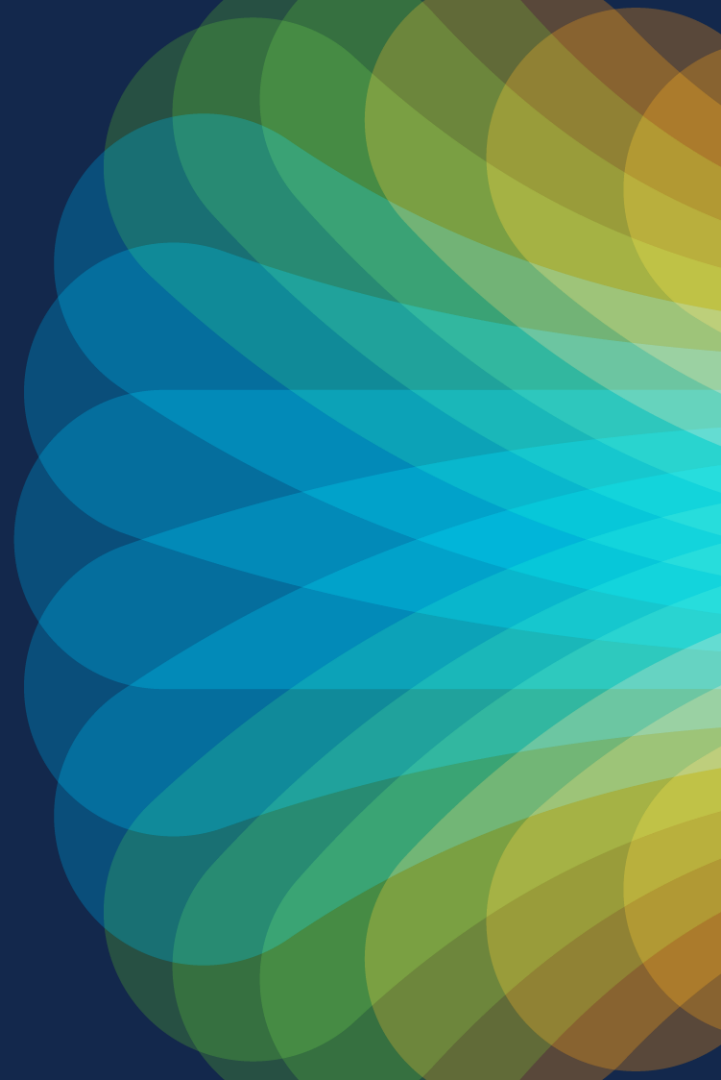
Implementing Segmentation in Industrial Networks

Andrew McPhee, Industrial Security Solutions Manager

CISCO *Live!*

BRKIOT-2882

Security can –
and should be –
simple!



Agenda

- What do we mean by Industrial Security?
- ISA/IEC 62443 Zones & Conduits Model
- Identifying the Assets
- Implementing the Zones & Conduits Model
- Remote Users
- Q&A

What do we mean by Industrial Security?



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

Notable OT Cyber Incidents in Recent Years

Colonial Pipeline

- Stolen Credentials for remote access
- \$200M over 5 years invested in IT + Security
- Single password with no MFA bypassed all of it

Industroyer2

- Failed attempt to takedown Ukraine energy grid
- Evolution of the malware that was successful in 2016
- Attack was stopped by cybersecurity implementation

JBS Foods

- Recon in Feb, Attack in June
- Leaked Credentials of JBS employees found
- \$11M ransom paid

COSMICENERGY Malware

- Similar to Industroyer2
- Designed to cause electric power disruptions by interacting with IEC-104 devices

PowerDrop Malware

- Targets the U.S aerospace industry
- Uses PowerShell and WMI to create a persistent remote access trojan
- Reaches back to C2 server to progress attack

2021

2022

2023

JBS Foods

- Recon in Feb, Attack in June
- Leaked Credentials of JBS employees found
- \$11M ransom paid

Kojima Industries & Toyota

- Supply Chain Attack
- 14 Factories shut down
- Malicious file found on File Server

Danish Rail Systems

- Sub-contractor IT network compromised
- Drivers could not operate locomotives for several hours

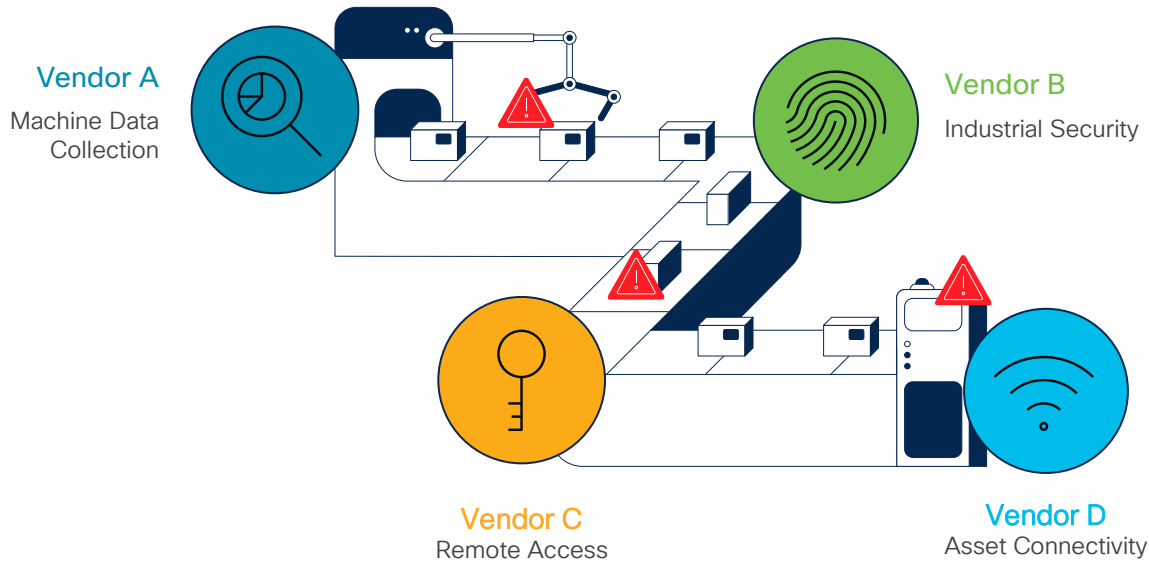
ABB

- Targeted Windows Active Directory
- ABB terminated all VPN connections to block attacker access

Lacroix

- Ransomware forced shutdown of 3 plants for a week

The market is fragmented by a patchwork of solutions from different vendors



Shadow IT & Security Risk

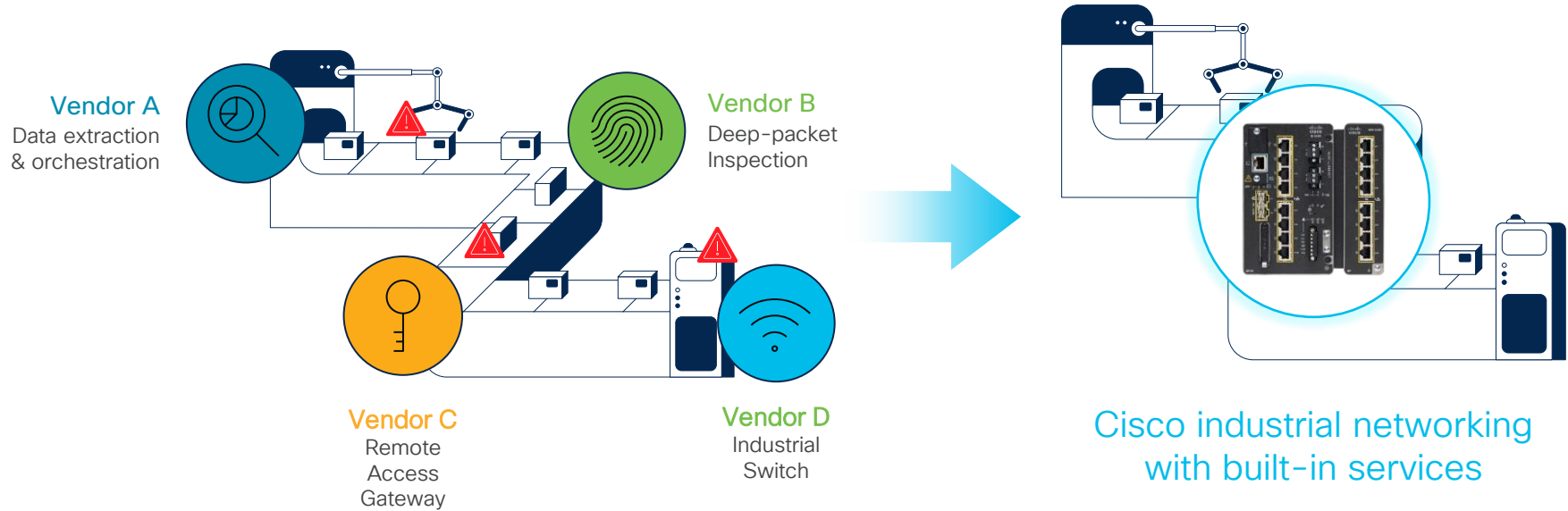


Complexity



Hard to Scale

Cisco is on a journey to help customers replace point hardware solutions

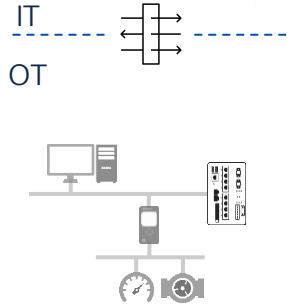


Eliminating complexity by converging functionality as software features on our industrial networking portfolio

Building a Security Foundation with Cisco

Build a Security Foundation

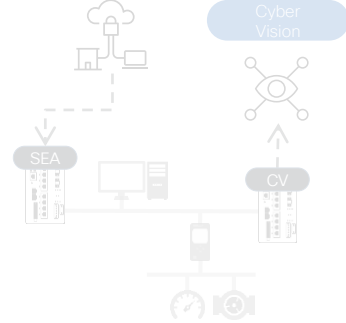
Cisco Industrial Networking



Security Posture & ZTNA of OT Assets

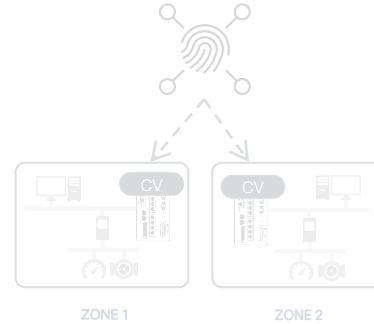
Secure Equipment Access

Cyber Vision



Segment Network into Smaller Trust Zones

Identity Services Engine



Develop Incident Investigation & Response

Cisco XDR



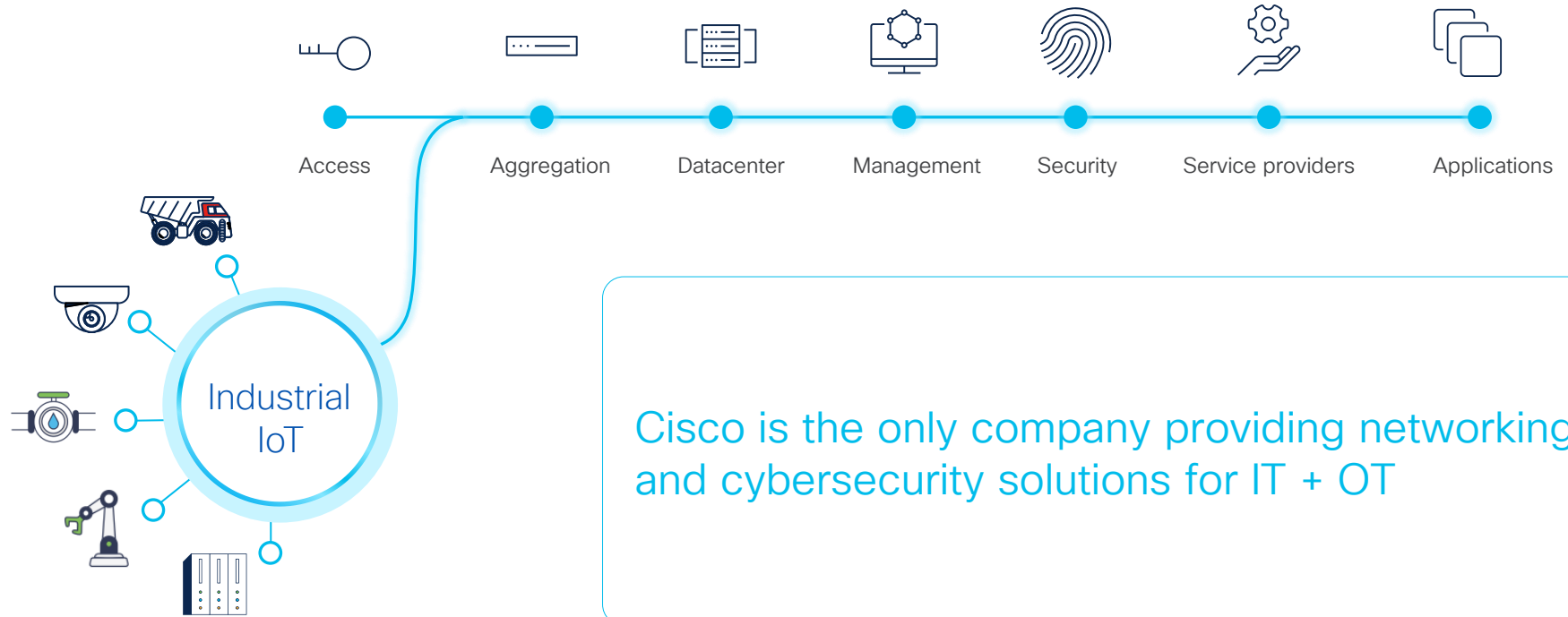
Talos Threat Intelligence

+



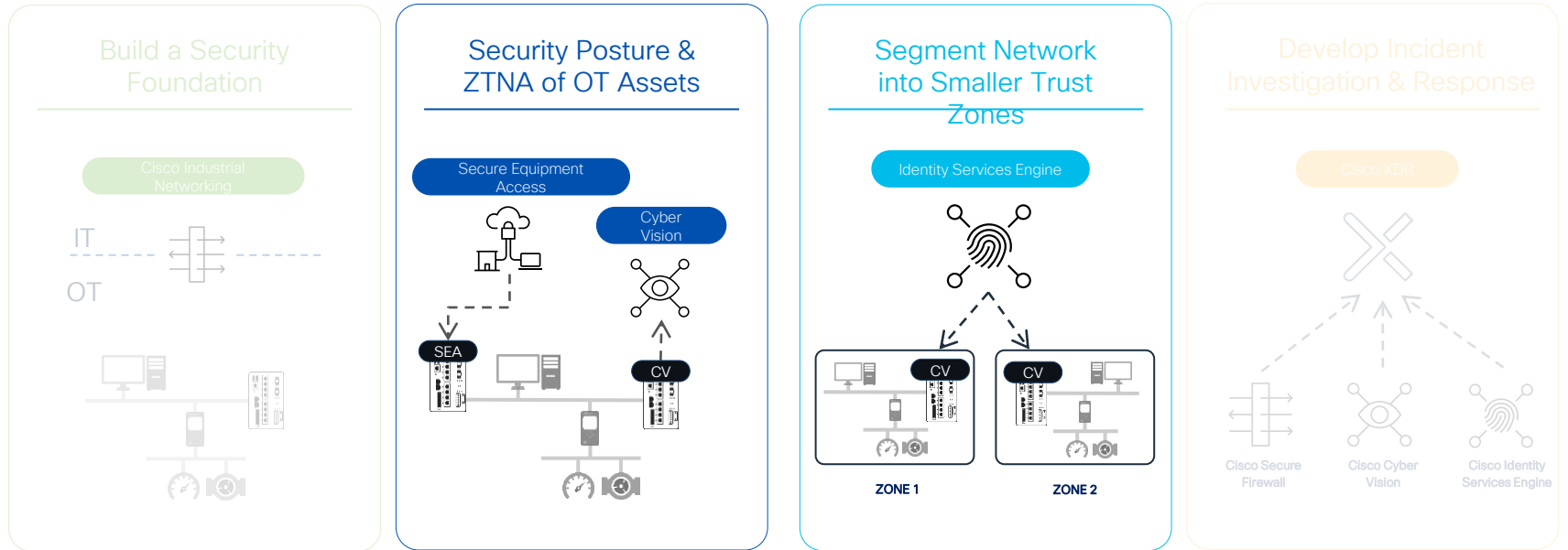
Talos Incident Response

Only Cisco can provide solutions to secure and connect businesses end-to-end



Cisco is the only company providing networking and cybersecurity solutions for IT + OT

