
cisco Live!
Let's go

The bridge to possible

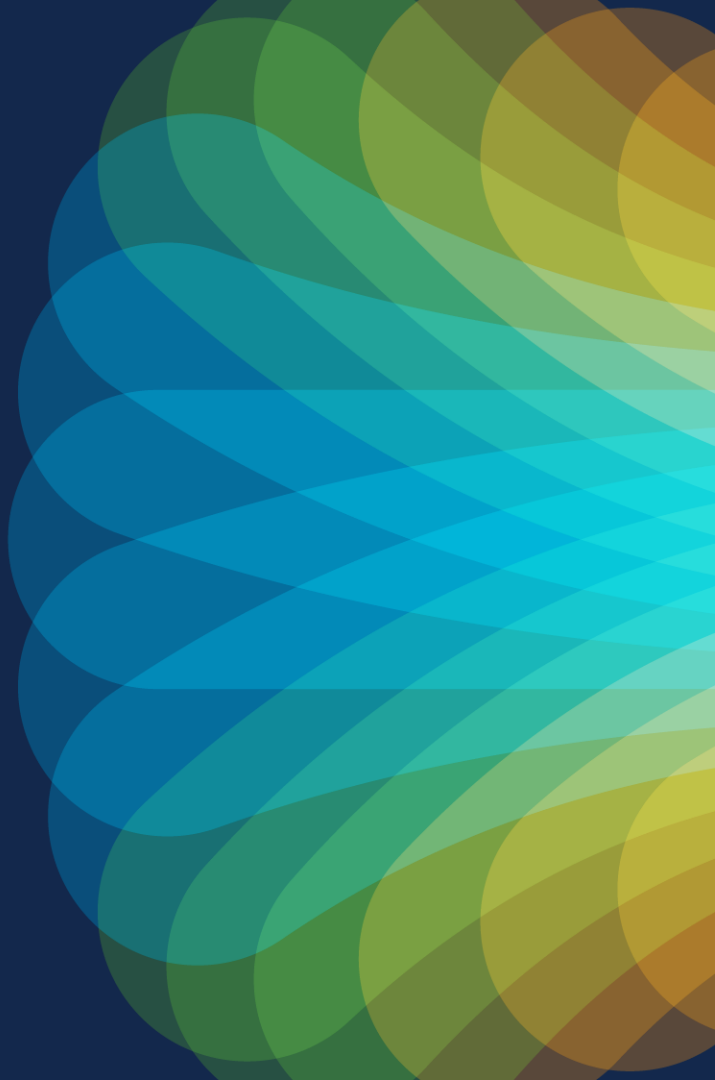
Implementing Segmentation in Industrial Networks

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

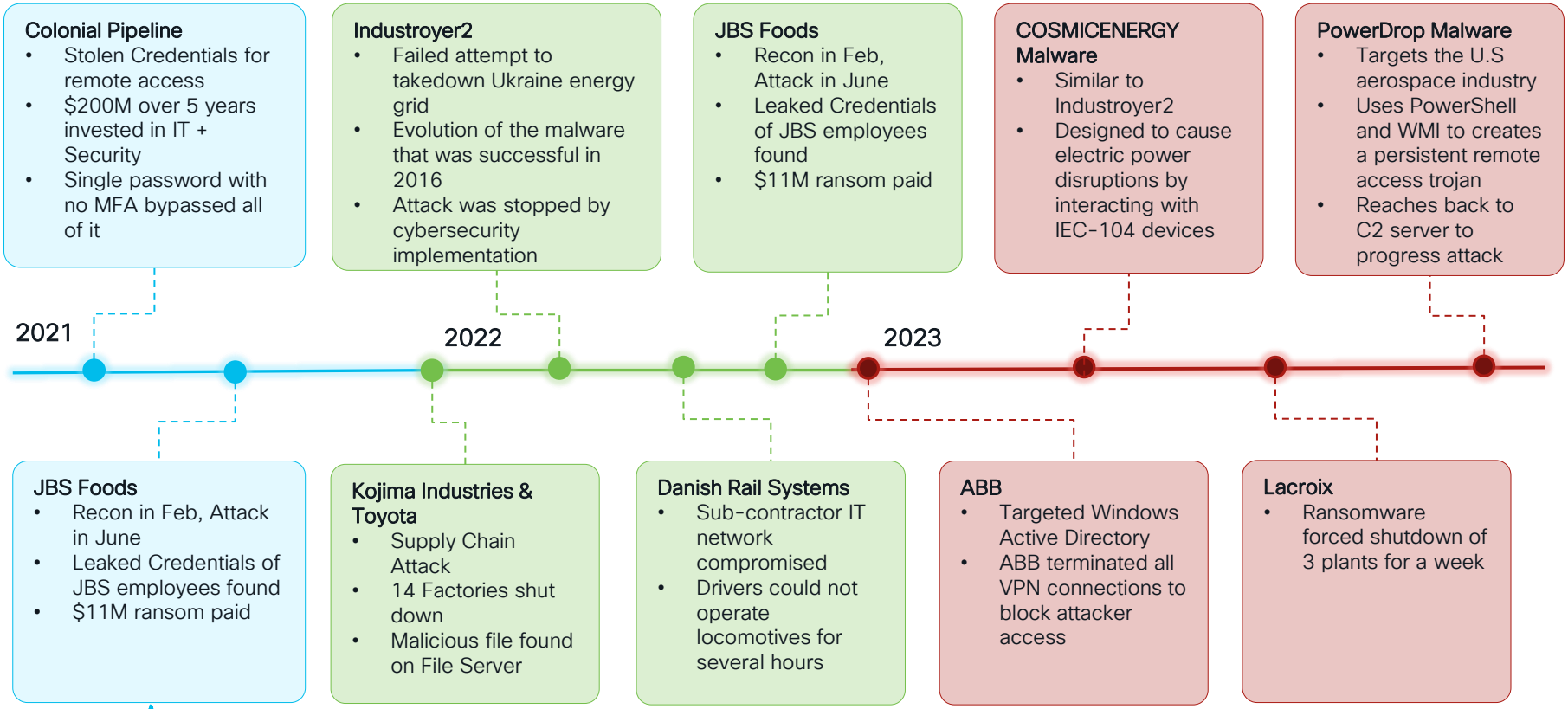
What do we mean by Industrial Security?

TSA definition of a Critical Cyber System

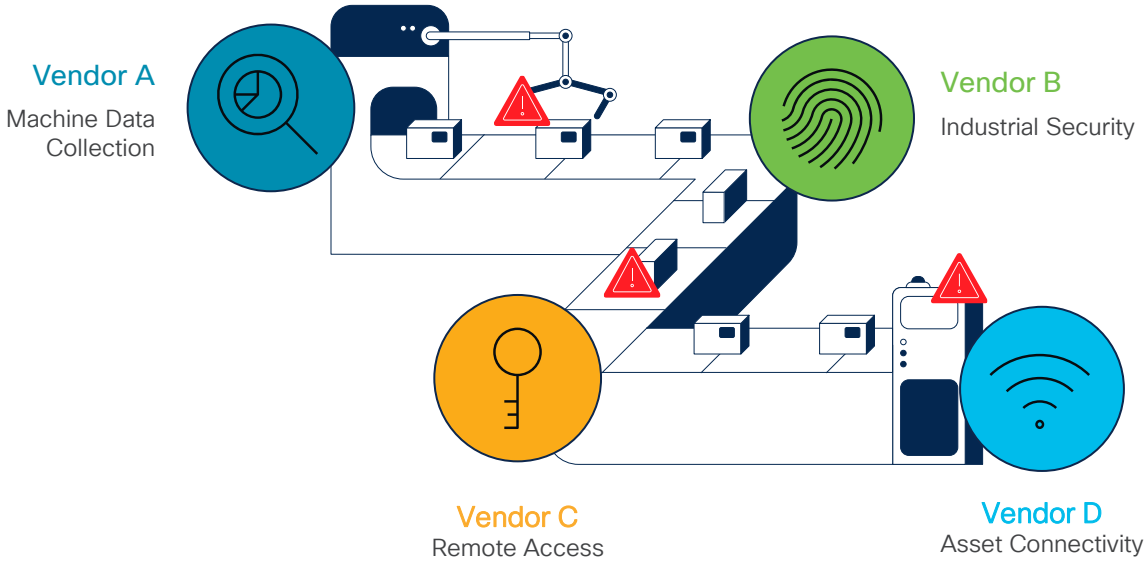
"Critical Cyber System means any Information or Operational Technology system or data that, if compromised or exploited, could result in operational disruption. Critical Cyber Systems include those business services that, if compromised or exploited, could result in operational disruption."

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

Notable OT Cyber Incidents in Recent Years



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

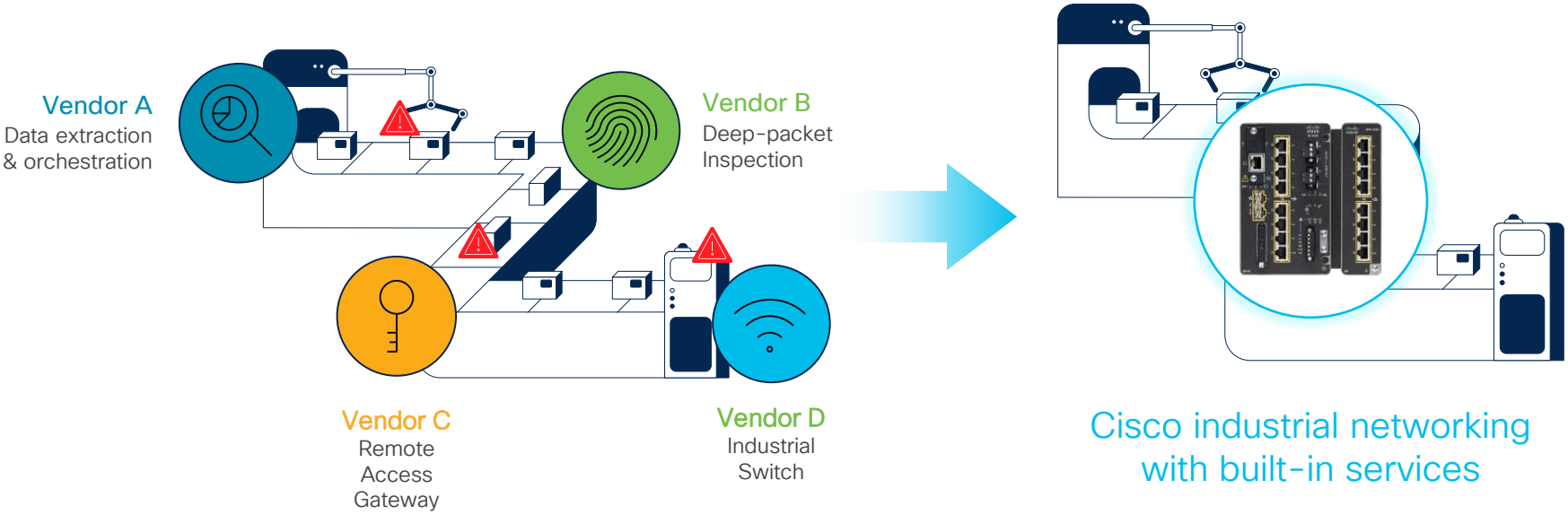


⚠ Shadow IT & Security Risk

⚠ Complexity

⚠ Hard to Scale

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

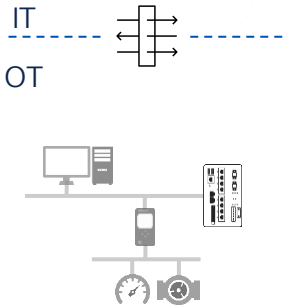


Eliminating complexity by converging functionality as software features on our industrial networking portfolio