Focus on Today's Session – Segmentation within OT



Talos Threat Intelligence

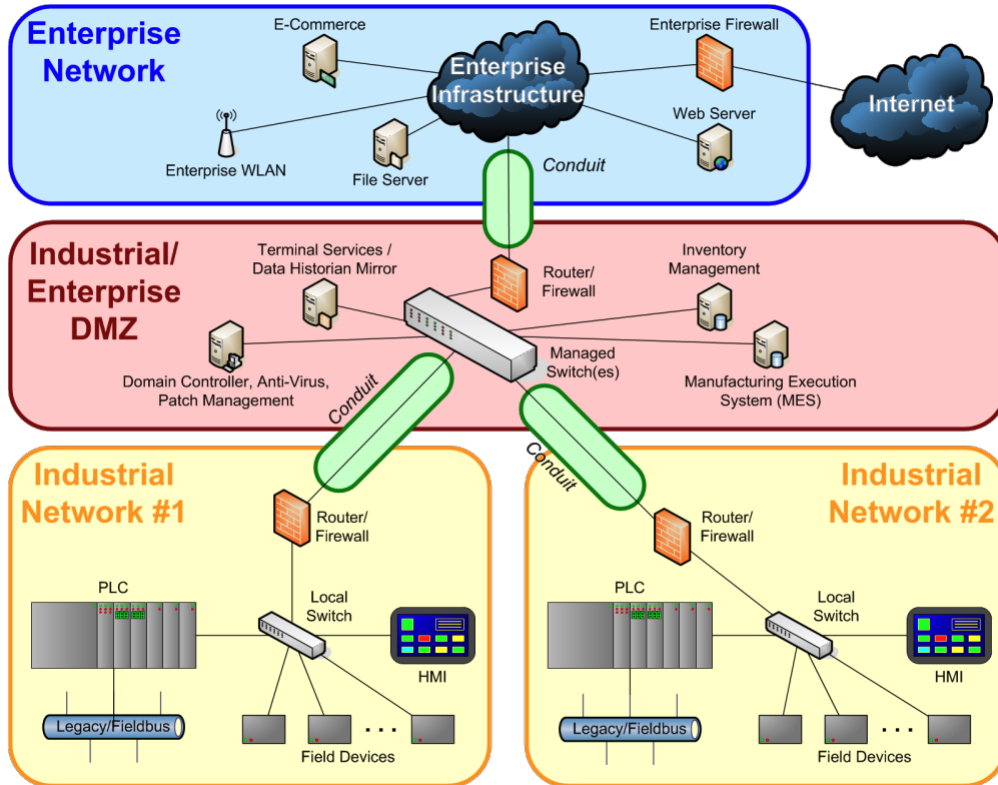
+



Talos Incident Response

ISA/IEC 62443 Zones & Conduits Model

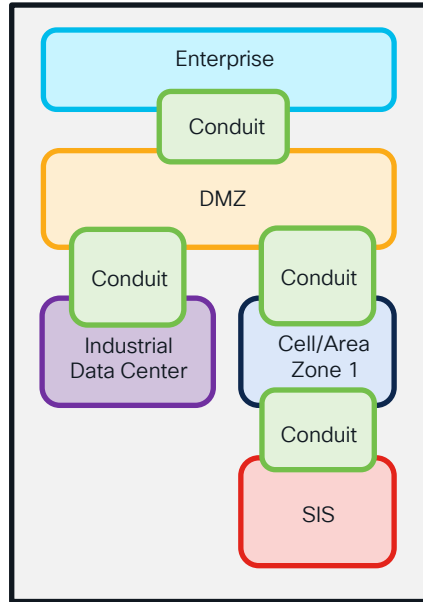
IEC 62443 Zones & Conduits



- **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

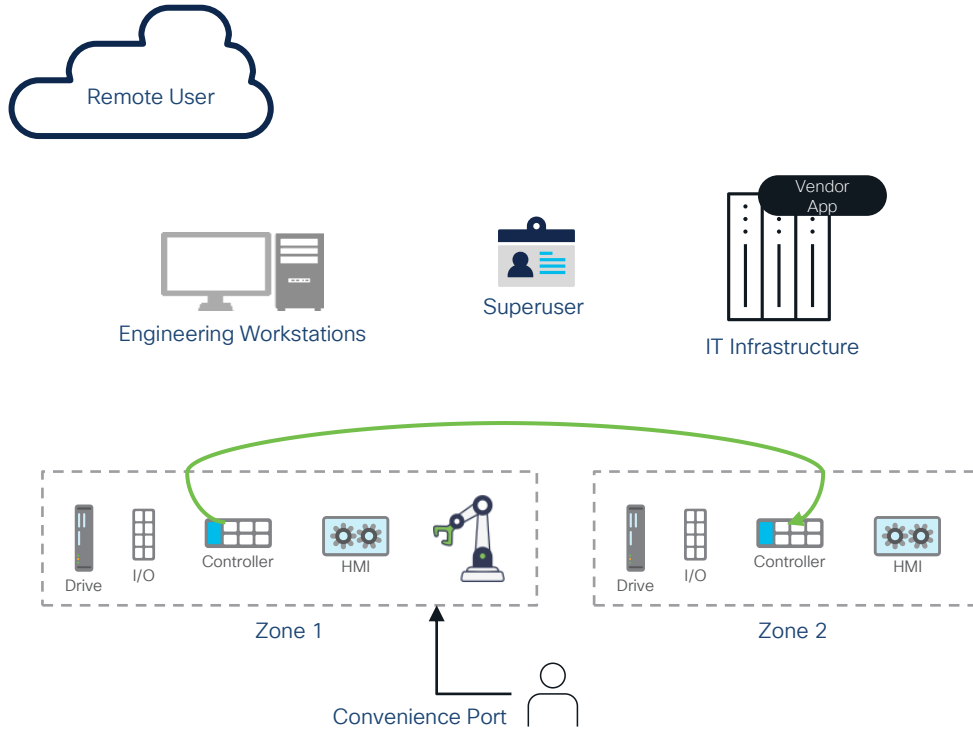
3.1.2 ZTA Using Micro-Segmentation

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.

9 Use Cases for Securing Industrial Networks

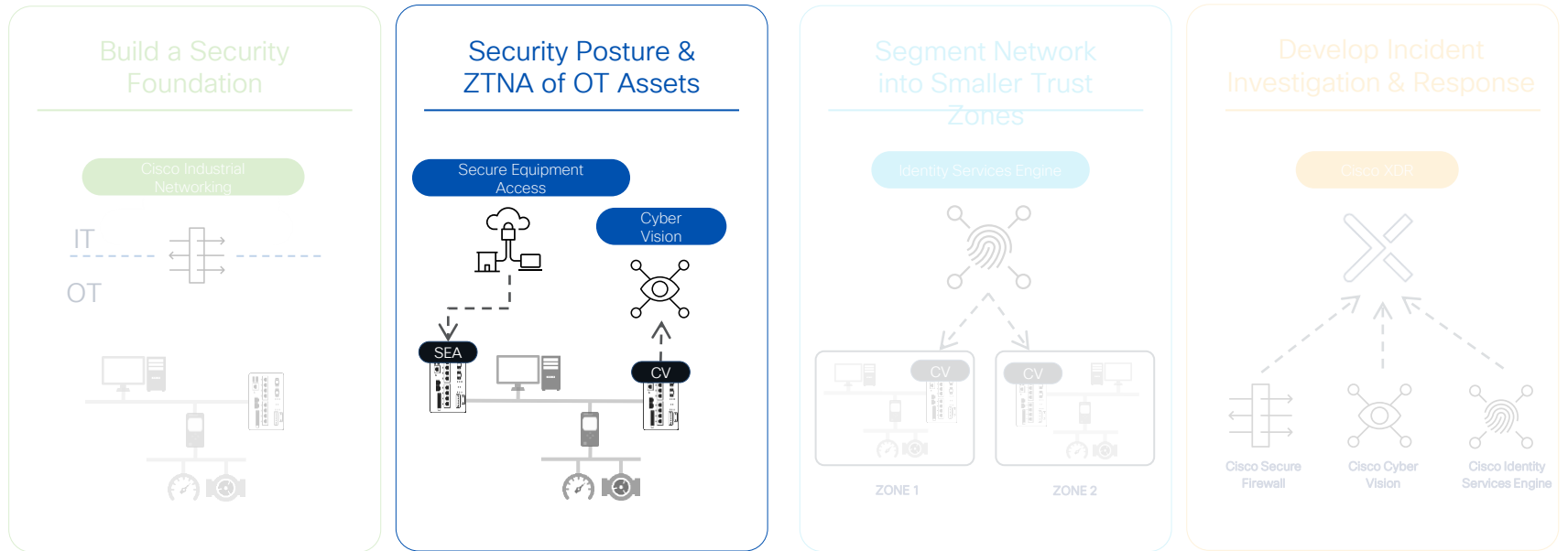


1. All devices within a zone can communicate freely
2. Deny by default across zone
3. Convenience Port within a zone
4. Engineering workstations to all devices within designated zones
5. Superusers – named employees to all devices
6. IT applications have restricted access to all zones
7. Vendor applications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

Identifying the Assets



Asset Visibility & Device Posture using the Network as a Sensor



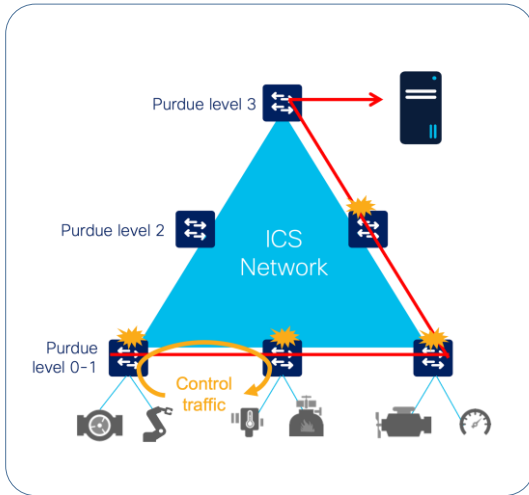
Talos Threat Intelligence


+

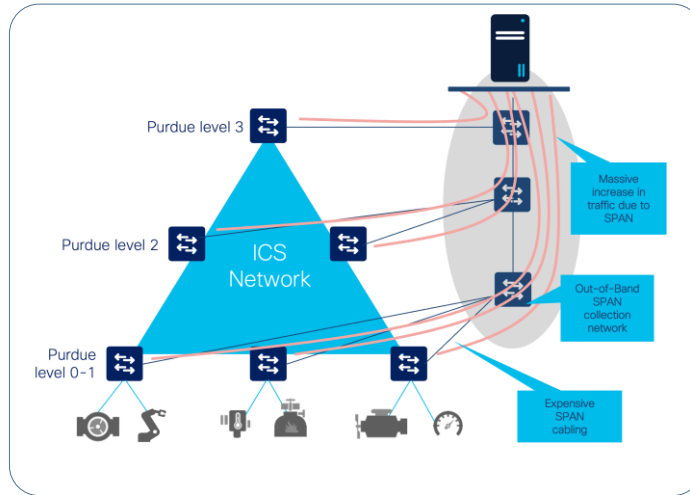



Talos Incident Response

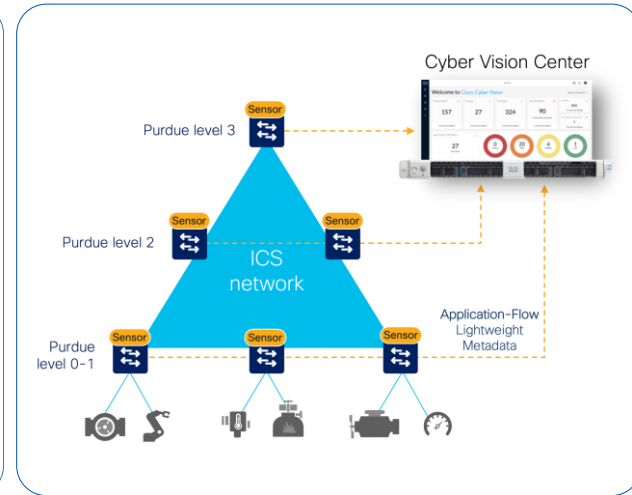
Leverage the network as a sensor to lower cost and complexity




 RSPAN introduces Jitter



 Out-of-Band SPAN is expensive

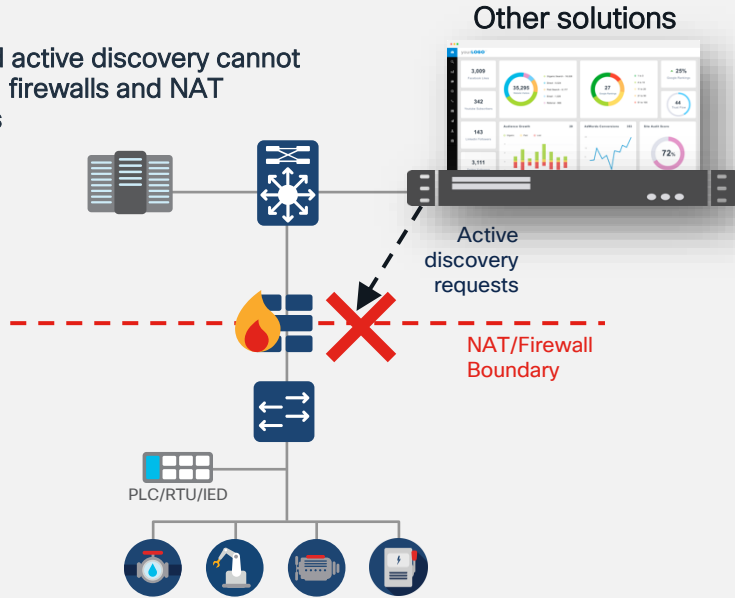


 Network sensors scale without SPAN

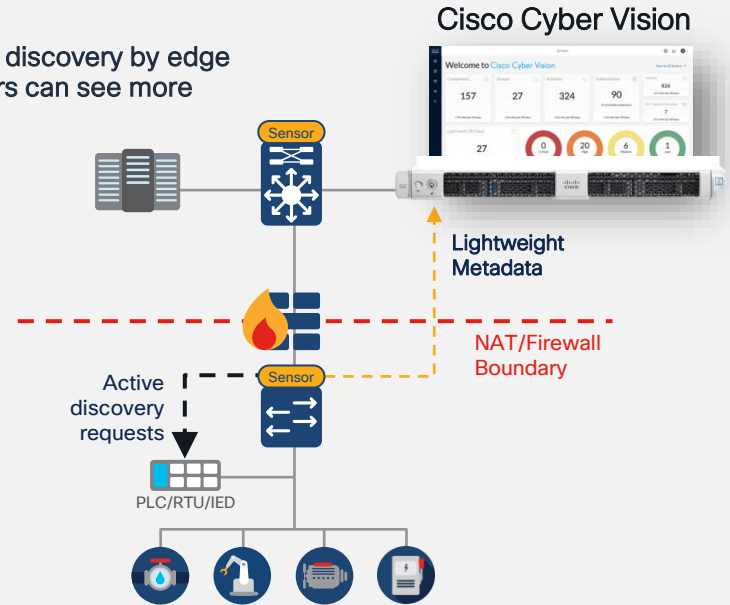
Why is a network-sensor important?

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



Cisco Cyber Vision portfolio

Cyber Vision Center

Hardware Appliance

UCS based servers with Hardware RAID



CV-CNTR-M5S5

- 16 core CPU
- 64 GB RAM
- 800GB drives

CV-CNTR-M5S3

- 10 core CPU
- 32 GB RAM
- 480GB drives

Software Appliance

Virtual Machines



VMWare ESXi OVA



HyperV VHD

Minimum requirements

- Intel Xeon, 10 cores
- 32GB RAM and 1TB SSD
- 1 or 2 network interfaces



Amazon Web Services



Microsoft Azure

Minimum requirements

- Intel Xeon, 10 cores
- 32GB RAM and 1TB SSD
- 1 or 2 network interfaces

Cyber Vision Sensors



Catalyst IE3300 and IE3400 Switches



Catalyst IE3400HD IP67 Switch



Catalyst IR1101 LTE/5G Gateway



Catalyst IR8300 Multiservice Router



Catalyst IE9300 Rugged Aggregation Switches



Network-Sensors

Deep Packet Inspection built into network-elements eliminating the need for SPAN



IC3000 Industrial Compute

Hardware-Sensor

DPI via SPAN to support brownfield



Asset Inventory

Comprehensive up to date inventory of all assets in your environment



Communication Patterns

Dynamic communication map with detailed application flow level information

Asset Visibility

The screenshot displays two main views from the Cisco Cyber Vision interface:

- Asset Inventory:** Shows details for a component named "1769-L16ER/B LOGIXS 316ER" from Rockwell Automation. It includes activity logs (e.g., "First activity Apr 14, 2021 11:45:12 AM"), tags (e.g., "Controller", "Rockwell Automation"), and activity tags (e.g., "Stop CPU", "Diagnostics"). A sidebar on the right shows counts for Flows (14), Events (9), Vulnerabilities (10), and Credentials.
- Communication Map:** A network diagram titled "Minimap" showing connections between various assets. A legend indicates categories like "Important" (red), "Control system behavior" (green), "IT Behavior" (blue), "Network analysis" (purple), and "Others" (grey). Key assets include "STATION-WINCC", "SIEMENS IM151-3PN", "SIEMENS ef 65 8d", "SIEMENS SENTRYO-XP-1", "Siemens 192.168.0.10", "SIMATIC 300(1)", "SENTRYO-SIMATI(Profinet DCP Multicast 0.0.0)", and "10.45.1.255". Labels above the map identify "Machines - To Investigate", "Manuf IO", and "Manuf - Scada & HMI".



Vulnerability Detection

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



Risk Scoring

Asset risk scoring based on impact and likelihood to help you improve compliance

Security Posture

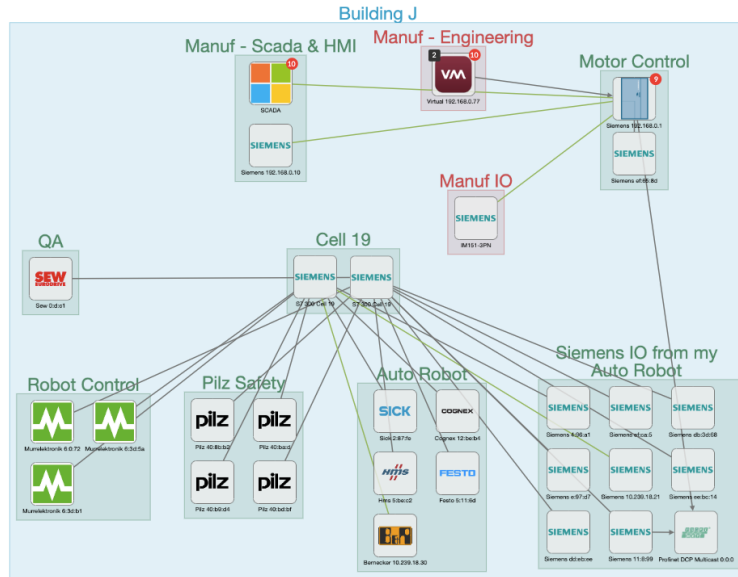
The screenshot displays the Cisco Cyber Vision Security Posture dashboard. The top section, titled "Vulnerability Detection", shows 73 vulnerabilities for the 192.168.1 subnet. A donut chart indicates the distribution of vulnerability severity levels: NONE (green), LOW (yellow), and HIGH (red). A list of 10 most matched vulnerabilities is provided, including CVE-2015-5627, CVE-2014-0781, CVE-2020-5609, CVE-2014-3888, CVE-2019-10936, CVE-2017-12743, CVE-2017-12741, CVE-2018-16156, and CVE-2019-13940. A summary indicates 9 total vulnerable components for the 192.168.1 subnet.

The bottom section, titled "Risk Scores", provides a detailed view for device SC50102. The device is identified as a Building 1C Controller (IP: 192.168.1.4) with a very high risk score of 69. A bar chart compares the current risk score (69) to the achievable risk score (44). The dashboard also shows 7 tags, 40 activities, 15 vulnerabilities, and 15 vulnerabilities for this device. A table of criteria and their matching scores is shown below:

Criteria	Matching	Distribution	Description
Device type	SC50102 type: Controller	13%	CC key element. Compromise could lead to large impact
Group impact	SC50102 group: Building 1C. It has an industrial impact. very high.	51%	
Activities	No matching activity	0%	
Vulnerabilities	SC50102 most impacting vulnerability is Path Traversal Vulnerability in Yokogawa CENTUM	36%	Path Traversal Vulnerability in Yokogawa CENTUM CVE-2020-5609 CVSS score: 9.8 Successful exploitation of these vulnerabilities could allow a remote unauthenticated attacker to see... See details

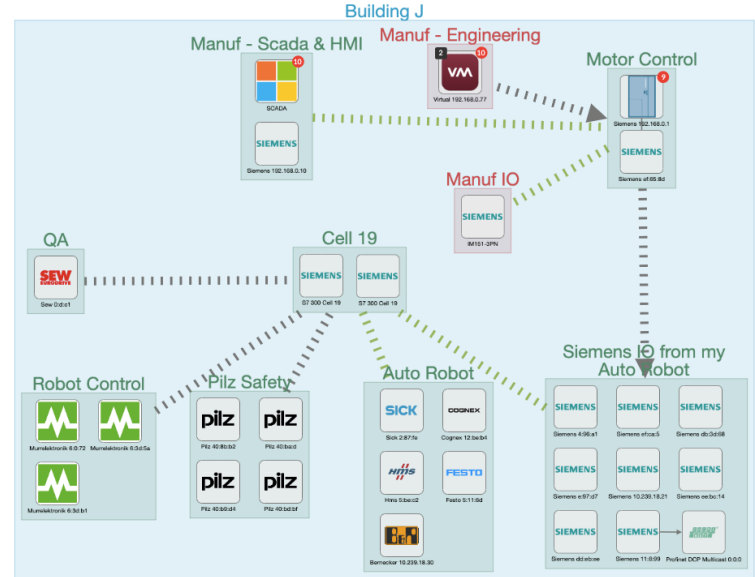
Aggregated activities match IEC62443 conduits

Unaggregated



[View all asset relationships](#)

Aggregated

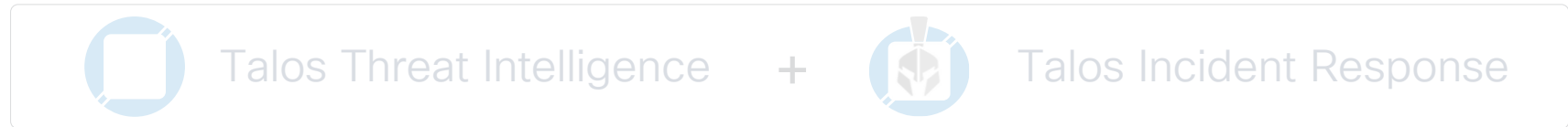
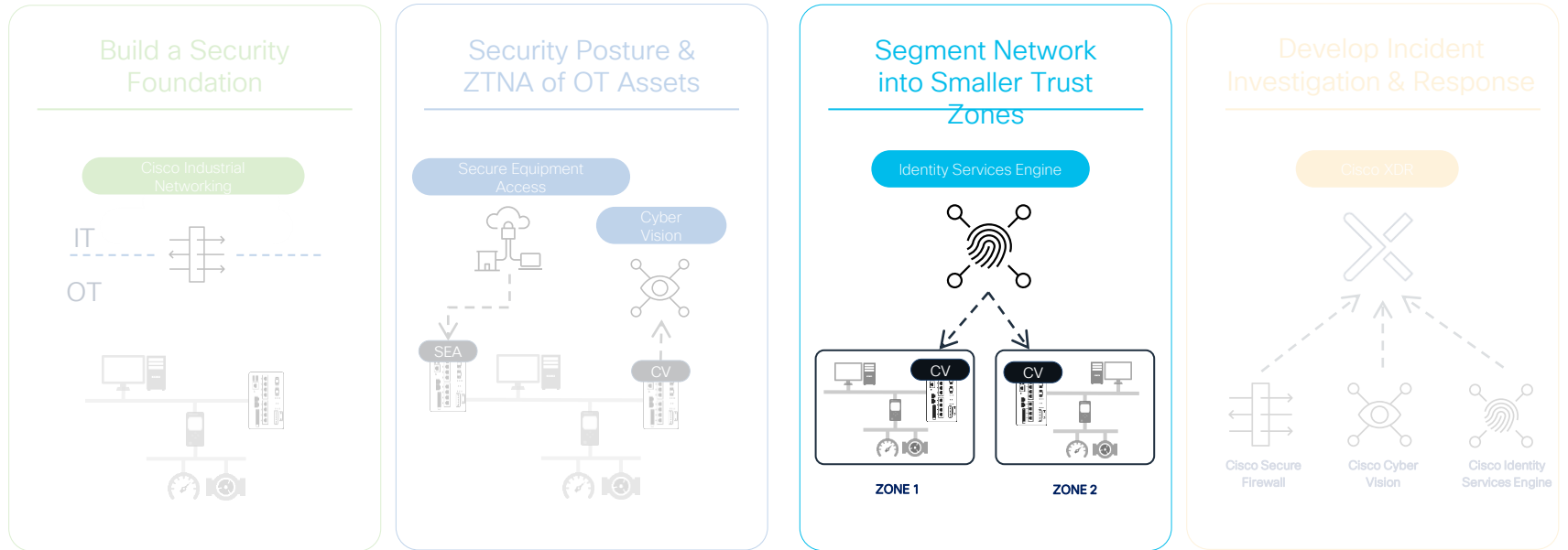


[Easily browse through conduits](#)

Implementing the Zones & Conduits Model



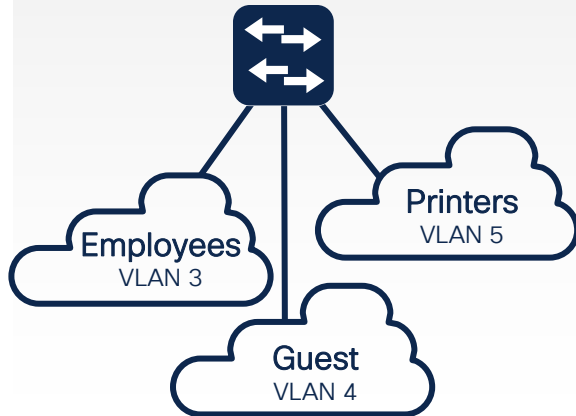
Using the Network as the Policy Enforcement Point



ISE Segmentation Technologies

VLANs

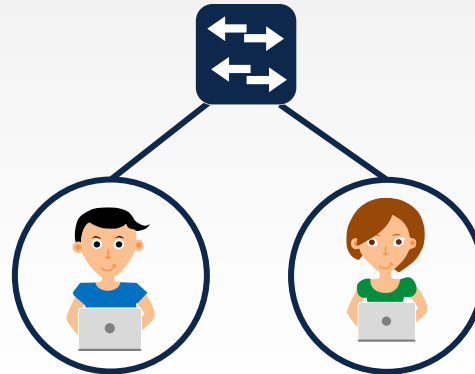
Dynamic VLAN Assignments



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

Security Group Tags

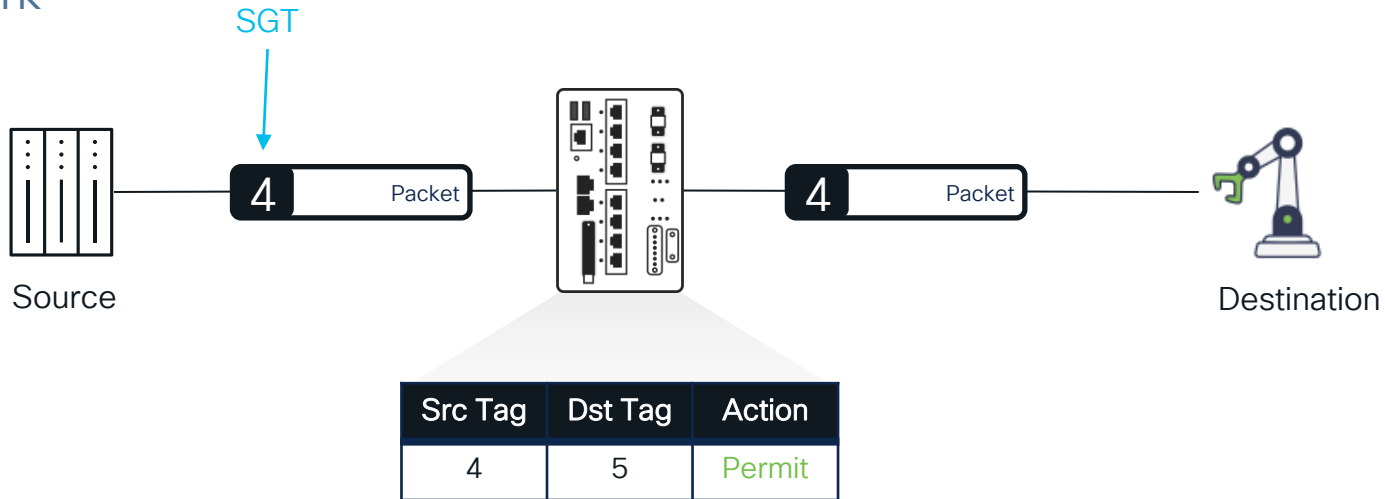
Cisco Group-Based Policy



16-bit SGT assignment and
SGT based Access Control

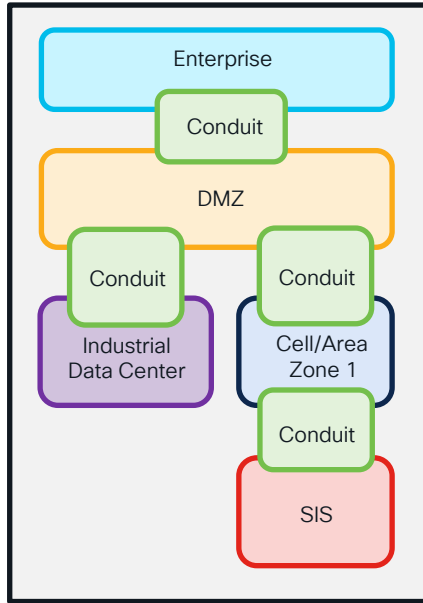
What are Security Group Tags (SGTs)?

Role Based Access Control embedded in the network



Zones & Conduits with SGTs

ISA/IEC 62443



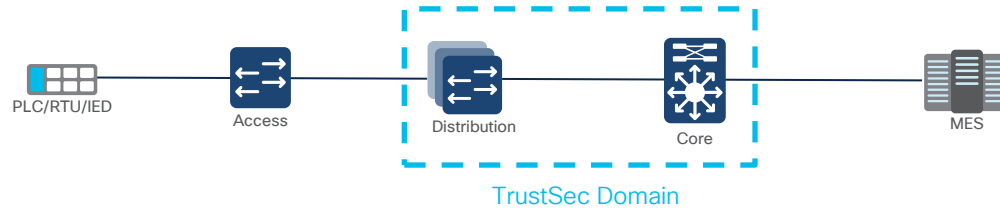
TrustSec Matrix

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

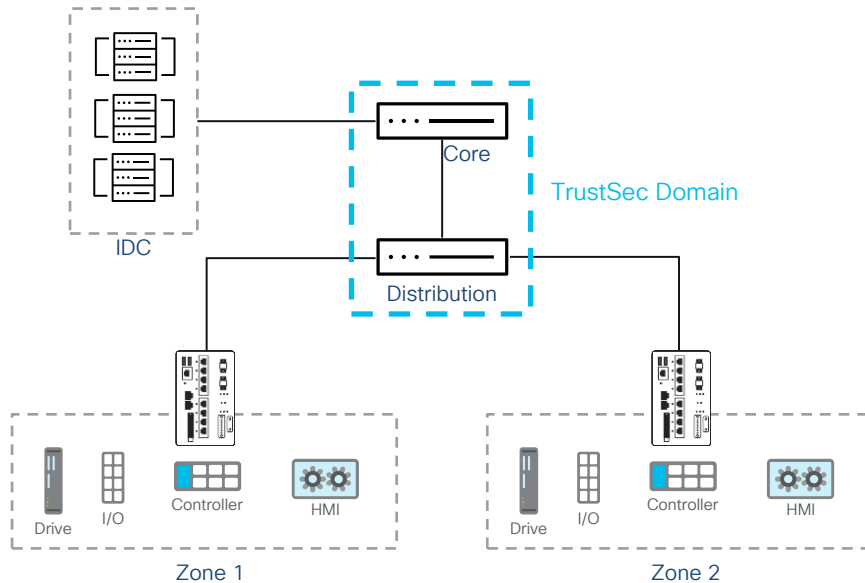
TrustSec Fundamentals



TrustSec Fundamentals – The TrustSec Domain

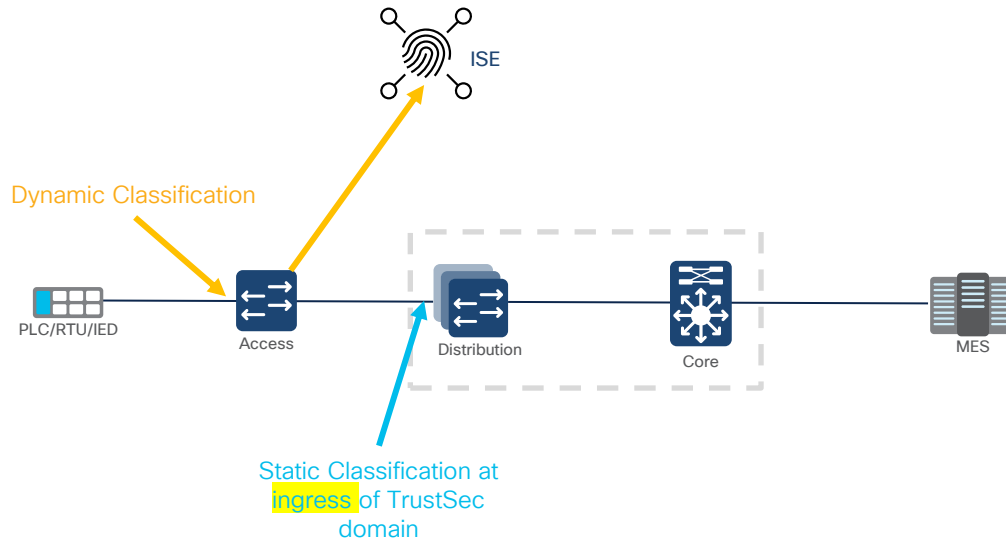


Use Case #1: All devices within a Zone should be able to communicate freely

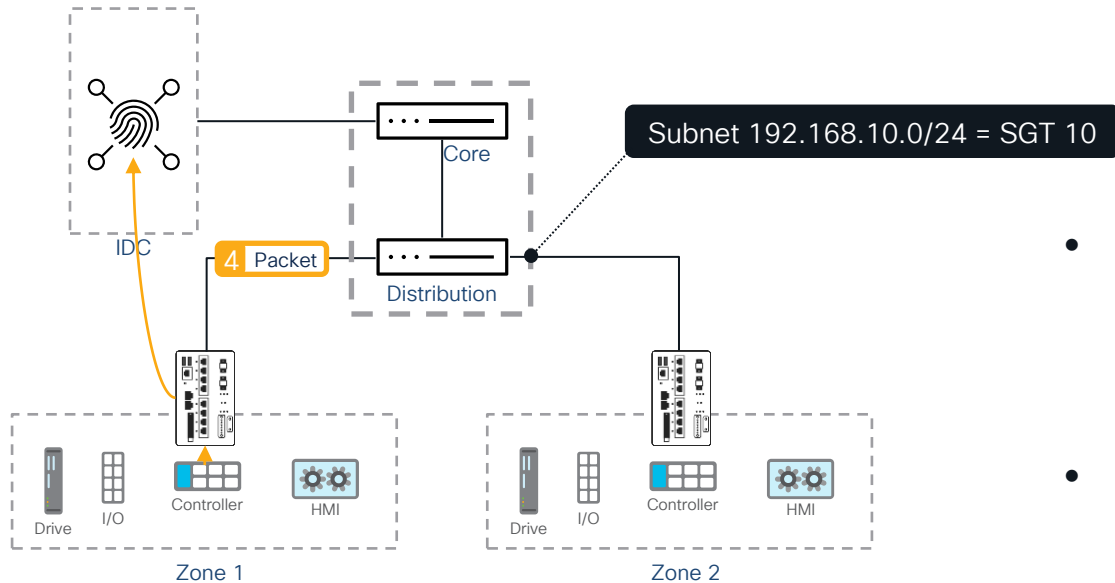


- If my TrustSec domain resides within a Cell/Area Zone, I must create policy to allow communication through the switches
 - More on this later!