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

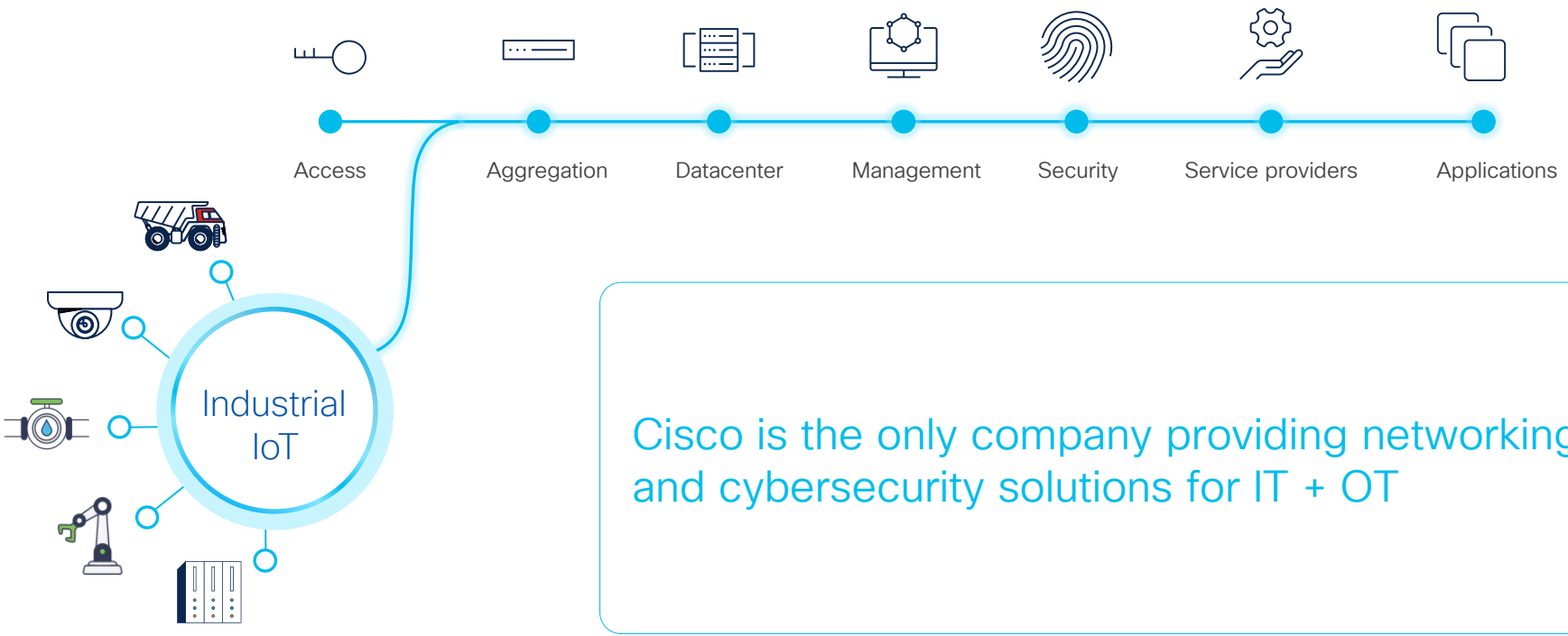
Identity Services Engine

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

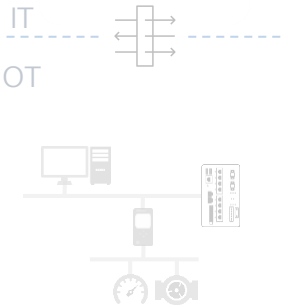


Cisco is the only company providing networking and cybersecurity solutions for IT + OT

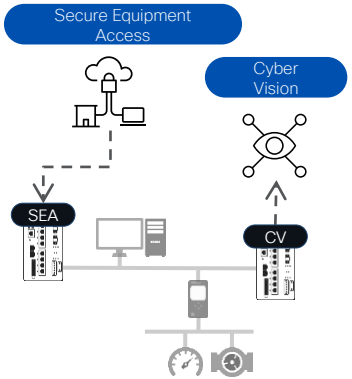
Focus on Today's Session – Segmentation within OT

Build a Security Foundation

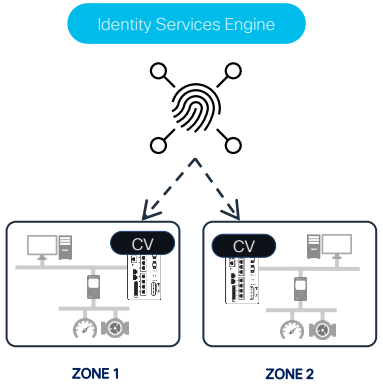
Cisco Industrial Networking



Security Posture & ZTNA of OT Assets



Segment Network into Smaller Trust Zones

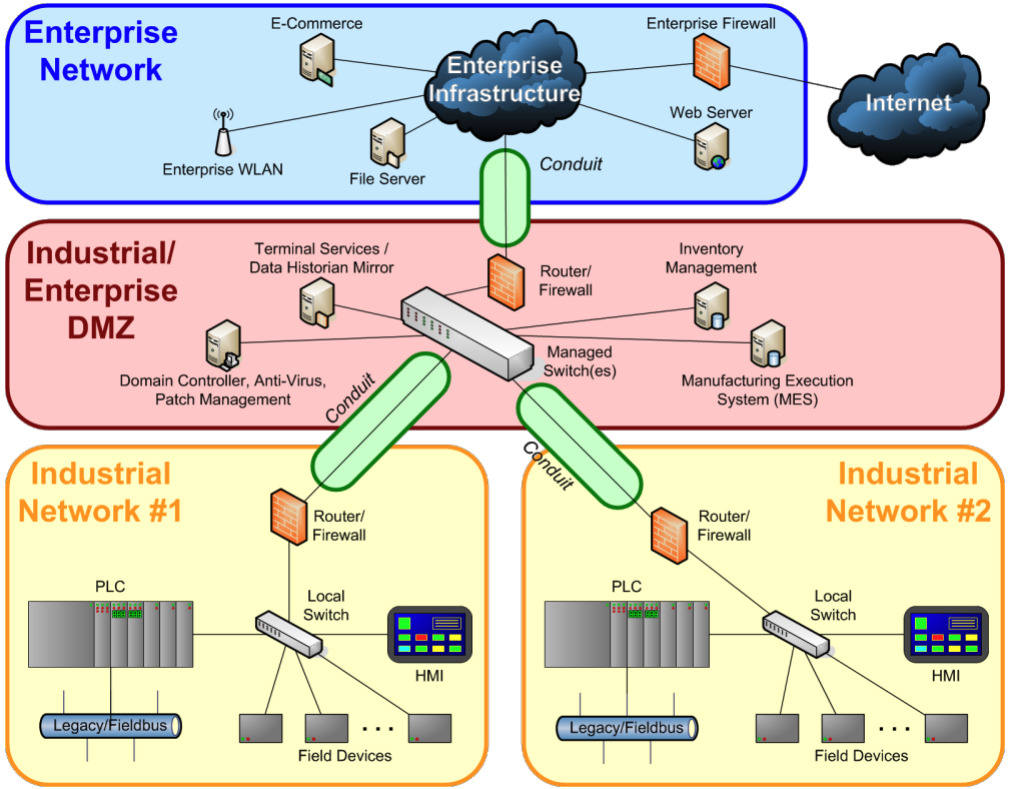


Develop Incident Investigation & Response

Talos Threat Intelligence + Talos Incident Response

ISA/IEC 62443 Zones & Conduits Model

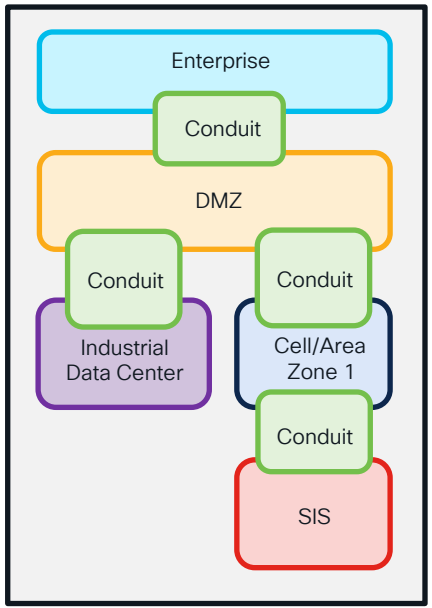
IEC 62443 Zones & Conduits



- **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

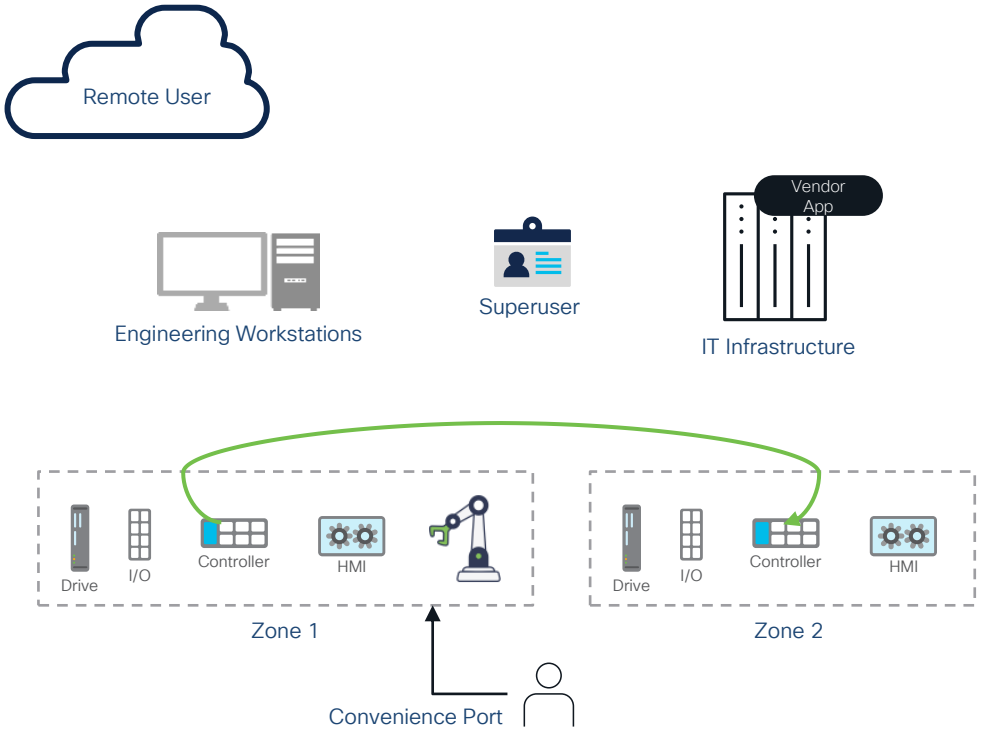
3.1.2 ZTA Using Micro-Segmentation

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



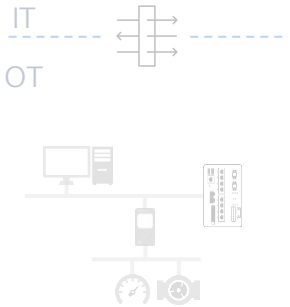
1. All devices within a zone can communicate freely
2. Deny by default across zone
3. Convenience Port within a zone
4. Engineering workstations to all devices within designated zones
5. Superusers – named employees to all devices
6. IT applications have restricted access to all zones
7. Vendor applications 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

Build a Security Foundation

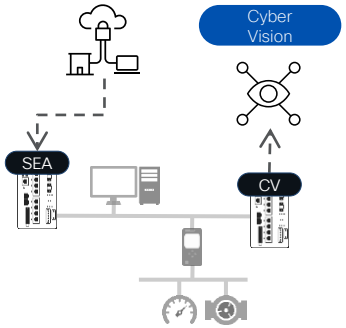
Cisco Industrial Networking



Security Posture & ZTNA of OT Assets

Secure Equipment Access

Cyber Vision



Segment Network into Smaller Trust Zones

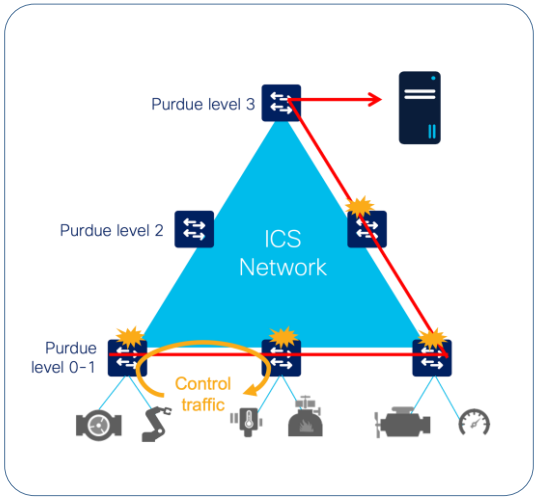
Identity Services Engine

Develop Incident Investigation & Response

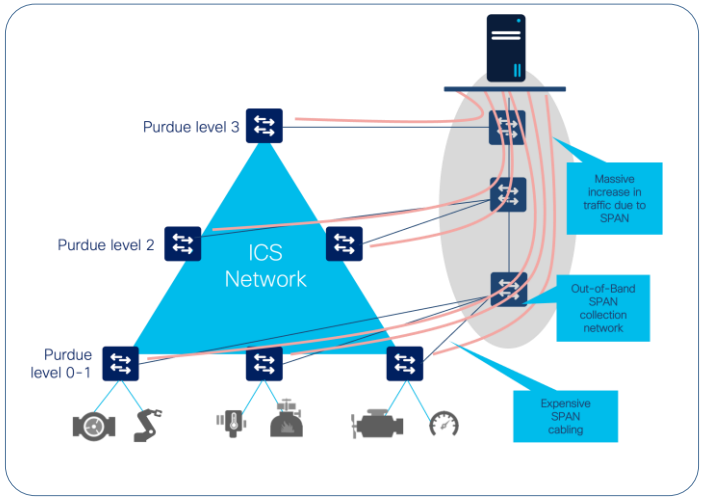
Cisco XDR

Talos Threat Intelligence + Talos Incident Response

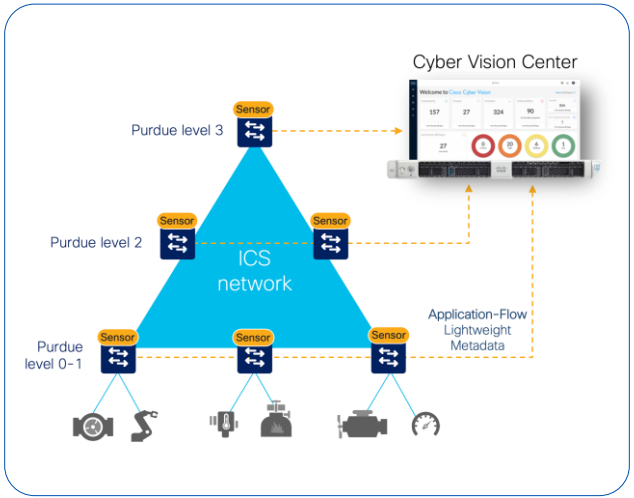
Leverage the network as a sensor to lower cost and complexity



RSPAN introduces Jitter



Out-of-Band SPAN is expensive



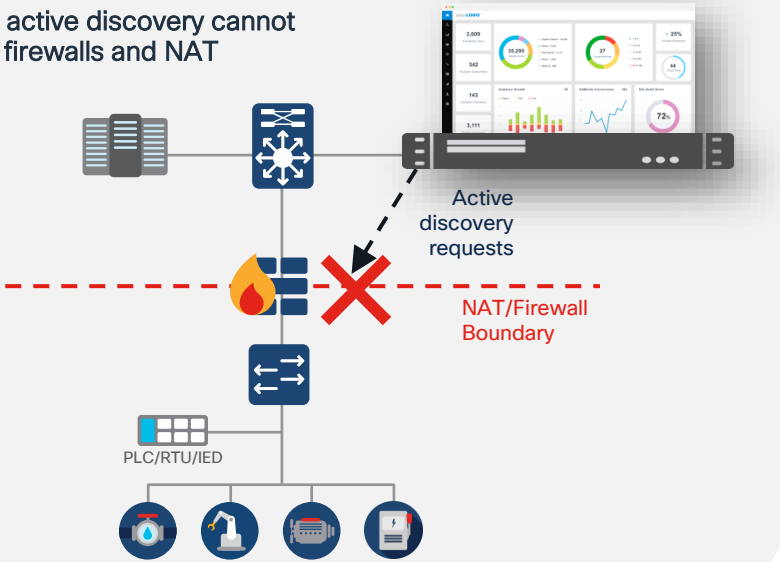
Network sensors scale without SPAN

Why is a network-sensor important?