TrustSec Fundamentals – Static & Dynamic Classification

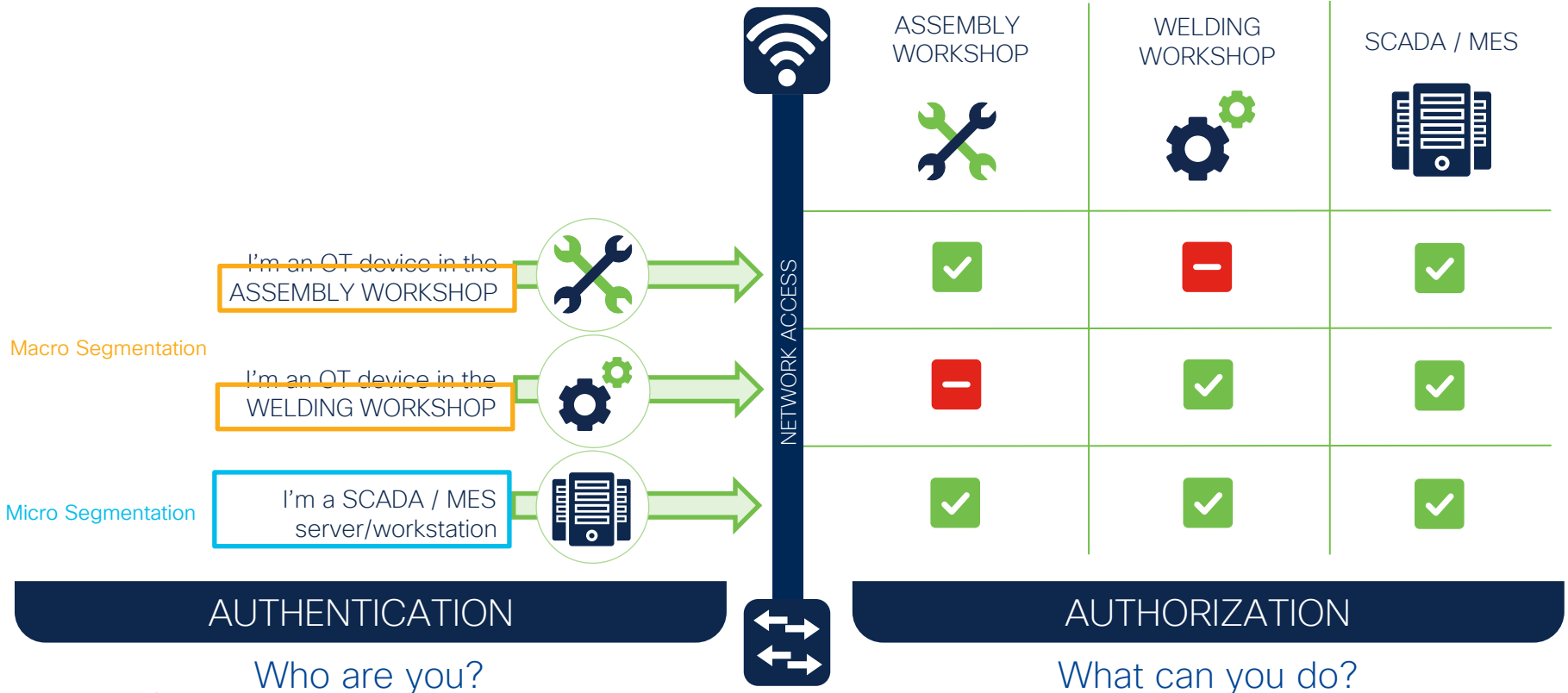


How do we classify an SGT?

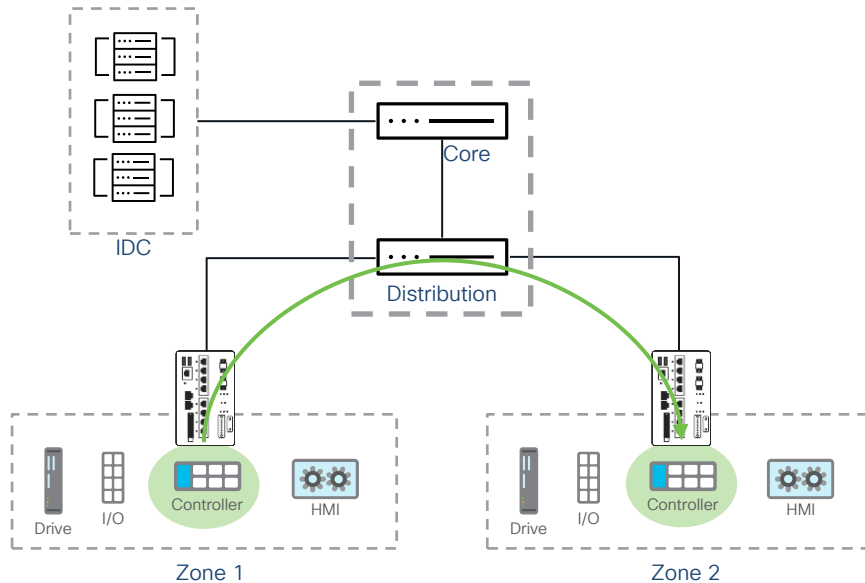


- Static Classification options:
 - VLAN to SGT
 - Subnet to SGT
 - IP to SGT
 - Interface to SGT
- Static classification can be done directly on a switch, or centrally in ISE
- Dynamic Classification is done via Authentication to ISE

Cisco TrustSec – Hybrid Macro / Micro Segmentation



Use Case #8: Communication of named devices between zones is allowed



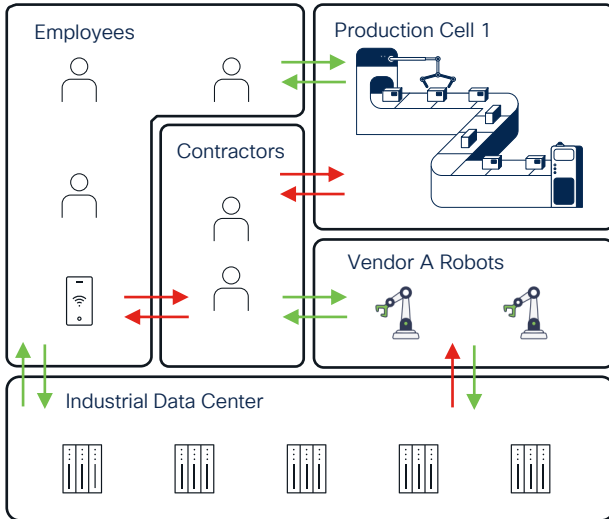
- Zone 1 -> Zone 2 is denied
- Zone 1 PLC -> Zone 2 PLC is allowed

Dynamic Classification of SGTs in ISE

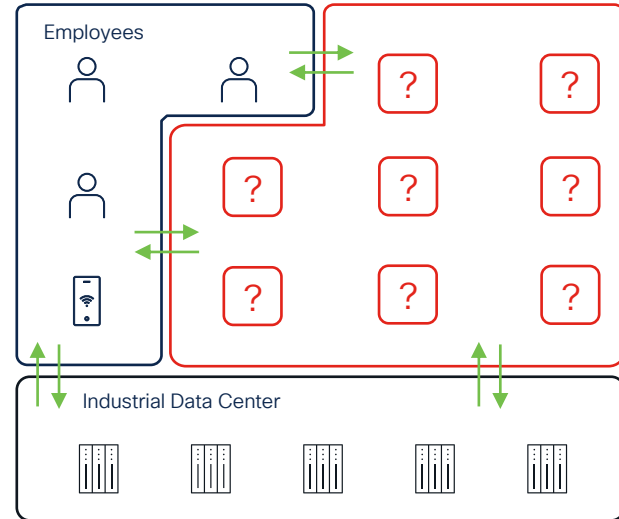


Least Privilege Access: Expectation vs. Reality

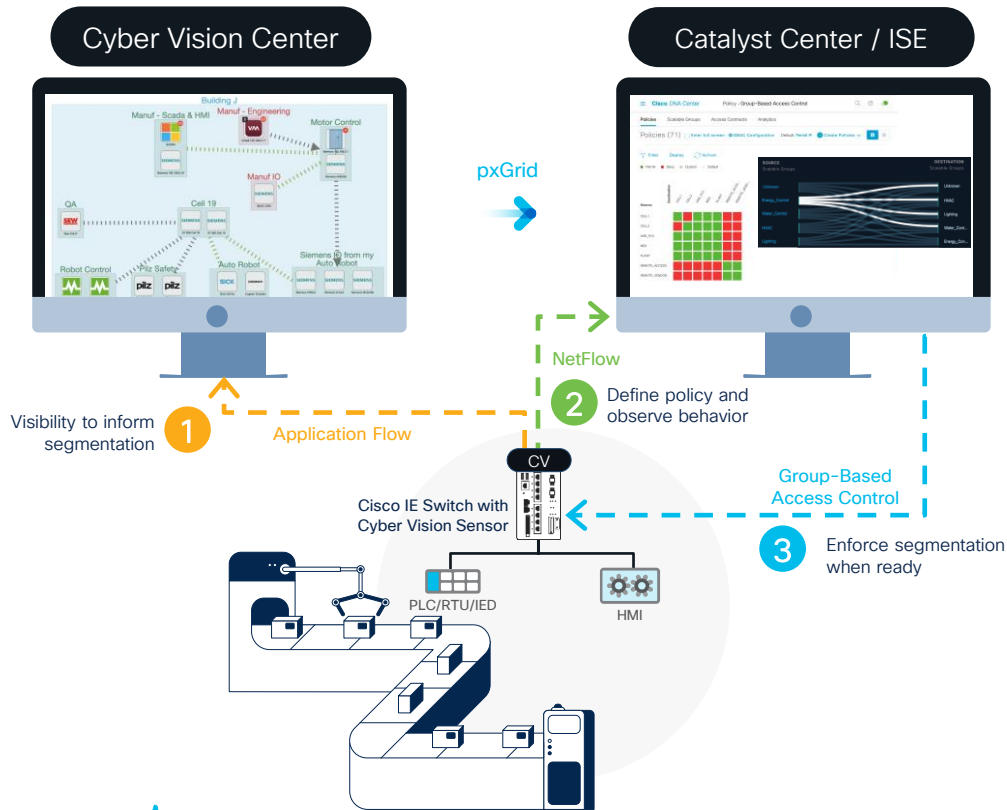
Expectation



Reality



Use visibility to influence segmentation



Visualize Zones & Conduits

visualize aggregated flows as conduits to inform segmentation policy



Dynamic SGT Mapping

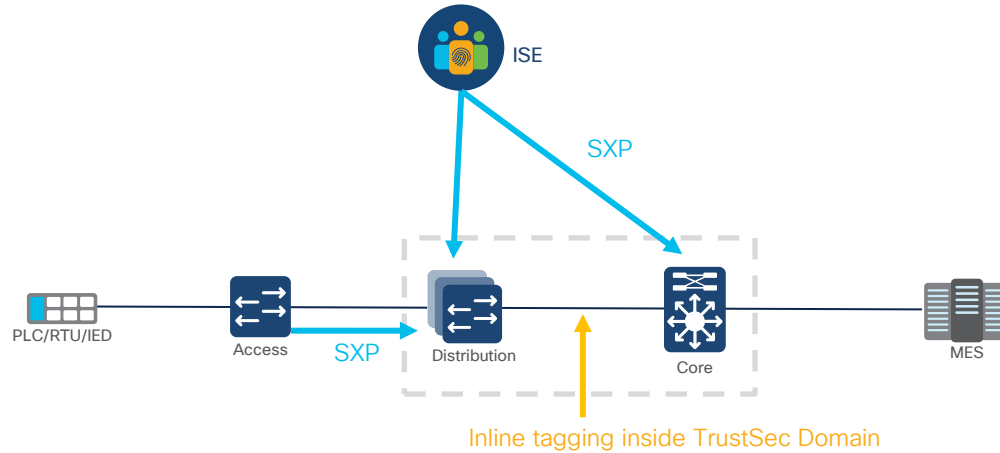
Cyber Vision grouping results in dynamic Group-based policy assignment to endpoints through ISE



Monitor Before Enforcement

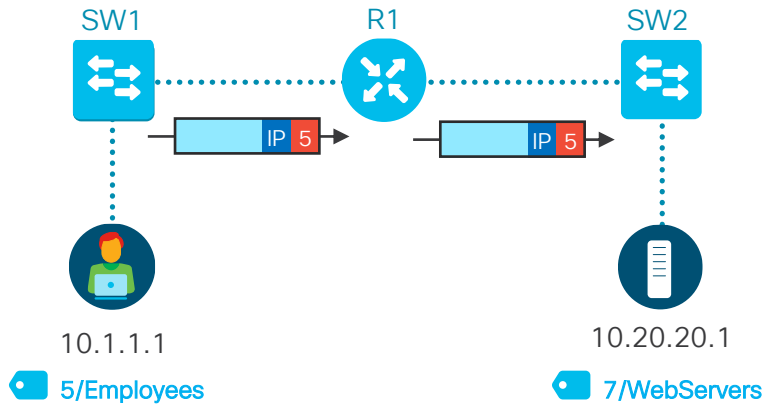
Visualize Group-based network behavior in Catalyst Center and enable enforcement when confident after monitoring

TrustSec Fundamentals – SXP & Inline Tagging



TrustSec Propagation

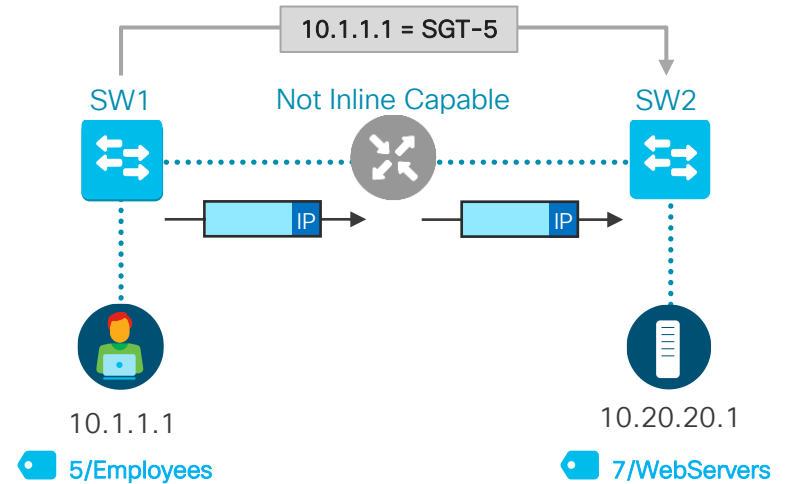
DATA PLANE PROPOGATION (INLINE TAGGING)