Distributed edge active discovery gives you 100% visibility

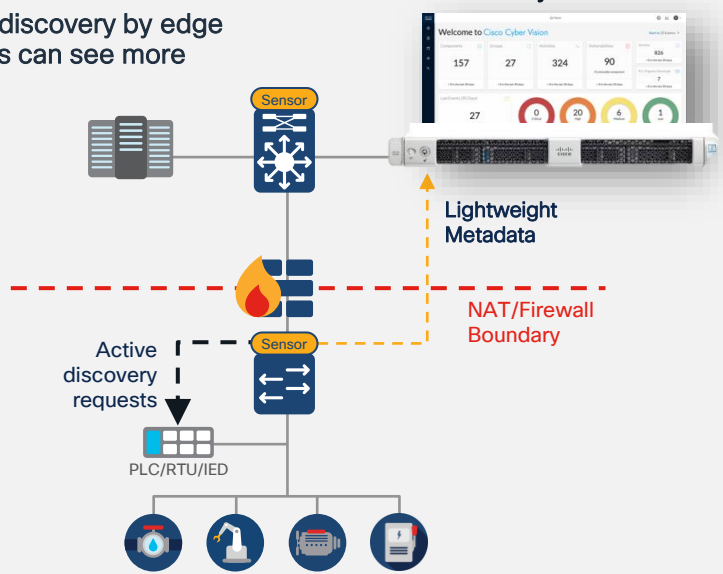
Other solutions

Centralized active discovery cannot see behind firewalls and NAT boundaries



Cisco Cyber Vision

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

Catalyst 9300/9400 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

Cisco Cyber Vision

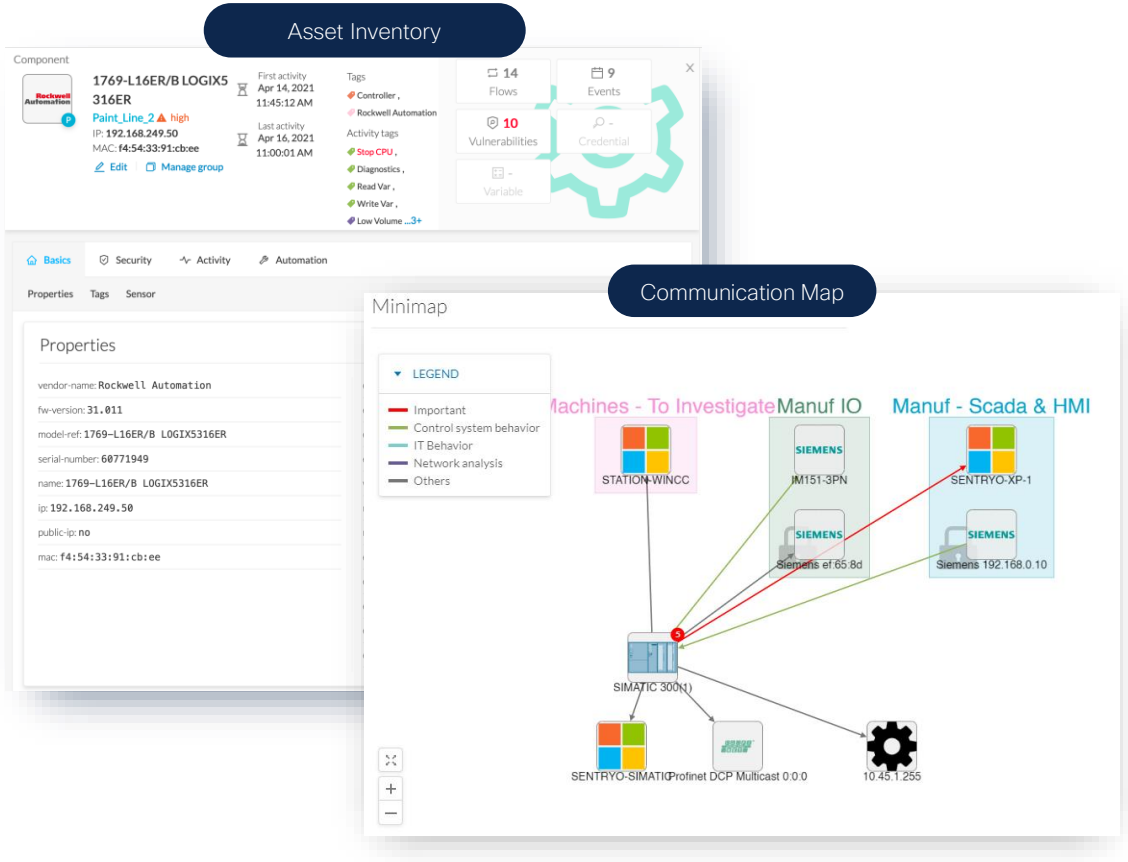
Asset Inventory

Comprehensive up to date inventory of all assets in your environment

Communication Patterns

Dynamic communication map with detailed application flow level information

Asset Visibility



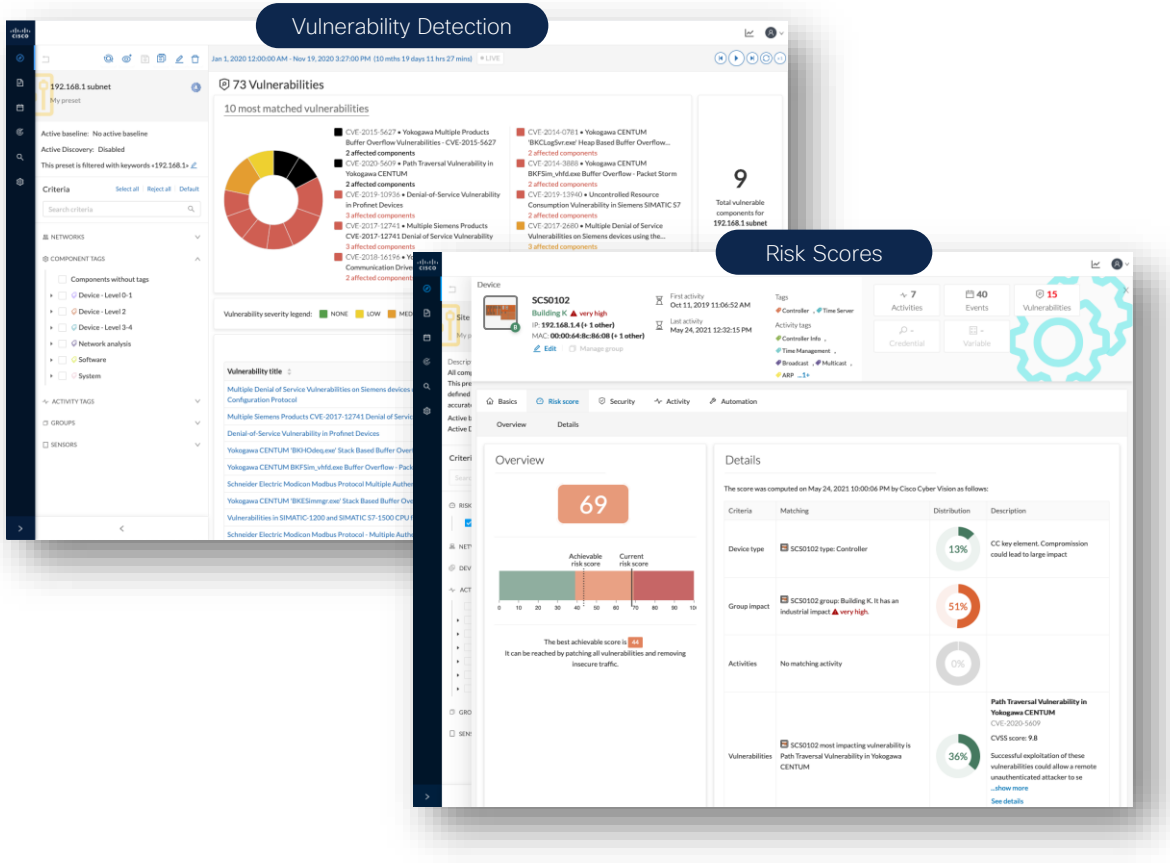
Security Posture

Vulnerability Detection

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

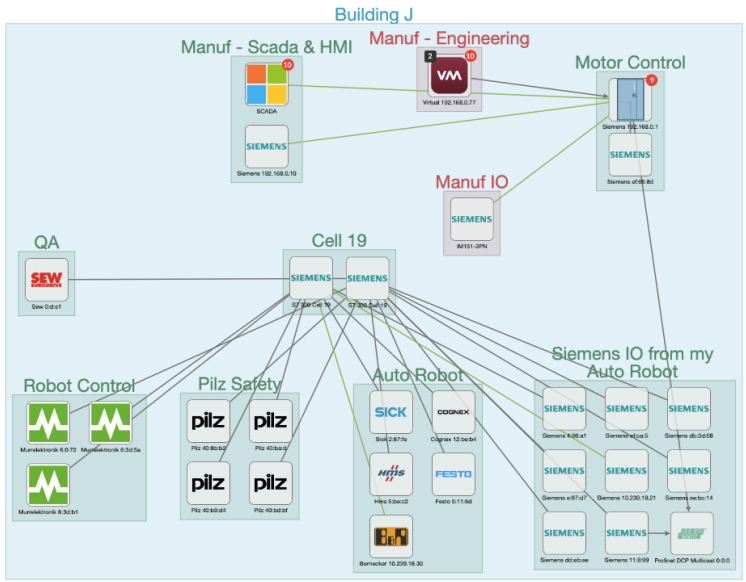
Risk Scoring

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



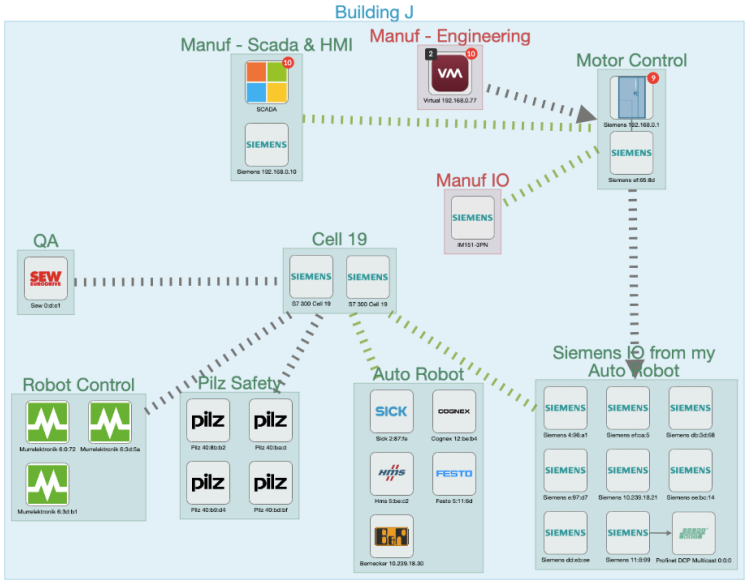
Aggregated activities match IEC62443 conduits

Unaggregated



View all asset relationships

Aggregated

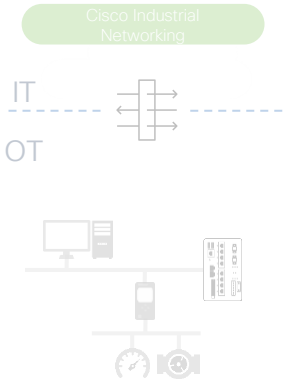


Easily browse through conduits

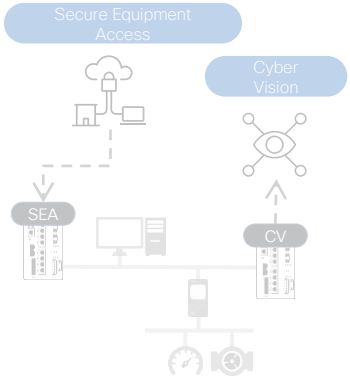
Implementing the Zones & Conduits Model

Using the Network as the Policy Enforcement Point

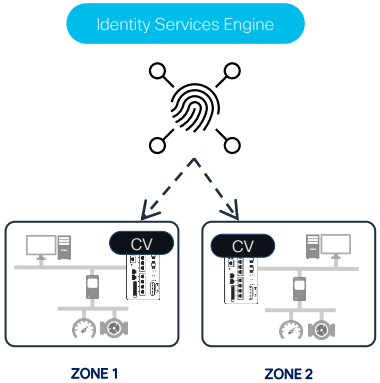
Build a Security Foundation



Security Posture & ZTNA of OT Assets



Segment Network into Smaller Trust Zones



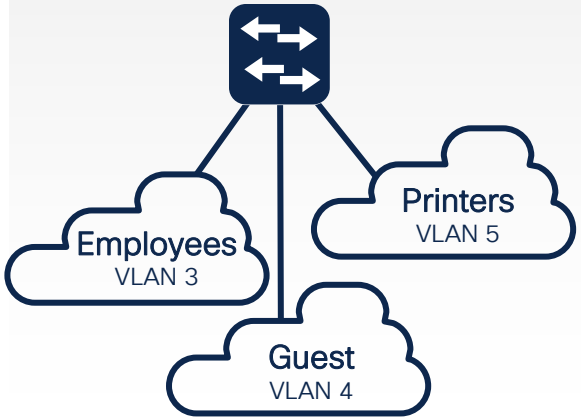
Develop Incident Investigation & Response

Talos Threat Intelligence + Talos Incident Response

ISE Segmentation Technologies

VLANs

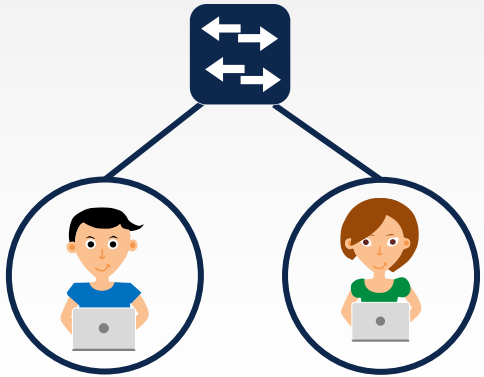
Dynamic VLAN Assignments



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`

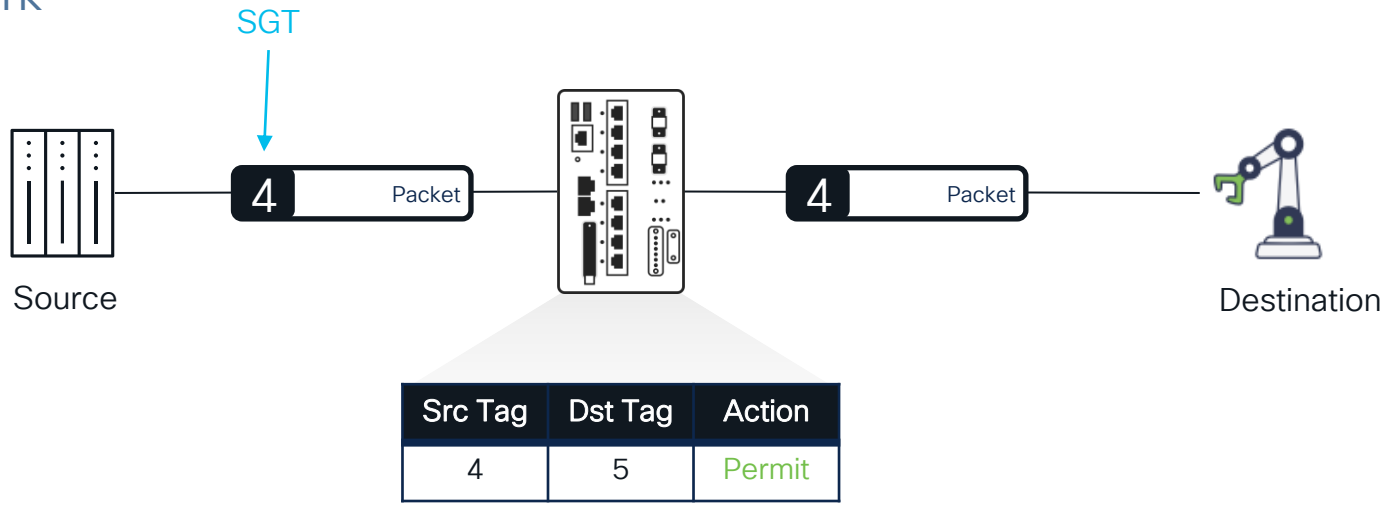
Security Group Tags

Cisco Group-Based Policy

16-bit SGT assignment and
SGT based Access Control

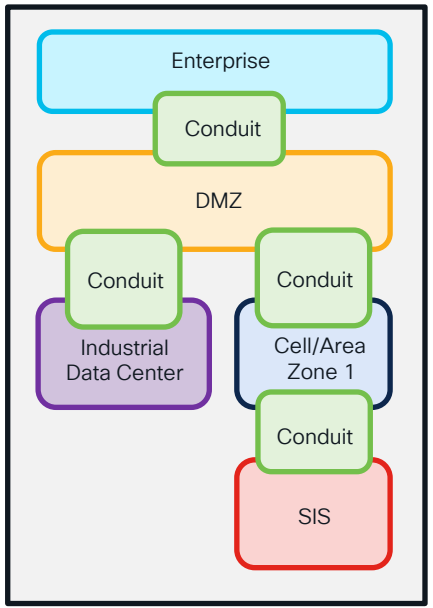
What are Security Group Tags (SGTs)?

Role Based Access Control embedded in the network



Zones & Conduits with SGTs

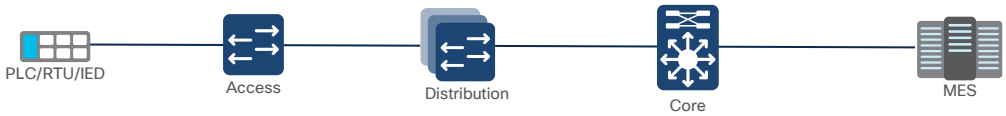
ISA/IEC 62443



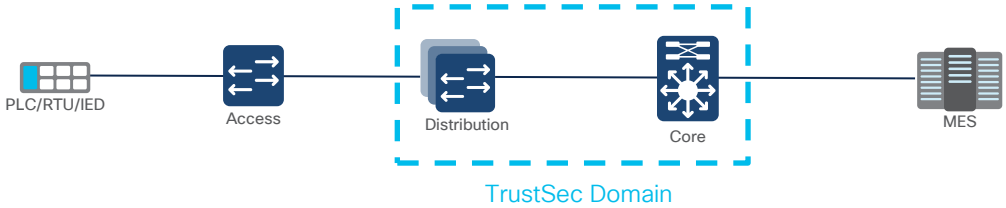
TrustSec Matrix

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

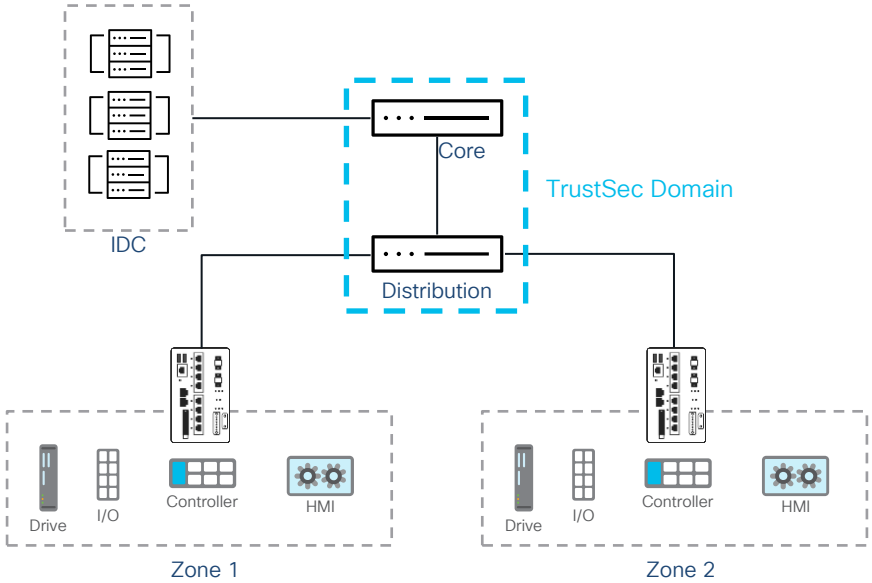
TrustSec Fundamentals



TrustSec Fundamentals – The TrustSec Domain

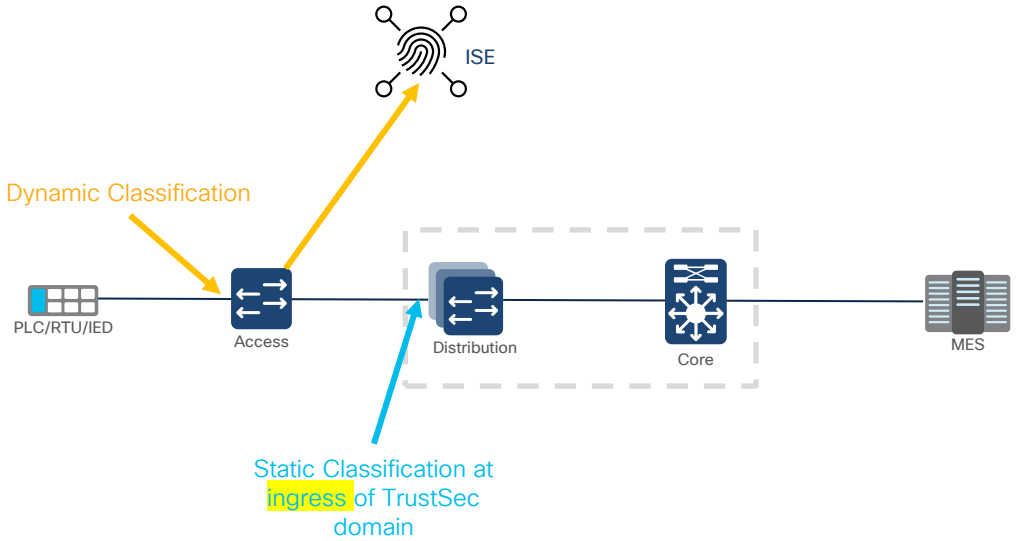


Use Case #1: All devices within a Zone should be able to communicate freely

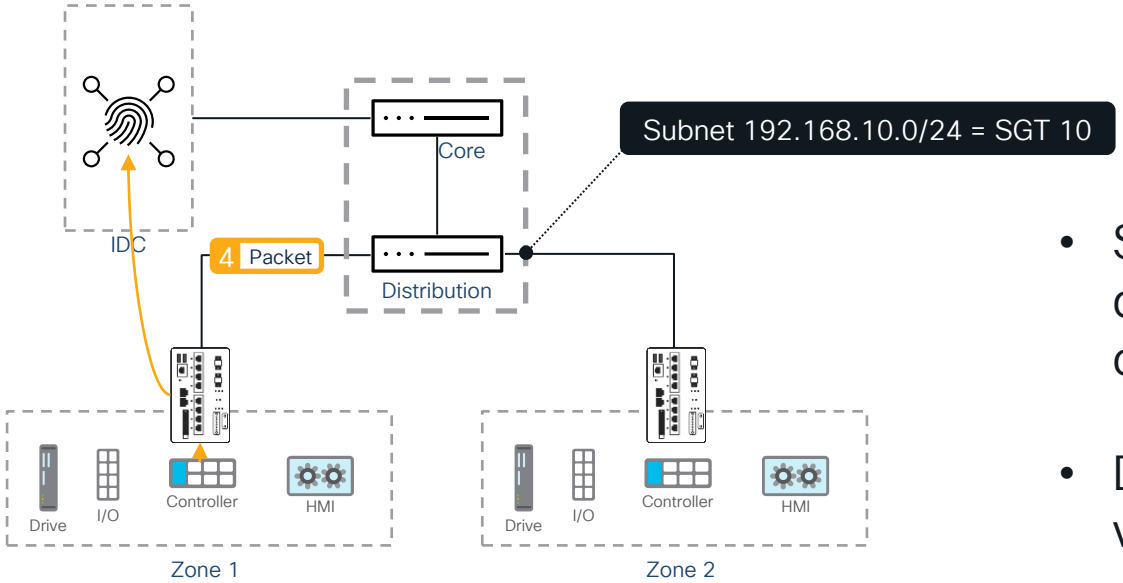


- If my TrustSec domain resides within a Cell/Area Zone, I must create policy to allow communication through the switches
  - More on this later!