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

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

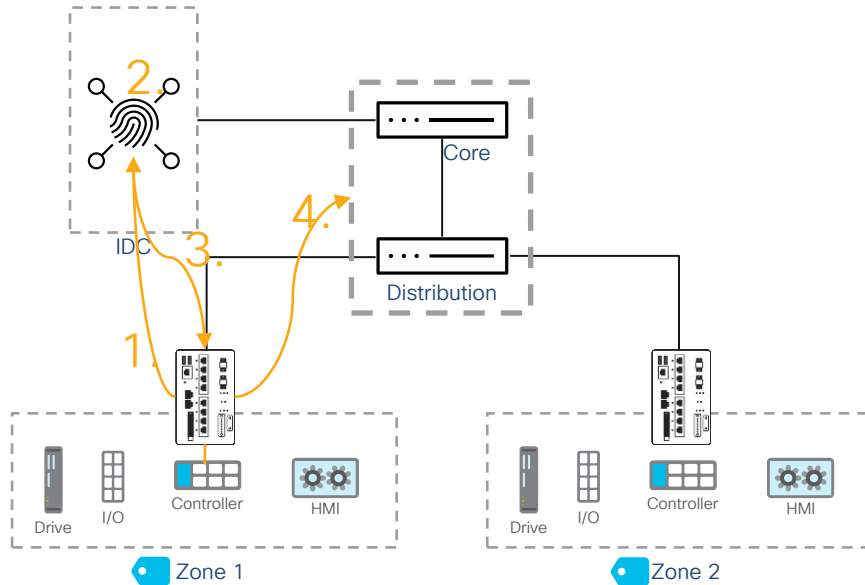
CONTROL PLANE PROPOGATION (SXP)



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

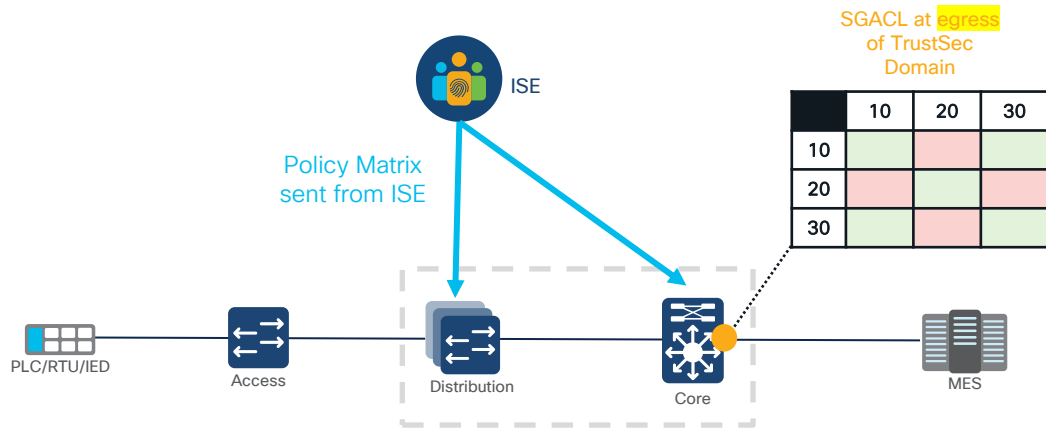
- SXP
- pxGrid

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

TrustSec Fundamentals – TrustSec Enforcement happens at egress of TrustSec Domain



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

SGACL vs IPACL

Policy Objective: “Allow Workstation Group to Cell Area Zones”



IPACL

```
Switch-1#show ip access-list
Extended IP access list Workstation_Policy
 10 permit tcp 10.1.100.0 0.0.0.255 172.16.100.0 0.0.0.255 eq 443
 20 permit tcp 10.1.100.0 0.0.0.255 172.16.100.0 0.0.0.255 eq 22
 30 permit tcp 10.1.101.0 0.0.0.255 172.16.100.0 0.0.0.255 eq 443
 40 permit tcp 10.1.101.0 0.0.0.255 172.16.100.0 0.0.0.255 eq 22
 50 permit tcp 10.1.100.0 0.0.0.255 172.16.101.0 0.0.0.255 eq 443
...
```

SGACL

```
Switch-1# show cts role-based permissions
IPv4 Role-based permissions default:
  Deny IP-00
IPv4 Role-based permissions from group 10:WorkstationGroup_SGT to group
100:ProdCells_SGT:
  Web_SSH-10
```

Making use of the default policy

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

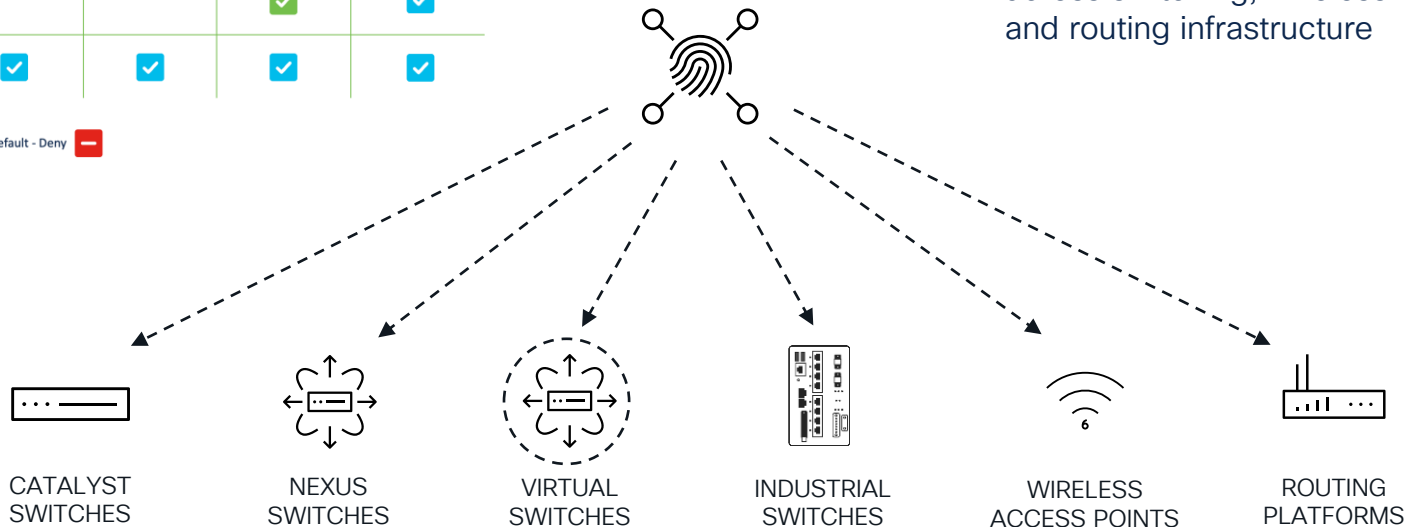
Default - Deny 

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



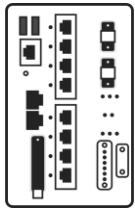
What Devices Support SGT Enforcement?

Enforcement Nodes: Can actively block traffic



Catalyst Switches

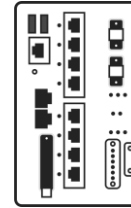
Typically used at the distribution & core



IE3400, IE9300 & IE4000

Typically used at access & aggregation

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



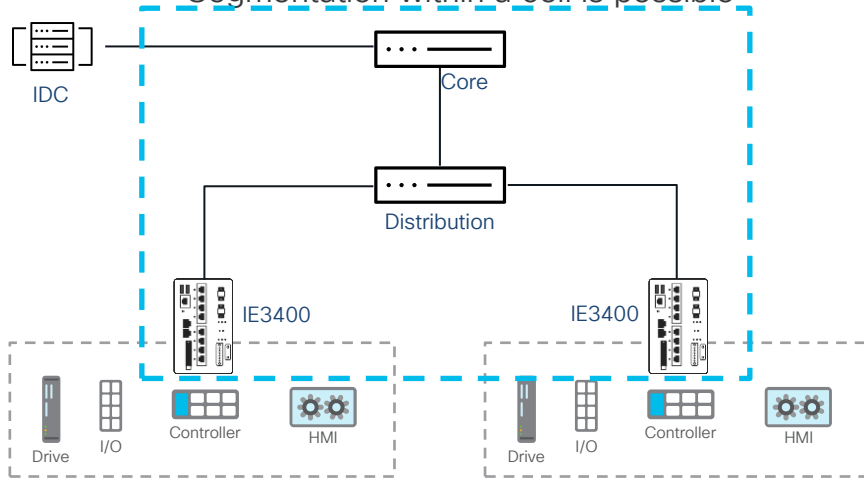
- IE3300
- IE3200
- IE3100
- IE2000

*IE4000 is technically an enforcement node, however, it does not support SXP listener mode so can be used within inline tagging deployments only

How device support effects the TrustSec domain

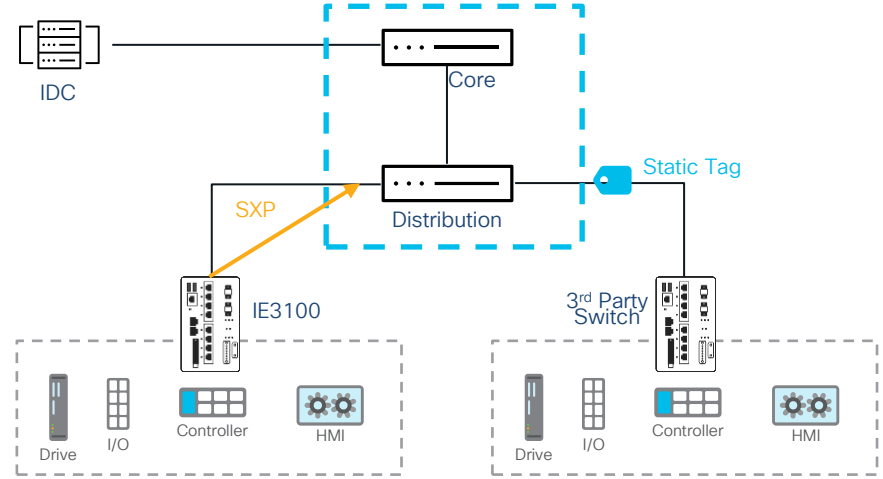
If all switches are capable of enforcement, my TrustSec domain can be everywhere

- Segmentation within a cell is possible



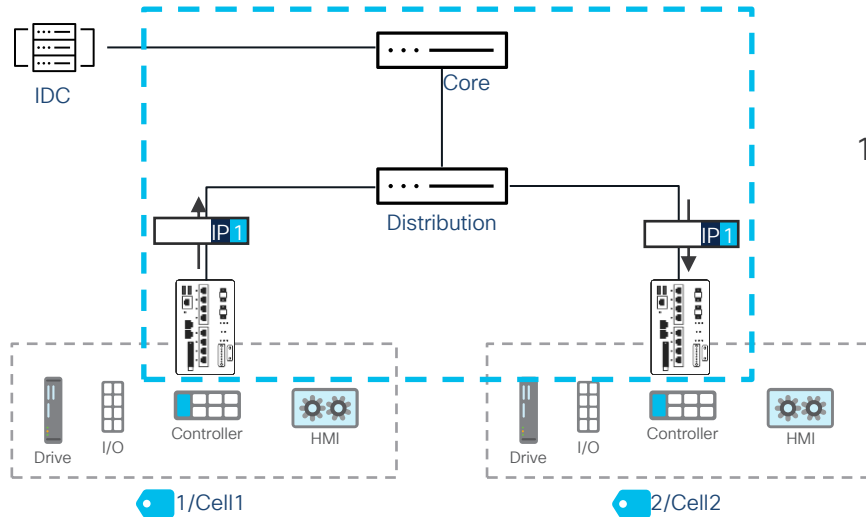
Not all switches need to be enforcement nodes to do TrustSec

- Segmentation between cells still possible

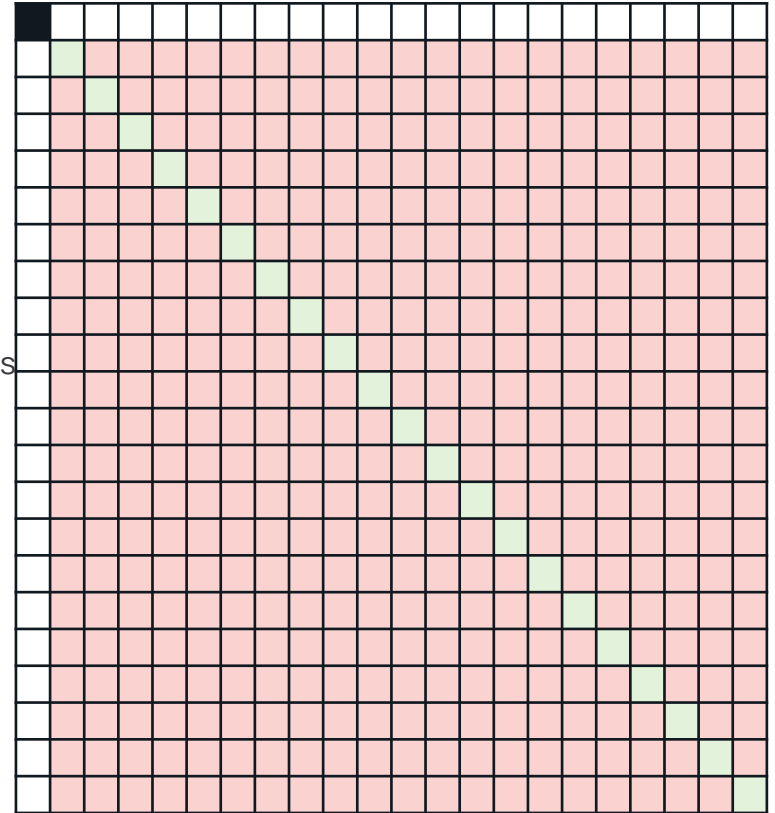


How the TrustSec domain enables you to reduce the number of policies in your network

TrustSec Domain Includes Access Switches

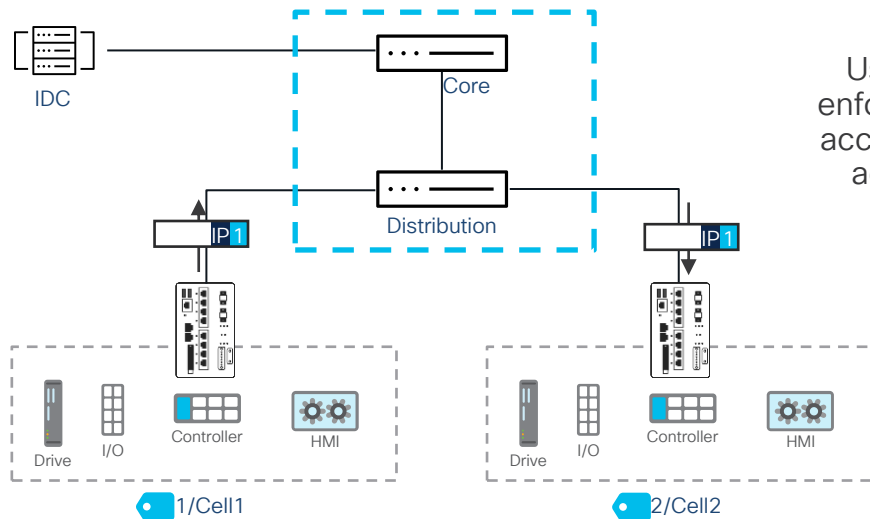


100s of Cells



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

TrustSec Domain Includes Access Switches



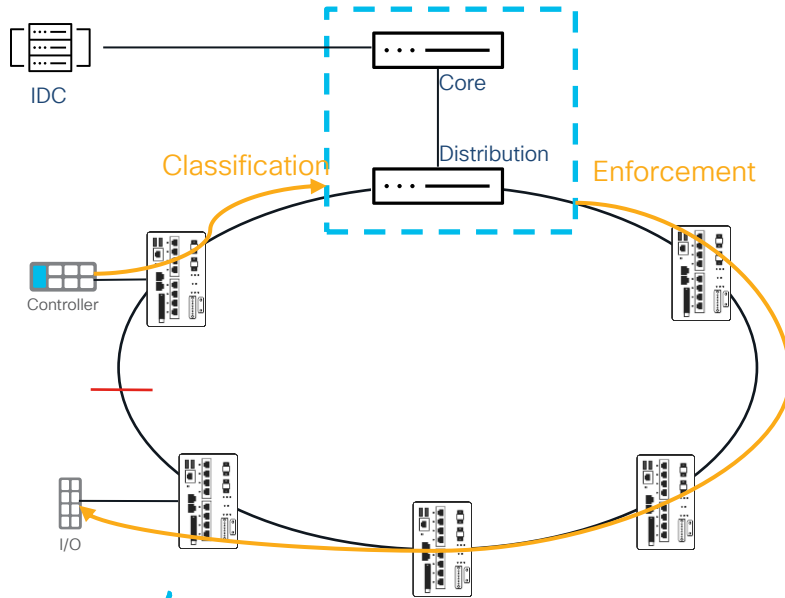
Use lack of enforcement in access to your advantage



- 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

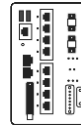


- In this case, aggregation of the SGT does NOT work
- TrustSec domain is part of the ring
- Each ring must have its own SGT so traffic can be permitted through

Change of Authorization (CoA)