TrustSec Fundamentals – Static & Dynamic Classification

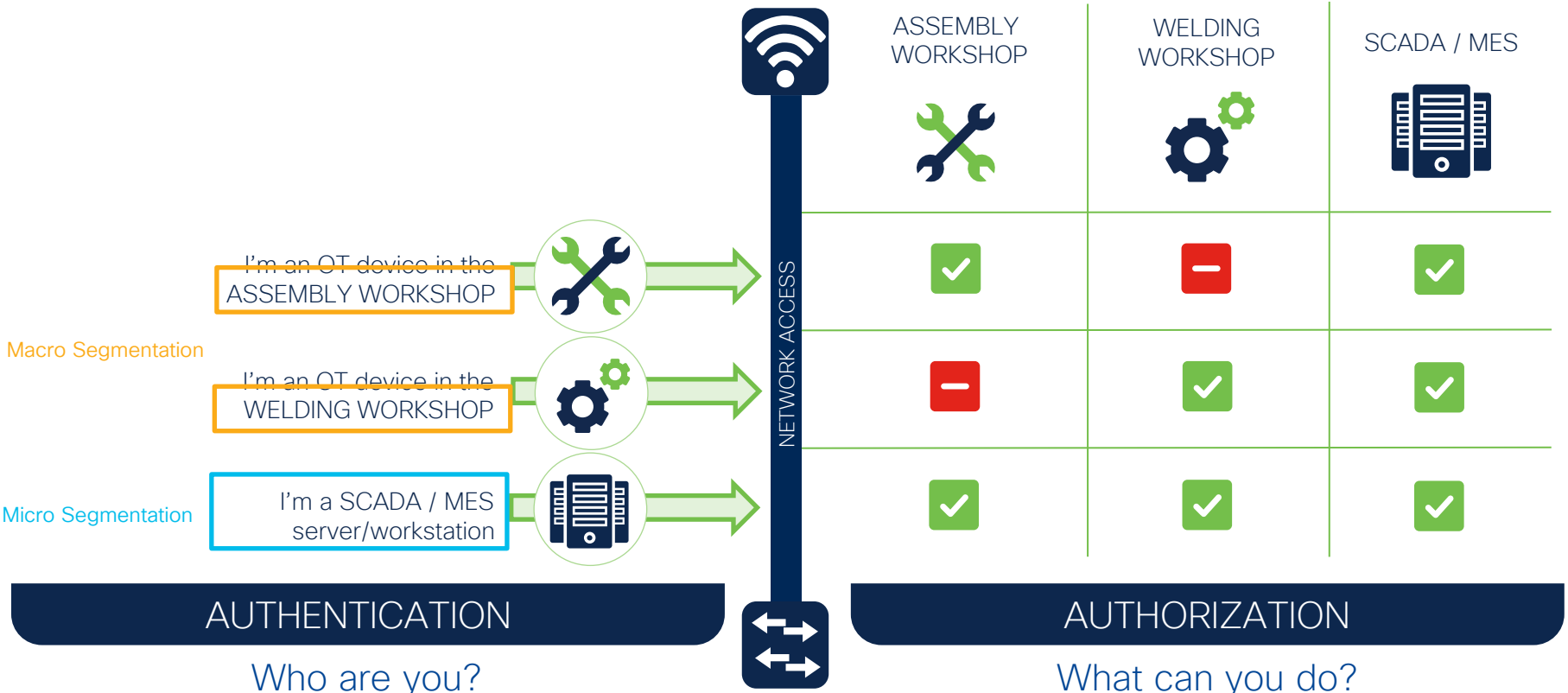


How do we classify an SGT?

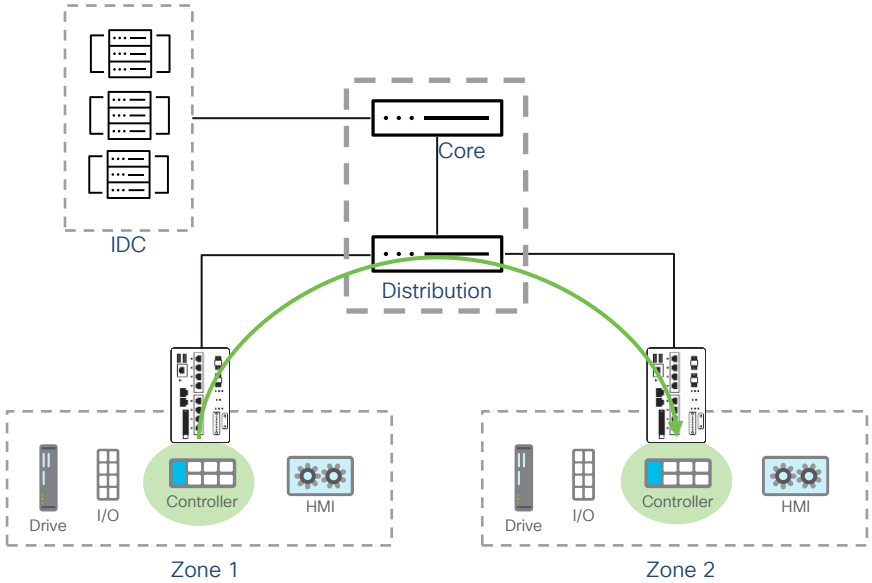


- Static Classification options:
  - VLAN to SGT
  - Subnet to SGT
  - IP to SGT
  - Interface to SGT
- Static classification can be done directly on a switch, or centrally in ISE
- Dynamic Classification is done via Authentication to ISE

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

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

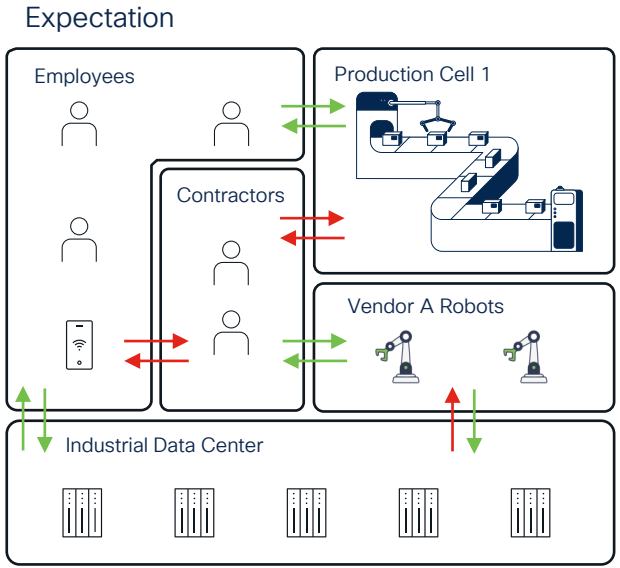
Endpoint authorized access based on least privilege

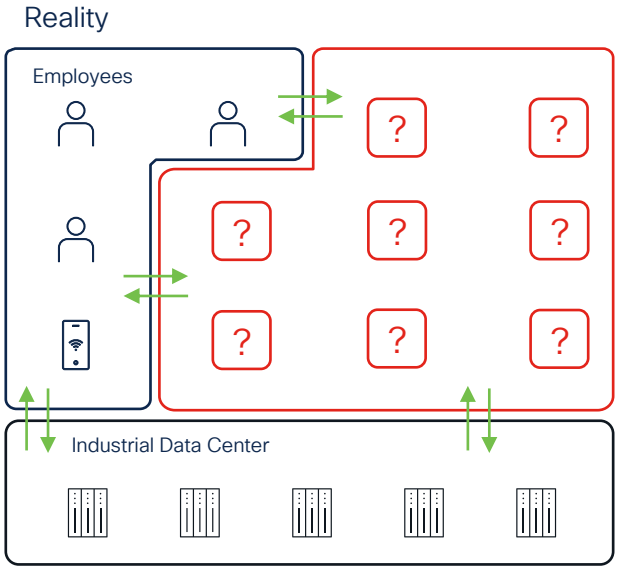
- Access granted
- Network segmentation achieved

Trust continually verified

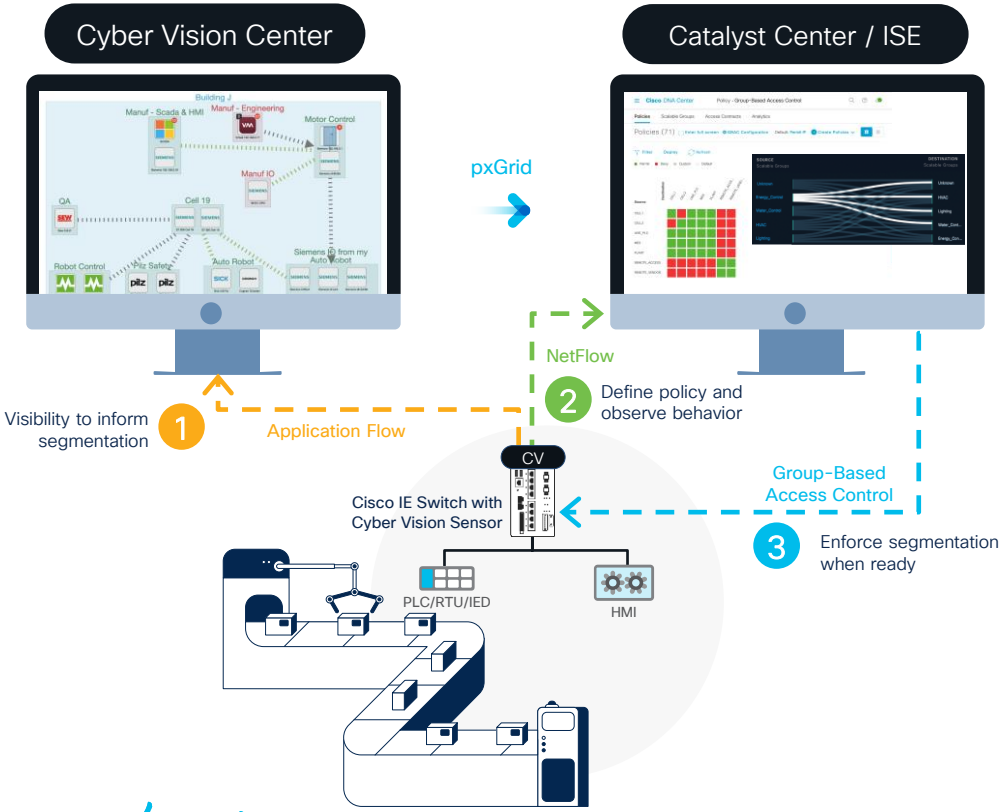
- Continually monitors and verifies endpoint trust level
- Vulnerability assessments to identify indicators of compromise
- Automatically Updates access policy

Least Privilege Access: Expectation vs. Reality





Use visibility to influence segmentation



Visualize Zones & Conduits

visualize aggregated flows as conduits to inform segmentation policy

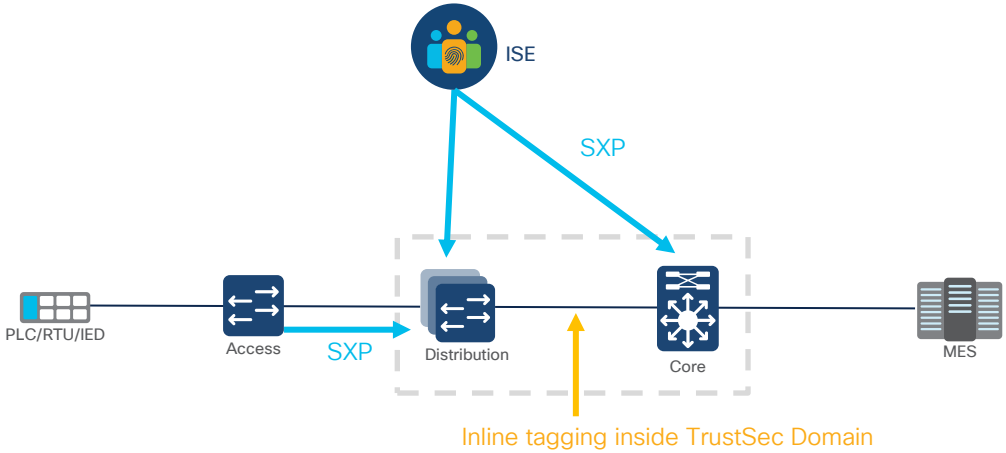
Dynamic SGT Mapping

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

Monitor Before Enforcement

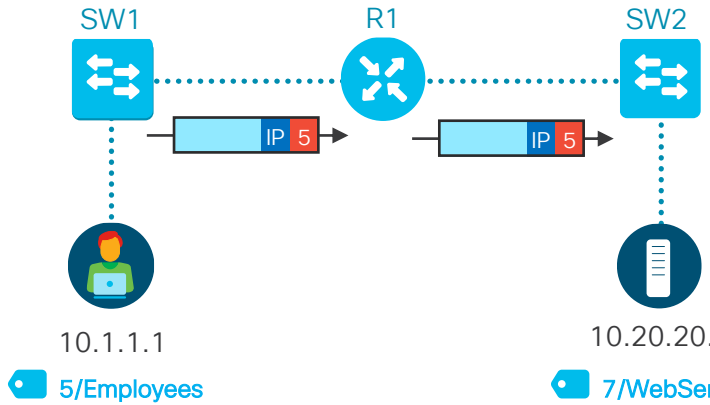
Visualize Group-based network behavior in Catalyst Center and enable enforcement when confident after monitoring

TrustSec Fundamentals – SXP & Inline Tagging



TrustSec Propogation

DATA PLANE PROPOGATION (INLINE TAGGING)

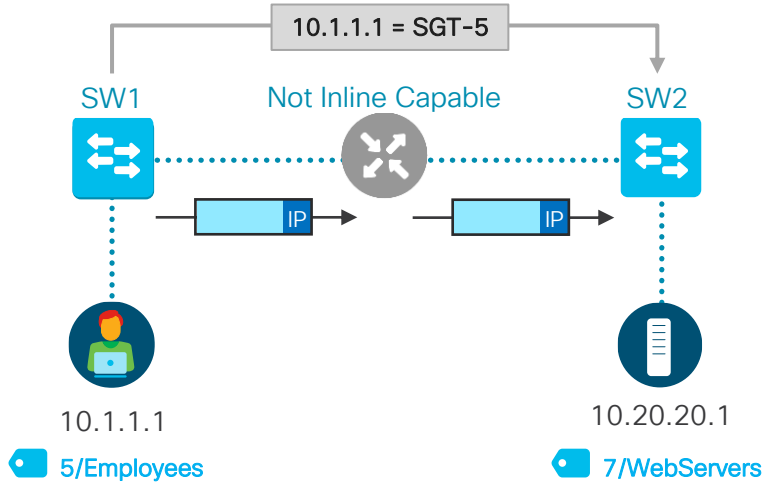


SGT carried inline in the data traffic. Methods include, SGT over:

Ethernet | MACSec | LISP/VxLAN

IPSec | DMVPN | GETVPN

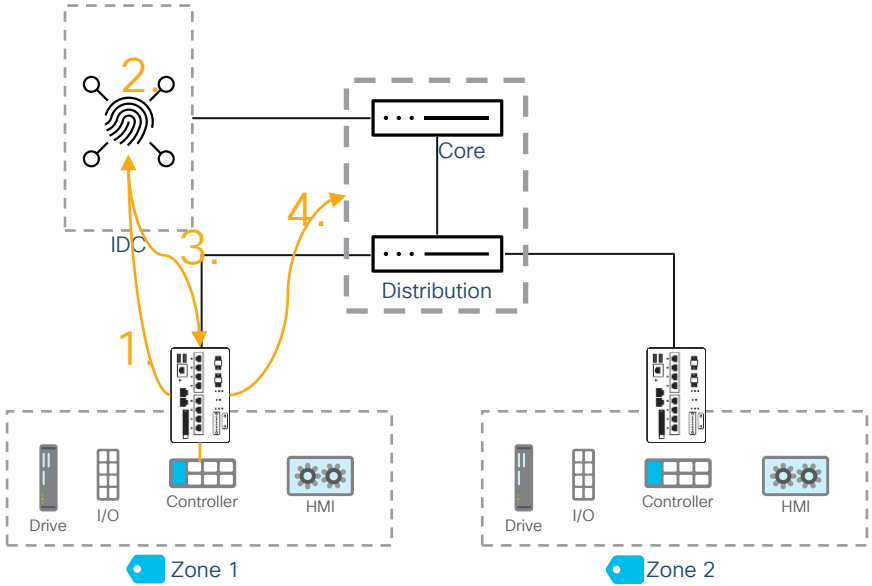
CONTROL PLANE PROPOGATION (SXP)



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

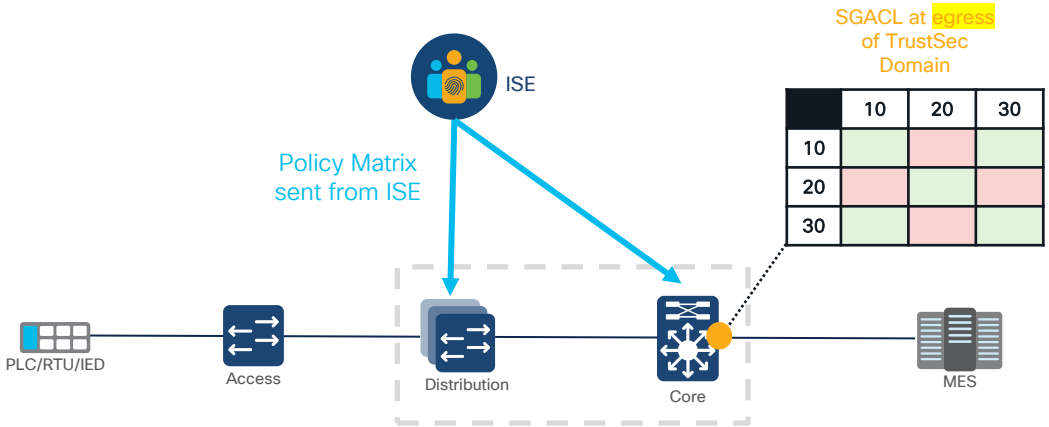
SXP | pxGrid

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	✓	✓	✓	✓

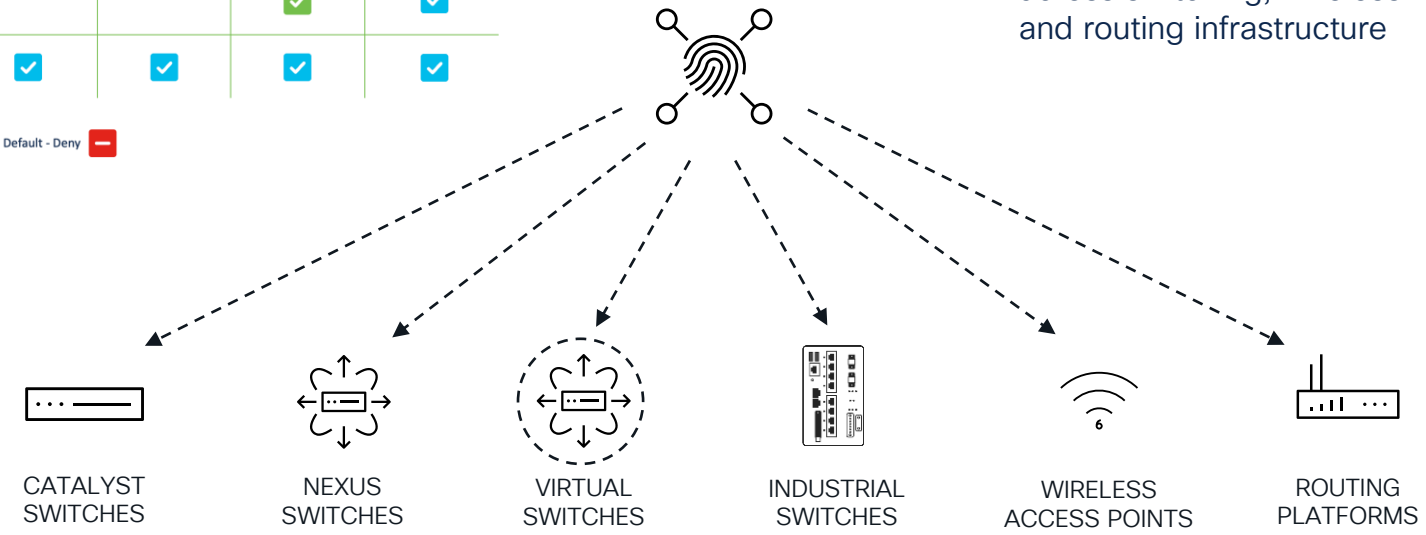
Default – Deny ⛔

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

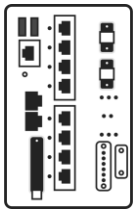


What Devices Support SGT Enforcement?