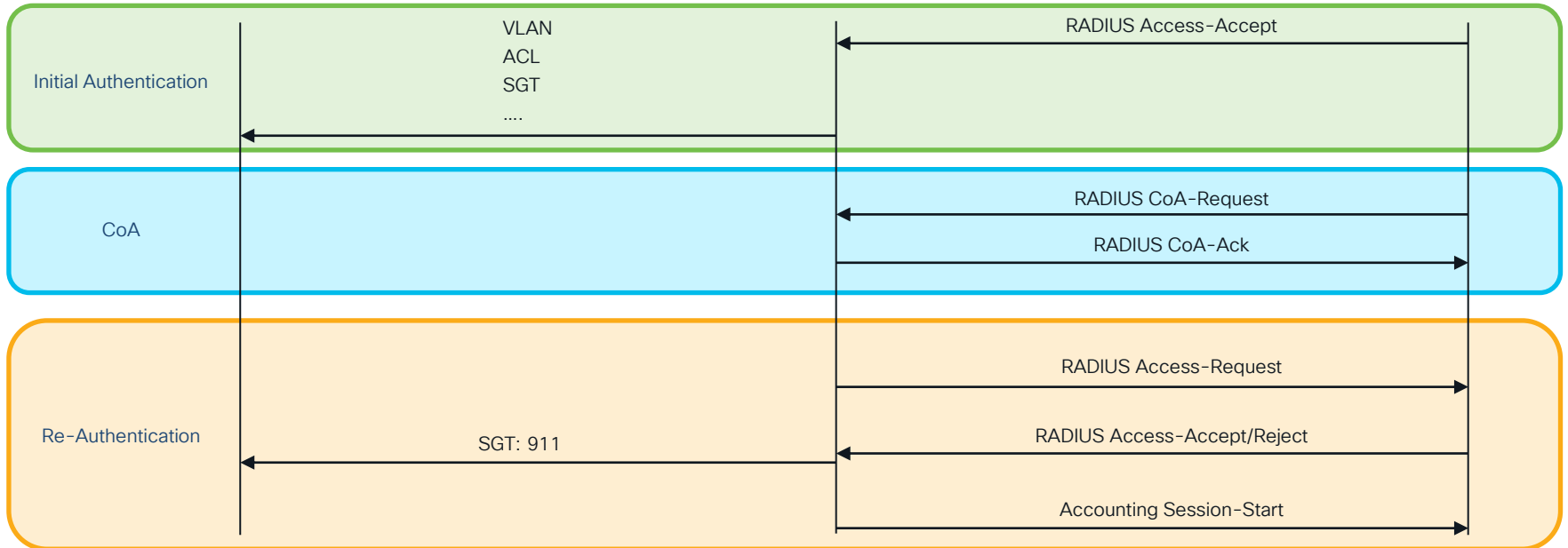
Endpoint



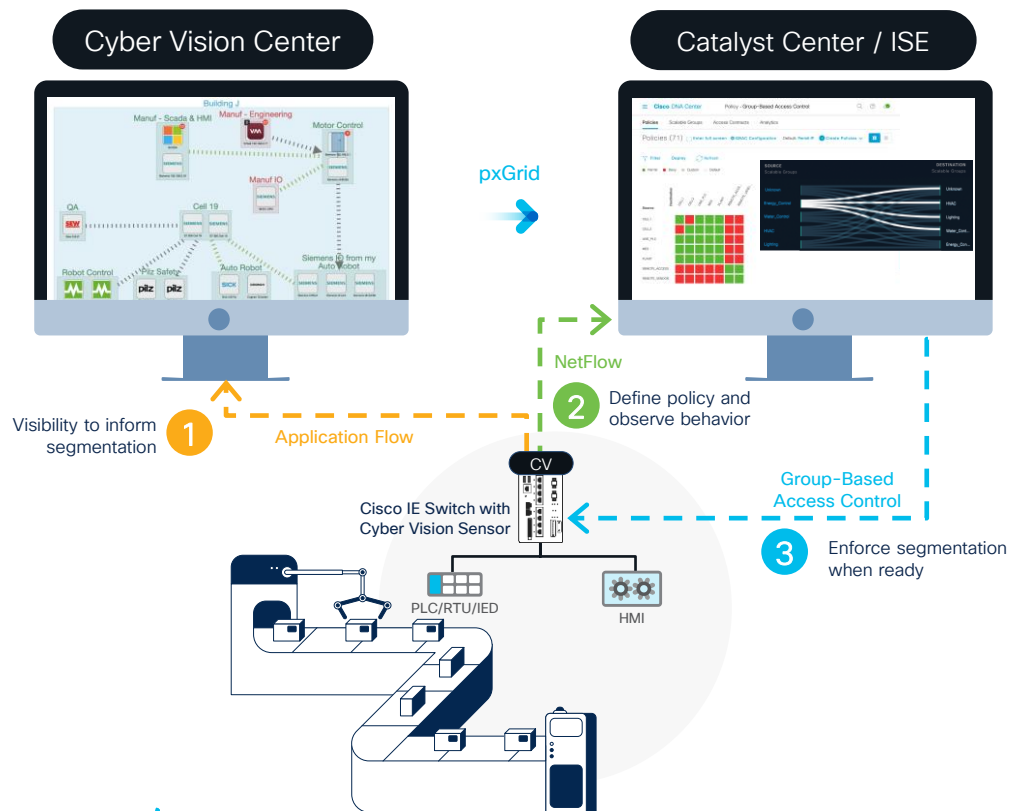
Authenticator



Authentication Server



Recap: Use visibility to influence segmentation



Visualize Zones & Conduits

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

The screenshot displays the Cisco Cyber Vision interface. On the left is a 'Mini Map' with a legend and node types. The main area shows a network diagram with three zones: Zone1, Zone2, and OT-Applications. A device 'Interlock7' in Zone2 is highlighted with a yellow box. A detailed view of this device is shown on the right, including its MAC address, IP address, and various attributes.

Mini Map

Show inner components

LEGEND

- Important
- Control system behavior
- IT Behavior
- Security analysis
- Network analysis
- Others

Node type

- Device
- Component

Device

CLX_P | 17
IP: 10.17.20.72
MAC: 00:00:BC:2D:21:70

Basics Risk score
Mini Map Activities

Zone1
Interlock1

Zone2
Interlock7

OT-Applications
OT

00:00:BC:2D:21:70

MAC Address: 00:00:BC:2D:21:70
Username: 00-00-BC-2D-21-70
Endpoint Profile: CVC_group_Interlock2
Current IP Address: 10.17.20.72
Location: Location → All Locations

Applications Attributes Authentication Threats Vulnerabilities

General Attributes

Description

Static Assignment false
Endpoint Policy CVC_group_Interlock2
Static Group Assignment false
Identity Group Assignment CVC_group_Interlock2

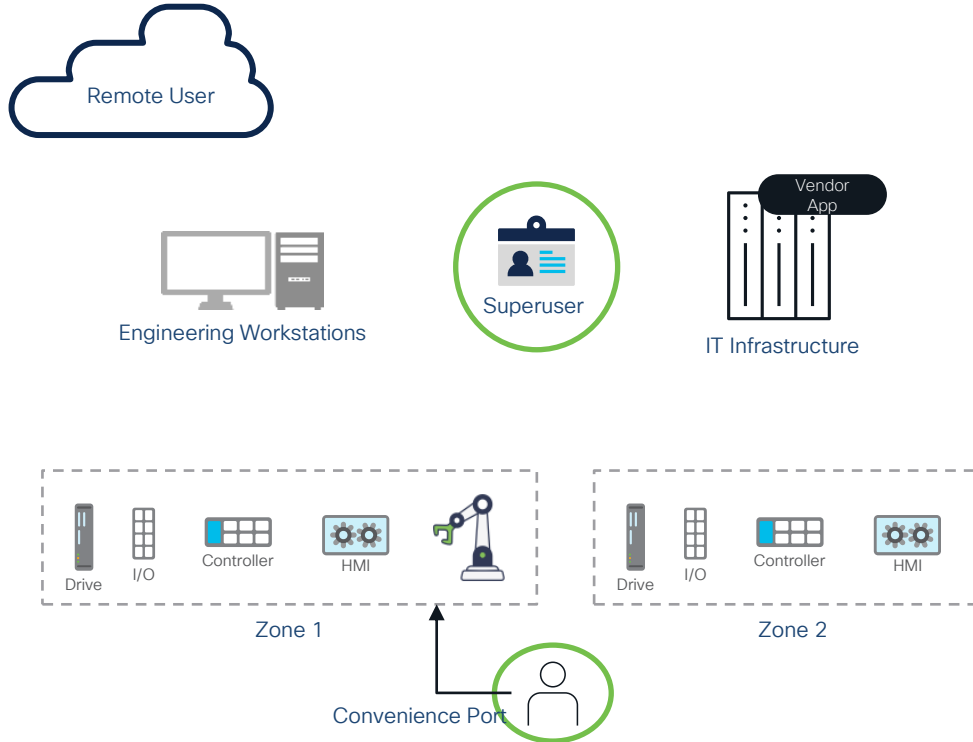
Custom Attributes

Attribute String	Attribute Value
assetGroup	Interlock2
assetCCVGrp	
assetSource	CCV

What about Users in OT networks?

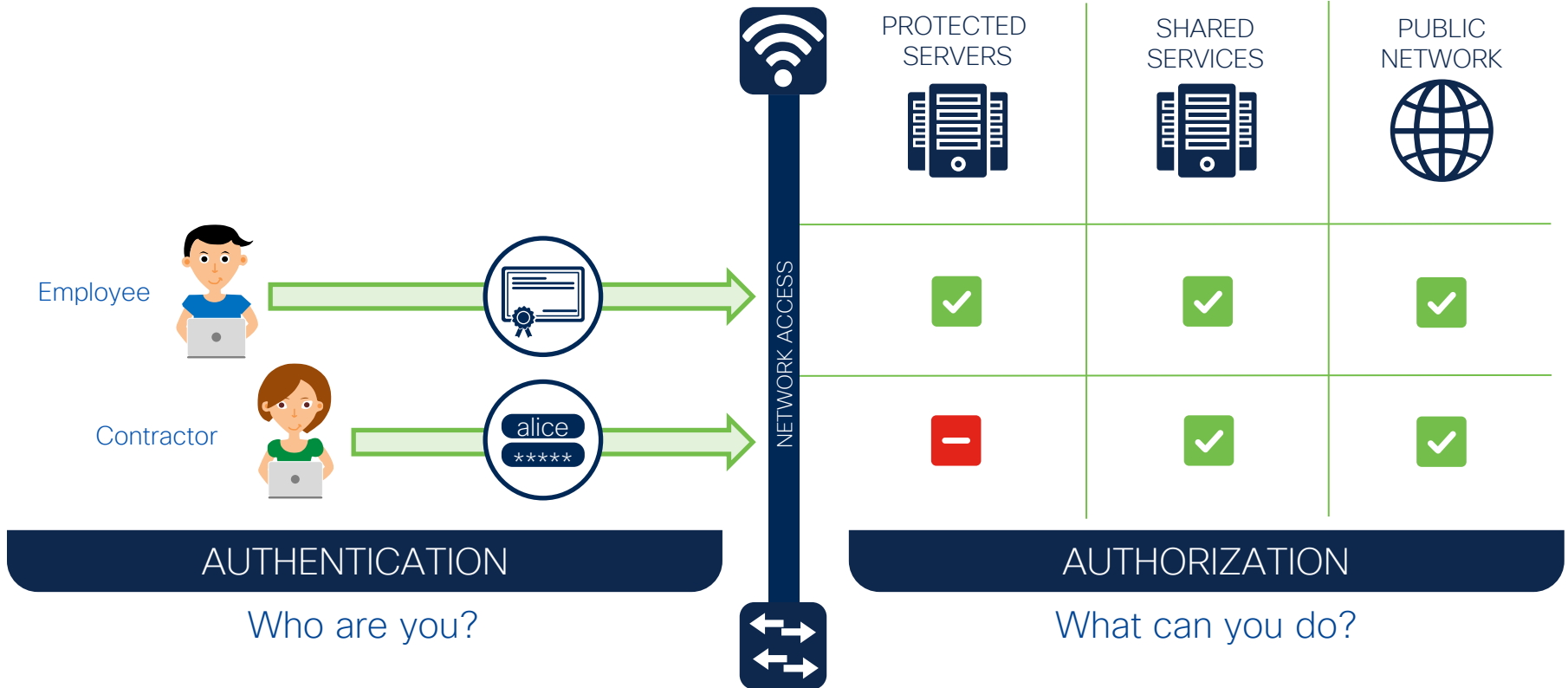


9 Use Cases for Securing Industrial Networks

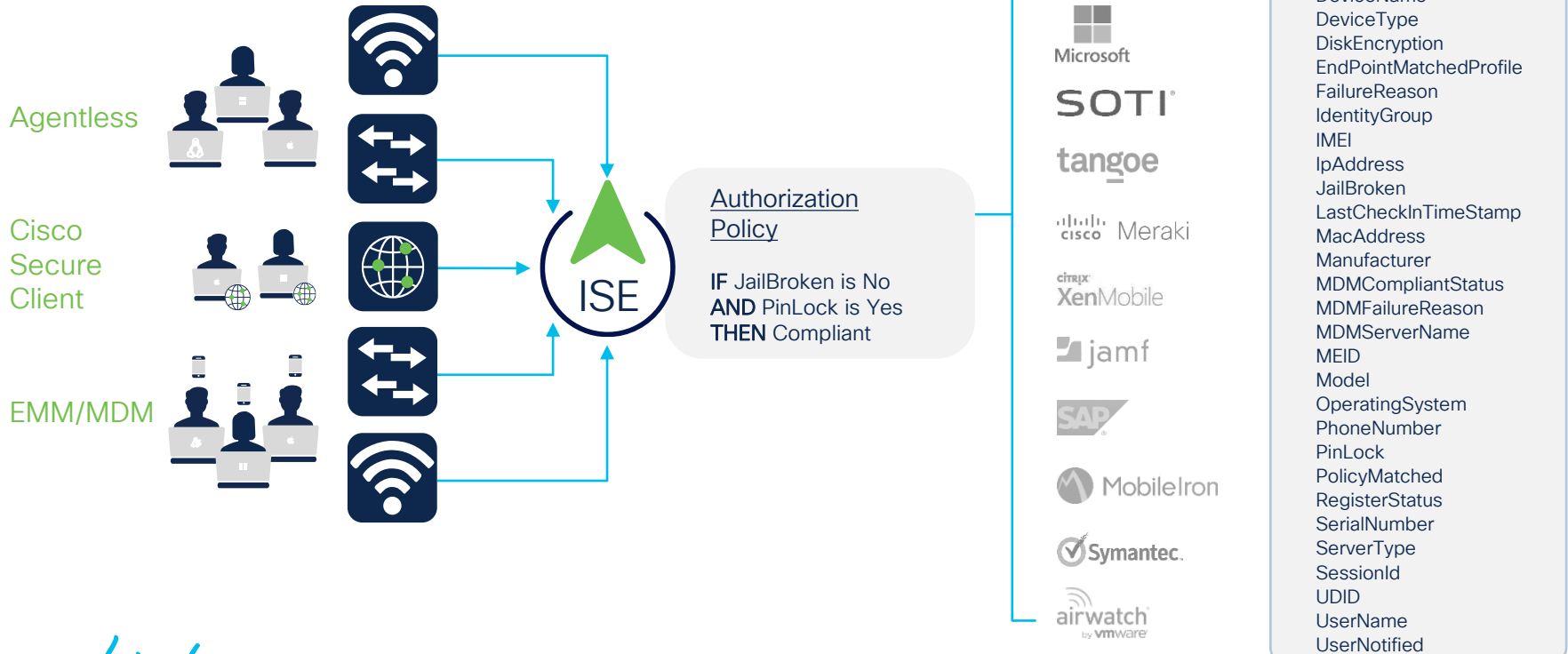


802.1X Authentication is primarily used to enable use cases associated with human interaction to the OT network

Authentication and Authorization



Posture & Compliance



Agentless Posture

Status	Rule Name	Conditions	Profiles	Security Groups
Unknown		AND	<ul style="list-style-type: none"> Network_Access_Authentication_Passed Compliance_Unknown_Devices 	Agentless_Posture
Compliant		AND	<ul style="list-style-type: none"> Network_Access_Authentication_Passed Compliant_Devices 	PermitAccess

Authorization Profile

* Name: Agentless_Posture

Description:

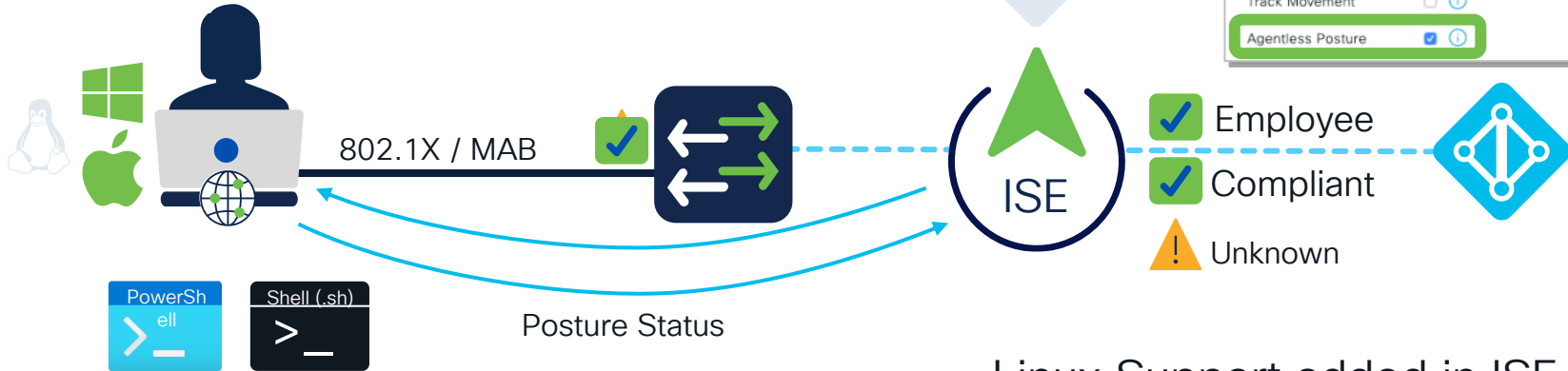
* Access Type: ACCESS_ACCEPT

Network Device Profile: Cisco

Service Template:

Track Movement:

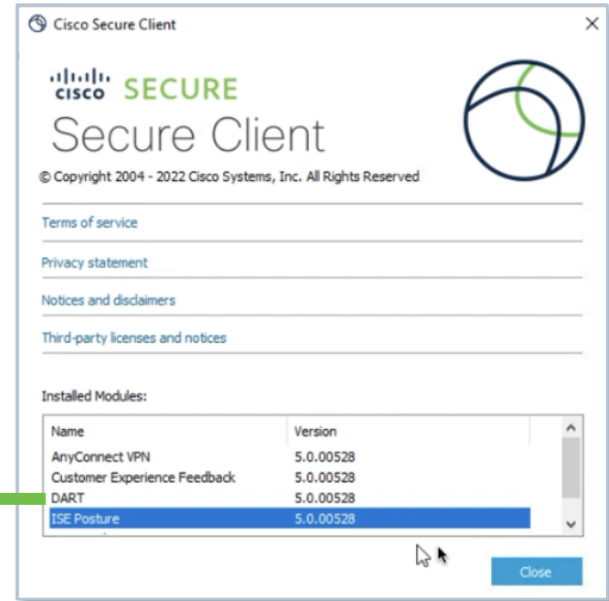
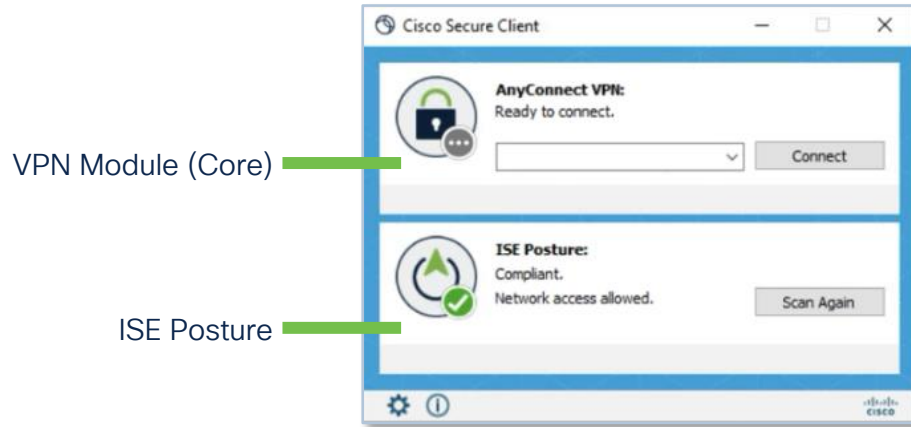
Agentless Posture:



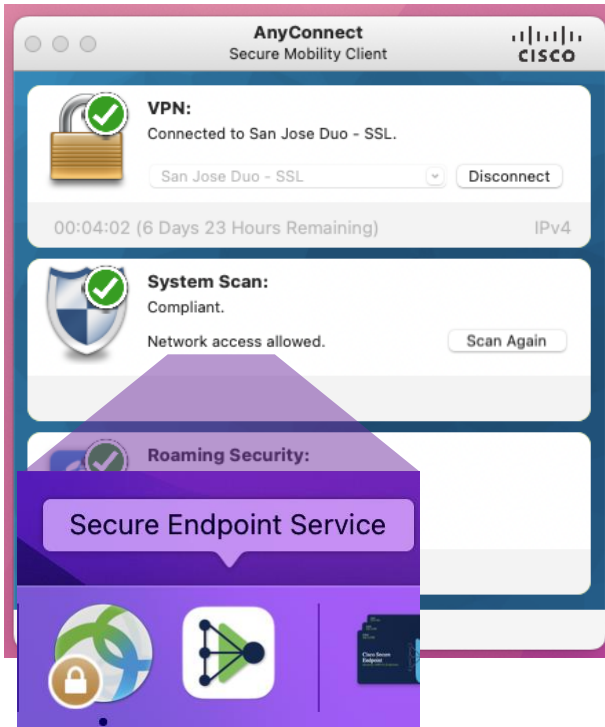
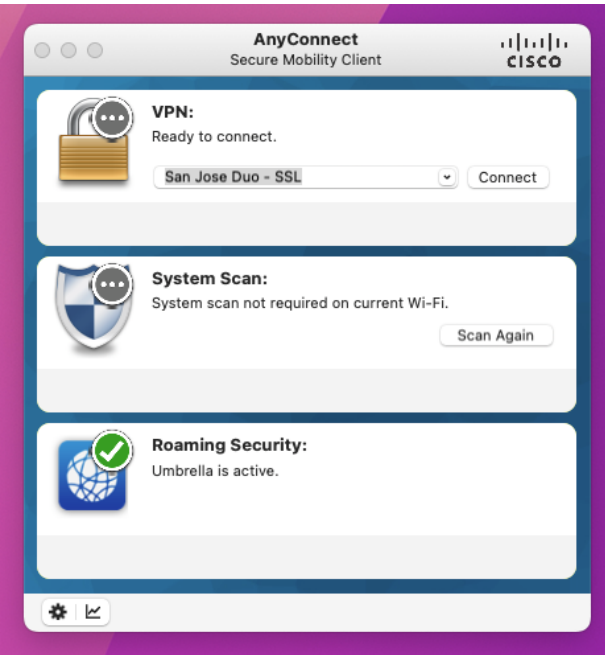
Linux Support added in ISE 3.1



Cisco Secure Client (formerly AnyConnect)



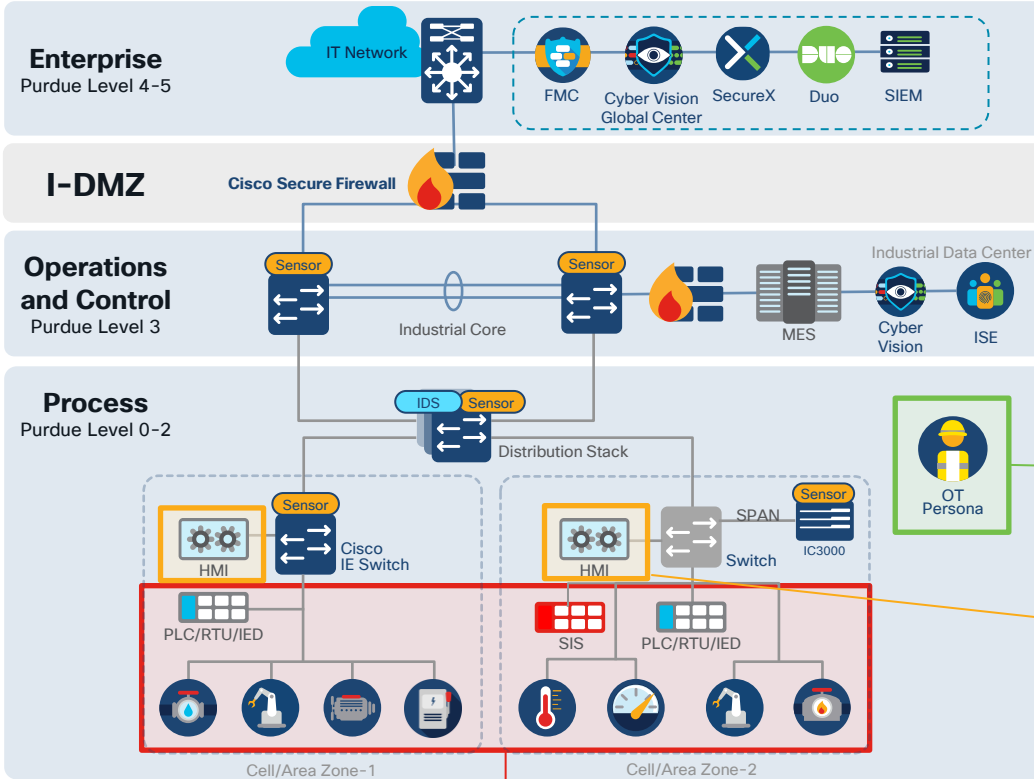
Endpoint Security is the Norm for IT systems



Where do you install Endpoint Protection in the OT?

IT

OT



Employee laptops / tablets / mobiles should always have it

Possibly, but policy may not allow it

Devices wont support it

USB drives still pose a major concern for Industrial Networks



Much of Malware Found by Industrial Firms on USB Drives in 2020 Targeted OT

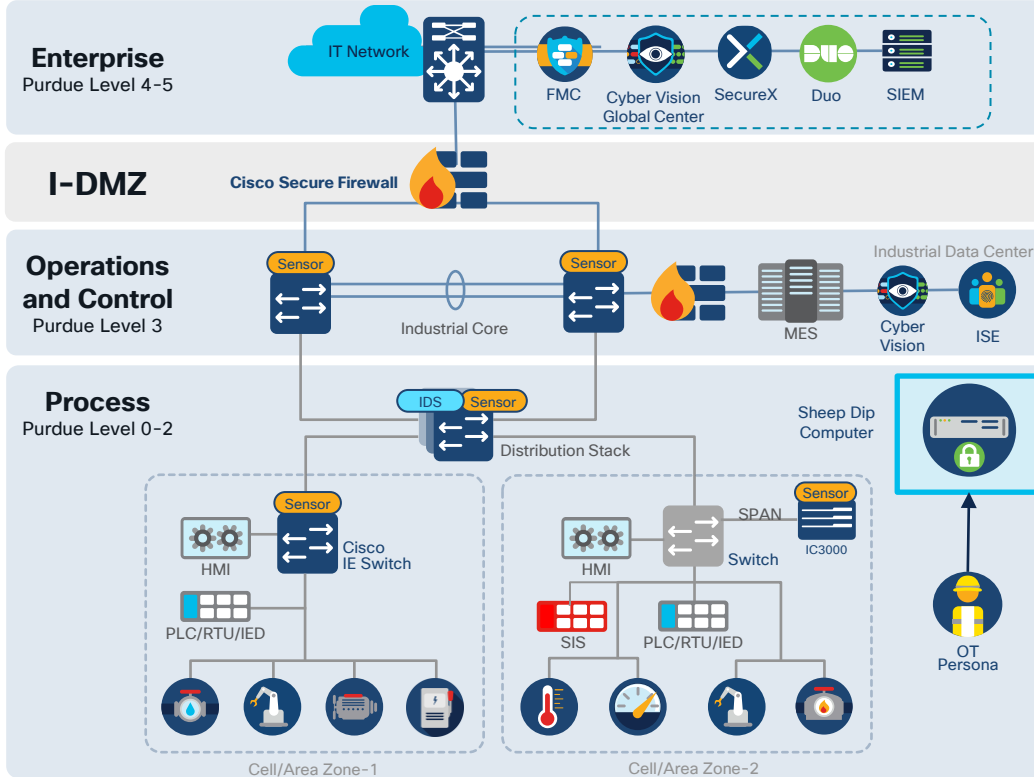
By [Eduard Kovacs](#) on June 22, 2021

“According to Honeywell, 79% of the malware identified by its USB security product on the drives scanned by customers in 2020 was capable of disrupting operational technology (OT) systems, up from 59% in 2019.”

Sheep dip computer for assessing USB drives

IT

OT



- USB will continue to be used in OT (e.g., firmware upgrades)

- Assign a machine on your network to assess USB drives

- Sheep dip computer scans the USB drive to check its content for malware

Remote Users
are the biggest
attack vector to
your network

Remote access to OT assets is key for operations

Maintenance

Remote configuration and maintenance by vendors and third-party technicians.

Troubleshooting

Remote experts helping quickly solve issues to maintain production uptime.

Avoiding Truck Rolls

Large sites, distributed operations, limited resources. Remote access helps lower OpEx.



Roadways



Transportation



Renewables



EV chargers



Utilities



Manufacturing



Oil & Gas



Mining



Ports

Operations need remote access to all assets at anytime, for internal and external experts

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

Zero Trust Network Access (ZTNA)

“ZTNA provides controlled **identity and context-aware** access to resources. It starts with a **default deny** posture and **adaptively offers the appropriate trust** required at the time. A **trust broker** mediates connections between applications and users. The result **reduces risk** and offers **more flexible and responsive** ways to connect and collaborate.

Gartner[®]

Market Guide for Zero Trust Network Access,
August 2023

CISCO *Live!*

Least privilege access

Assets hidden from discovery

No lateral movement

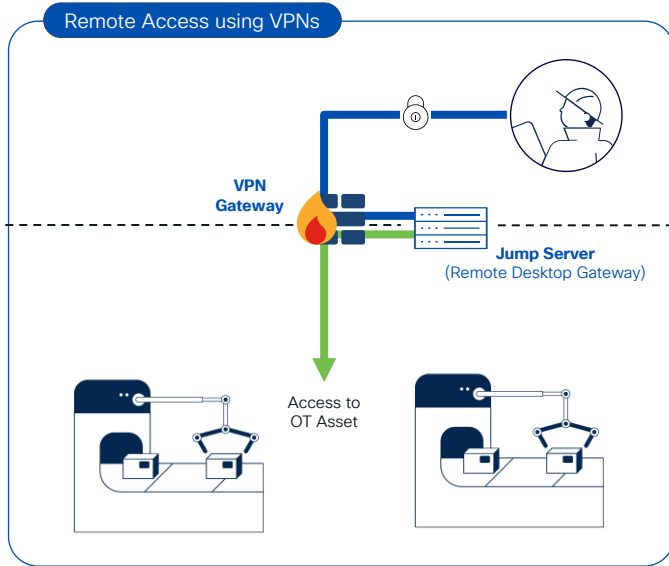
Device posture compliance

Time/date restricted access

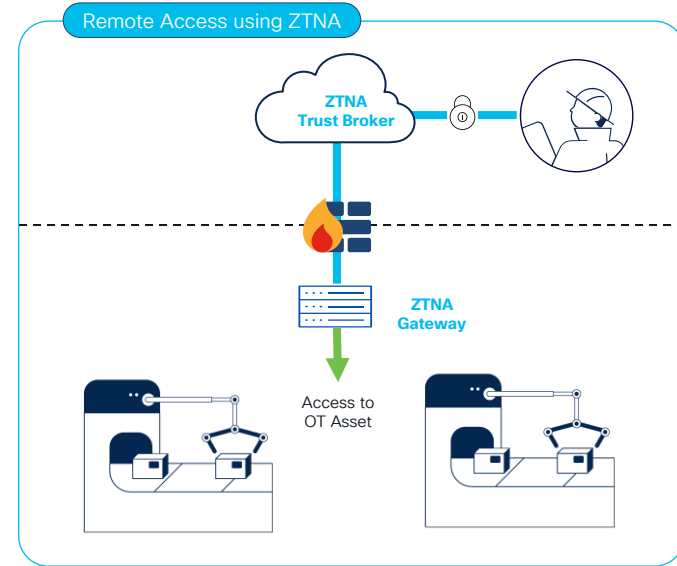
Reduced attack surface

More flexible and responsive

Evolving from VPNs to ZTNA



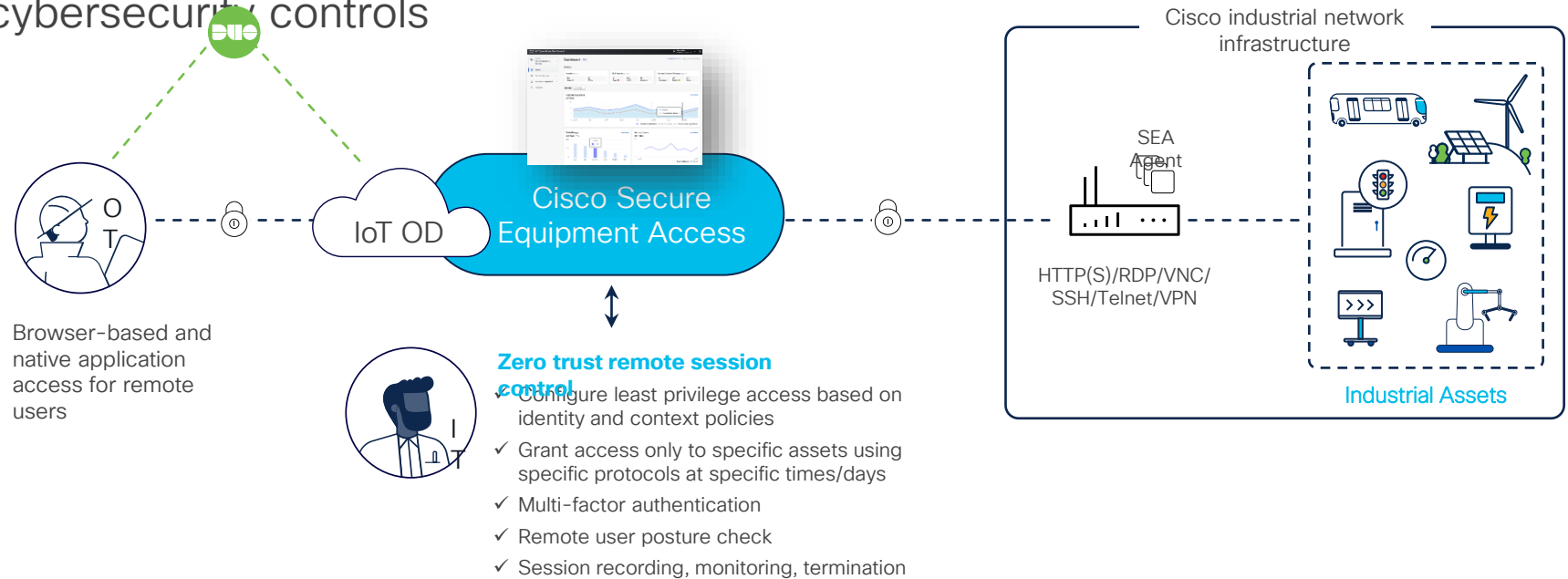
- Always-on solutions with all-or-nothing access
- Firewall rules need to be frequently updated
- Manual session management using jump servers



- 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

Zero Trust Network Access (ZTNA) for OT Assets

Empower OT teams to easily perform remote operations while enforcing strong zero trust cybersecurity controls



Cisco Secure Equipment Access

OT resources isolation

Never expose your entire network. Only assets you specify can be accessed by the remote users you choose.

Policy enforcement

Trust no one. Access is granted only on the day/time you decide and only using the protocols you choose for each asset.

Only assets you select can be accessed...

The screenshot displays a grid of asset cards under the heading "All Access Resources". Each card represents a different asset and its access method:

- IR1101-WebApp (WEB_APP)**: Via Web App, IR1101-SEA. Availability: Always Active, Last Accessed: Never.
- NUC - RDP (RDP)**: Via RDP, IR1101-SEA. Availability: Always Active, Last Accessed: 8 minutes ago.
- PLC (SEA_...)**: Availability: Always Active, Last Accessed: Never.
- RPI-Linux-VNC (VNC)**: Via VNC, IR1101-SEA. Availability: Always Active, Last Accessed: 9 minutes ago.
- SSH-IR1101 (SSH)**: Via SSH, IR1101-SEA. Availability: Always Active, Last Accessed: 15 days ago.

...using the protocols you choose

The "Add Access Method" dialog box is shown, allowing the user to select an access method for the asset "1769-L16ER/B".

Connected Client Details

Client Name	1769-L16ER/B	IP Address/Host Name	192.168.100.101
Device Type	PLC		
Description	Conveyor belt controller		

Access Method Details

Access Method*

- SSH
- RDP
- VNC
- Web App
- Telnet

...at the time/day you define

The "Group Details" dialog box for the "Fanuc Robots" group is shown, highlighting the schedule settings.

Name	Fanuc Robots
Description	-
Creation Date	Aug 31, 2023 11:22 AM
Enforce Full-Screen Monitoring & Recording	Off
Enforce Inline (SSH/RDP/VNC) Recording	On
Schedule Start	Aug 31, 2023 11:27 AM
Schedule End	Aug 31, 2023 12:27 PM
Duration	1 hour

Cisco Secure Equipment Access

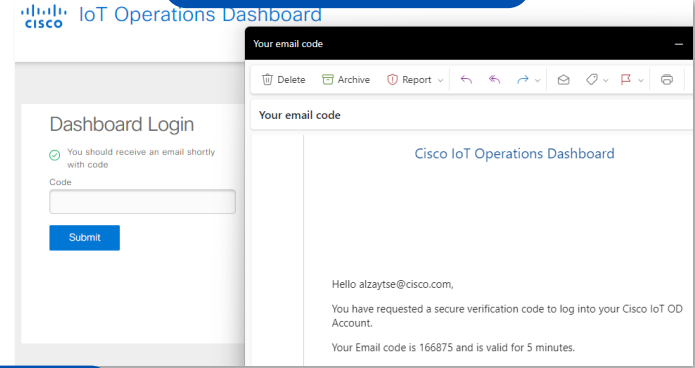
Identities and roles

Enforce identities with MFA & SSO. Simplify operations with custom roles and groups for assets segregation.

Security posture check

Prevent malware intrusion by verifying health of remote user's computers using Cisco Duo.

Zero trust with MFA and SSO

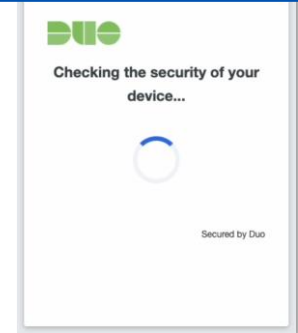


Custom user roles

Create Custom Role

Permission	Description
<input type="checkbox"/> Applications Application Inventory and Instances Read	<ul style="list-style-type: none">View list of ApplicationsView Application InstancesView Application details View More
<input type="checkbox"/> Applications Application Inventory and Instances Read-Write	<ul style="list-style-type: none">View list of ApplicationsView Application InstancesView Application detailsView Application Instance details and additional information (View Application Logs, View IP Configuration, View Resource usage)Perform Device level actions (Device Refresh, Download Tech support logs)Add ApplicationInstall ApplicationDelete ApplicationChange Application configurationPerform Application level actions (Start/Stop/Uninstall/Change version)

Posture check with Duo



Cisco Secure Equipment Access

Access remote assets with just a browser

Clientless ZTNA

Users only need a browser to access remote assets using RDP, VNC, SSH, Telnet or HTTP(S)

Use native client after security posture check

Agent-based ZTNA

Allow use of native desktop clients for advanced tasks, only once the user's computer has been verified for compliance with health policies.

The image displays three overlapping windows illustrating the Cisco Secure Equipment Access workflow:

- Top Window (Cisco IoT - Google Chrome):** Shows the 'Remote Sessions' page for 'Fanuc Robots (2)'. A session for 'LinuxServer (SSH)' is listed, accessed via SSH on host 'IR1101-SEA' 21 hours ago.
- Right Window (Terminal):** A terminal window showing a shell prompt 'pi@raspberrypi:~\$' and a directory listing of the home directory, including folders like 'Bookshelf', 'Downloads', and 'Pictures'.
- Bottom Window (FileZilla):** Shows a file transfer session from 'pi@192.168.2.2 - FileZilla'. The local site is 'C:\Users\labzytsf\Documents\Impact SEA Plus demo\'. The remote site is 'files'. A file named '3840x2160-spiral-abstract_1575661441.jpg' is selected for transfer.

Cisco Secure Equipment Access

Session monitoring

Take action with real-time visibility on all active sessions and the ability to join and terminate them.

Session audit trails

Fuel investigations and compliance reports with full history of past sessions, including their recordings.

Session monitoring and termination

Access Management

Access Control Groups Users **Active Sessions** Session History

Active Sessions (4)

Q Search Table

Refresh As of: Aug 31, 2023 12:05 PM

Connected Client	Access Method	User	Session Start	Duration	Monitor	Security
External-switch	External-switch (SSH)	alzaytse@cisco.com	2 minutes ago	Unscheduled	Join Session	Terminate
External-switch-Linux-Server	External-switch-Linux-Server (VNC)	alzaytse@cisco.com	a minute ago	Unscheduled	Join Session	Terminate
External-switch-Linux-Server	External-switch-Linux-Server (VNC)	alzaytse@cisco.com	a few seconds ago	Unscheduled	Not Monitored	Terminate
External-switch-Linux-Server	External-switch-Linux-Server (VNC)	alzaytse@cisco.com	a few seconds ago	Unscheduled	Join Session	Terminate

Session history with recordings and audit info

Access Management

Access Control Groups Users Active Sessions **Session History**

Session History (248)

Start Date: May 2, 2023 End Date: Aug 31, 2023 Only Show Recorded Sessions

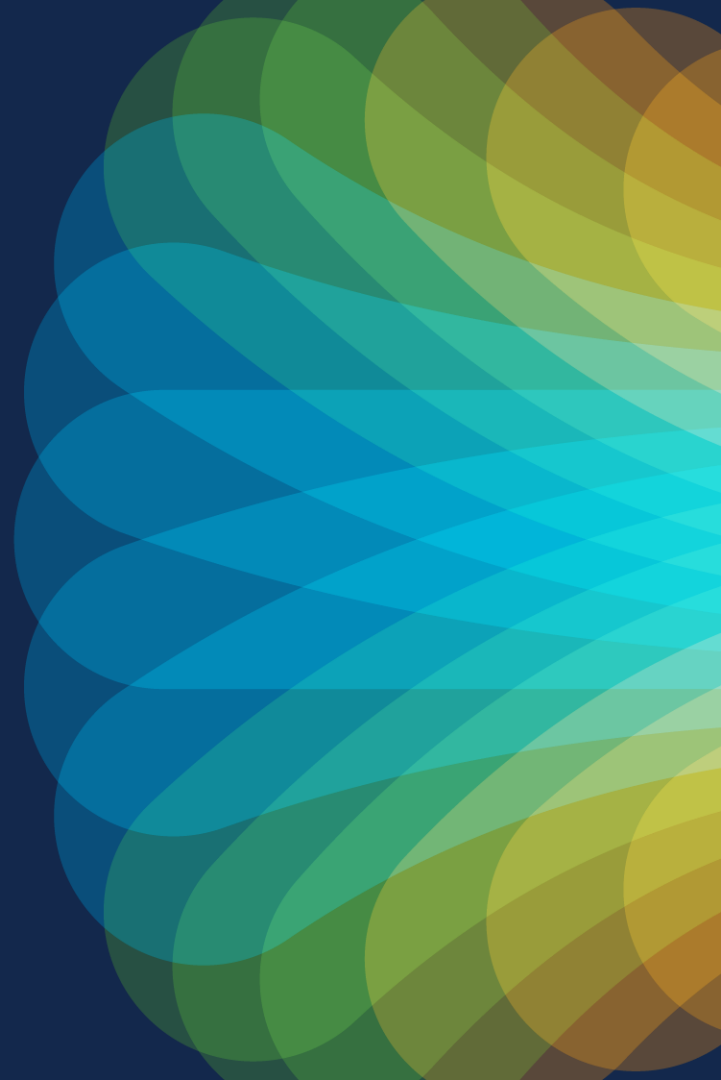
Q Search Table

Refresh As of: Aug 31, 2023 12:09 PM

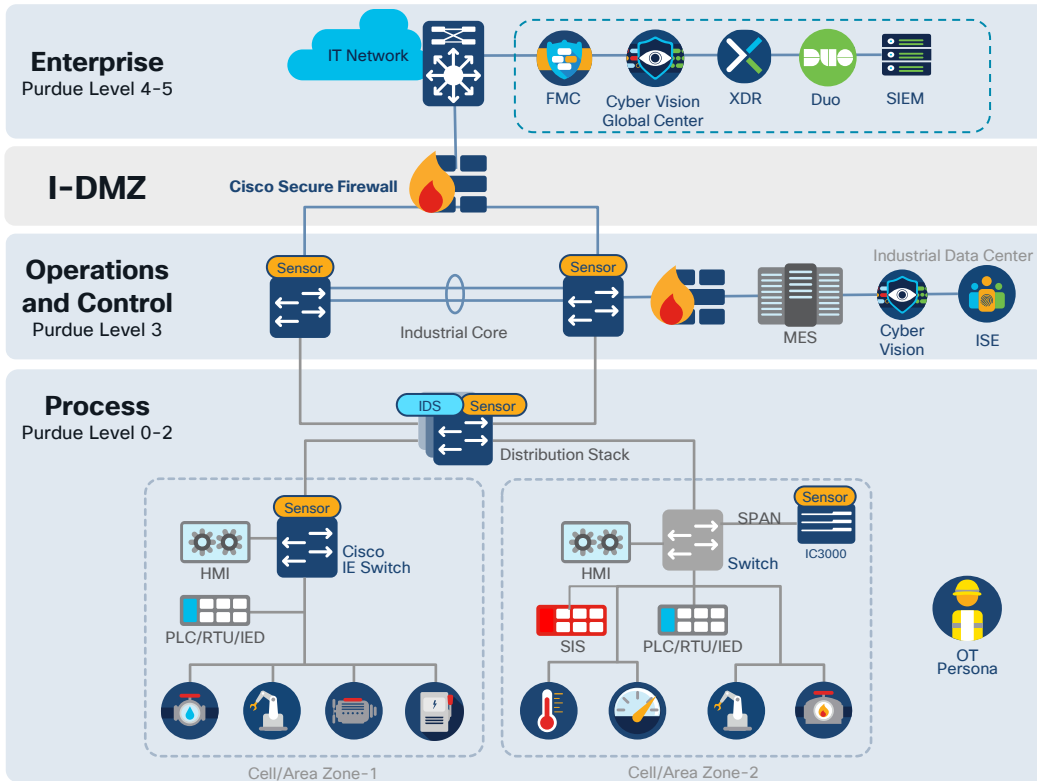
Session Start	Session End	Connected Client	Access Method	User	Terminated	Recorded	Actions
Aug 31, 2023 12:03 PM	Aug 31, 2023 12:07 PM	External-switch	External-switch (SSH)	alzaytse@cisco.com	No	Yes	...
Aug 31, 2023 10:39 AM	Aug 31, 2023 10:59 AM	LinuxServer	SEA* Filetransfer Linux 192.168.2.2 (NATIVE)	alzaytse@cisco.com	No	No	...
Aug 31, 2023 10:26 AM	Aug 31, 2023 10:36 AM	LinuxServer	LinuxServer (SSH)	alzaytse@cisco.com	No	Yes	...
Aug 31, 2023 10:26 AM	Aug 31, 2023 10:26 AM	External-switch-Linux-Server	External-switch-Linux-Server (VNC)	alzaytse@cisco.com	No	Yes	...

View Full Auditing Info
View Inline Recording
Download Inline Recording

Pulling it all
together

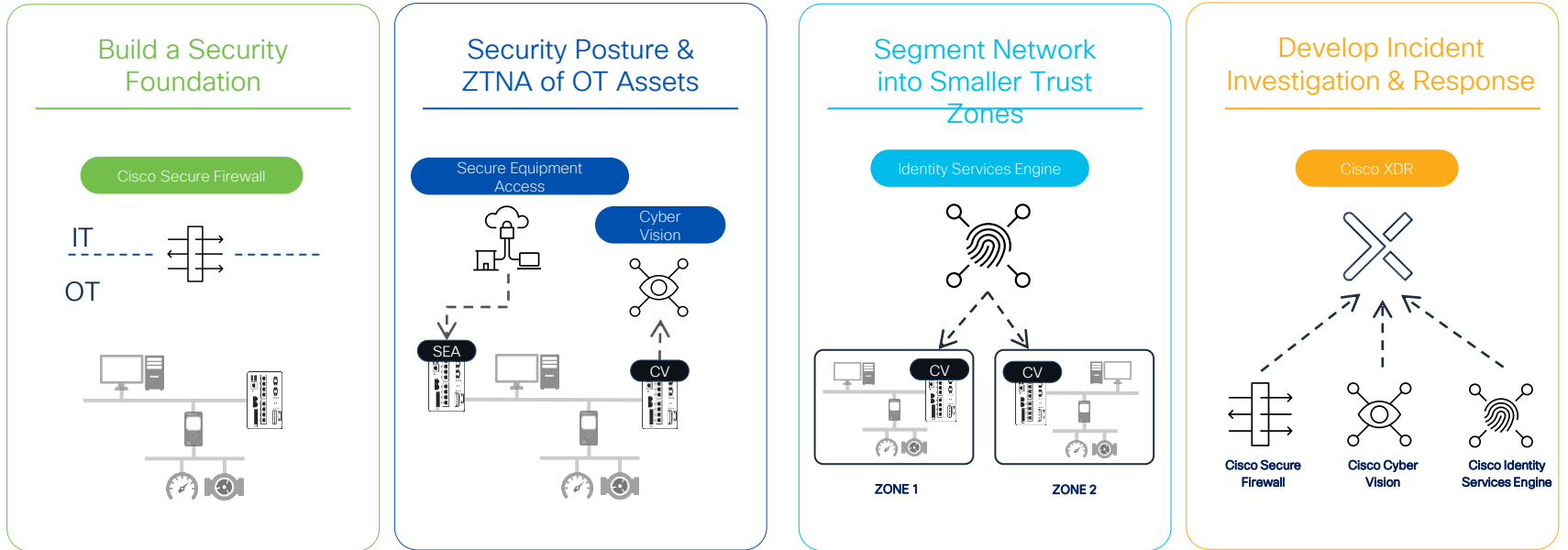


Let's put everything together



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 Cisco XDR and SOC** tools
8. Users can **trigger quarantine** of offending asset.

Cisco's Industrial Security Journey



Talos Threat Intelligence

+



Talos Incident Response

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



The bridge to possible

Thank you

CISCO *Live!*

The Cisco Live! logo features the word "CISCO" in a bold, black, sans-serif font, followed by "Live!" in a black, cursive script font. The background of the entire image is a vibrant, multi-colored abstract pattern of overlapping, wavy bands in shades of red, orange, yellow, green, and blue, creating a sense of motion and energy.

CISCO *Live!*

Let's go