Enforcement Nodes: Can actively block traffic

Catalyst Switches

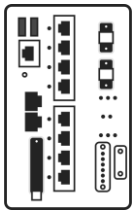
Typically used at the distribution & core



IE3400, IE9300 & IE4000

Typically used at access & aggregation

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



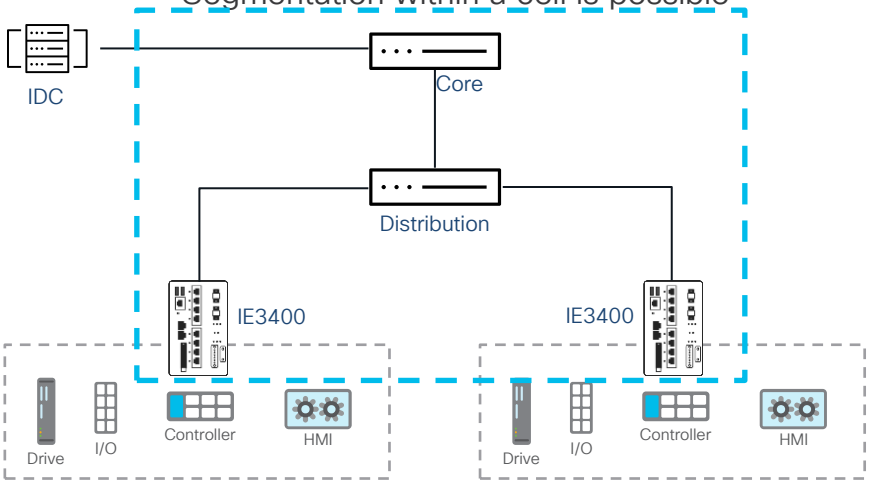
- IE3300
- IE3200
- IE3100
- IE2000

*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

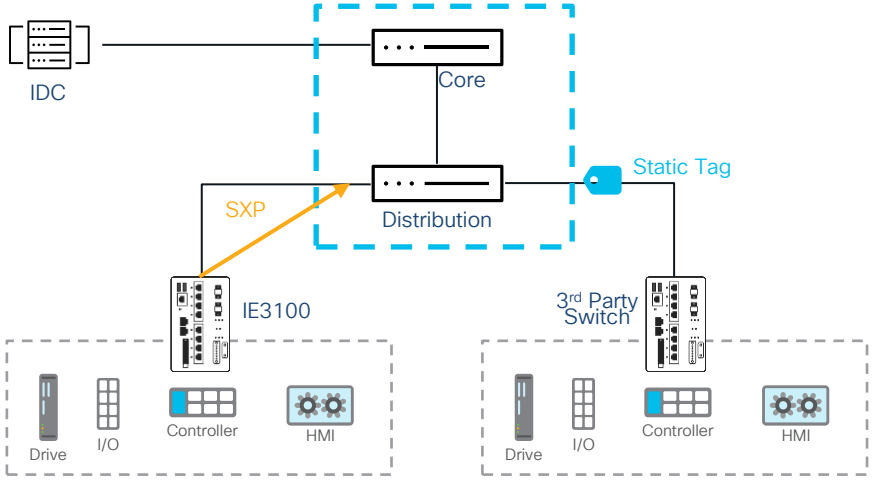
If all switches are capable of enforcement, my TrustSec domain can be everywhere

- Segmentation within a cell is possible

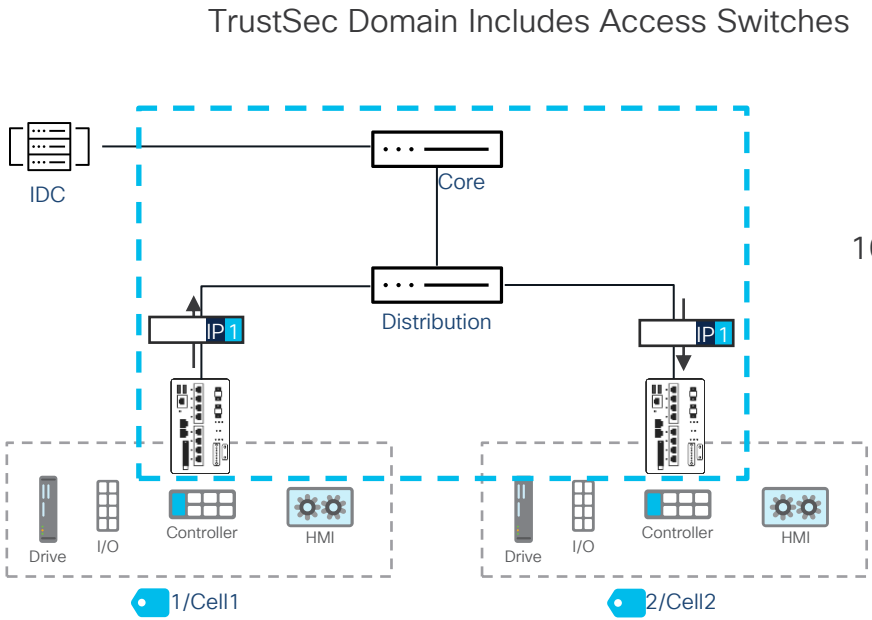


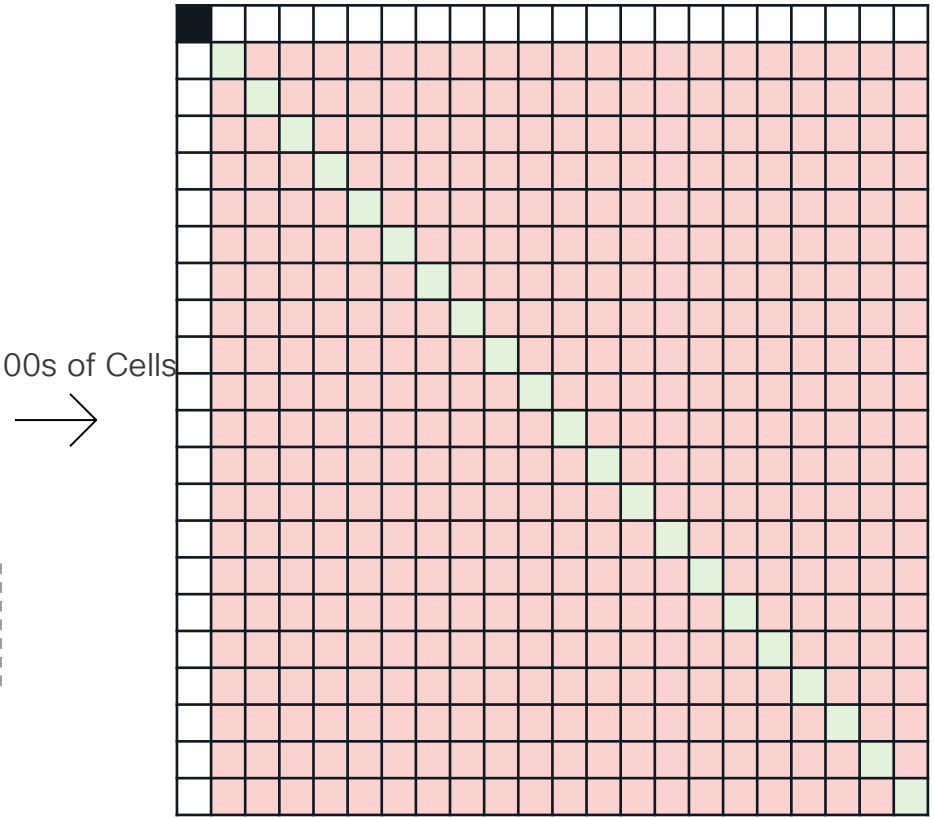
Not all switches need to be enforcement nodes to do TrustSec

- Segmentation between cells still possible

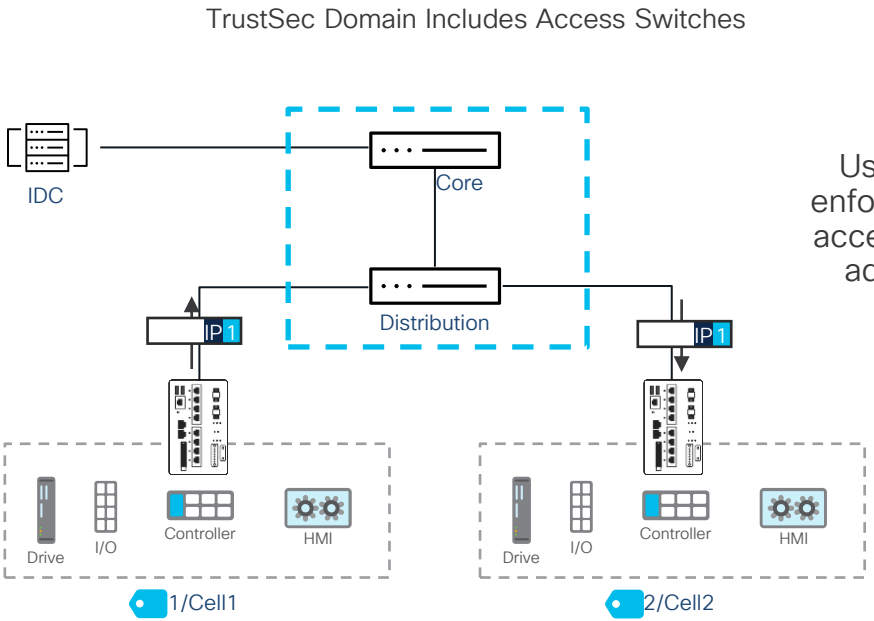


How the TrustSec domain enables you to reduce the number of policies in your network





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

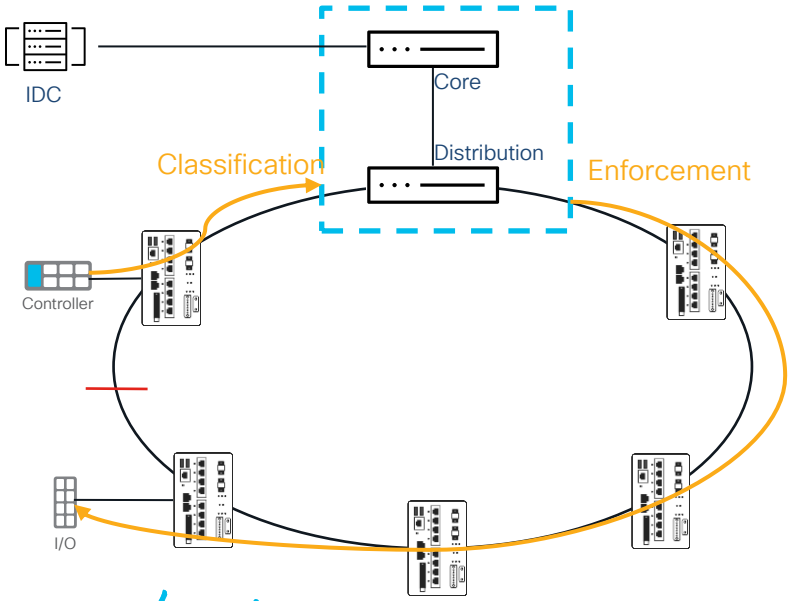


Use lack of enforcement in access to your advantage

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

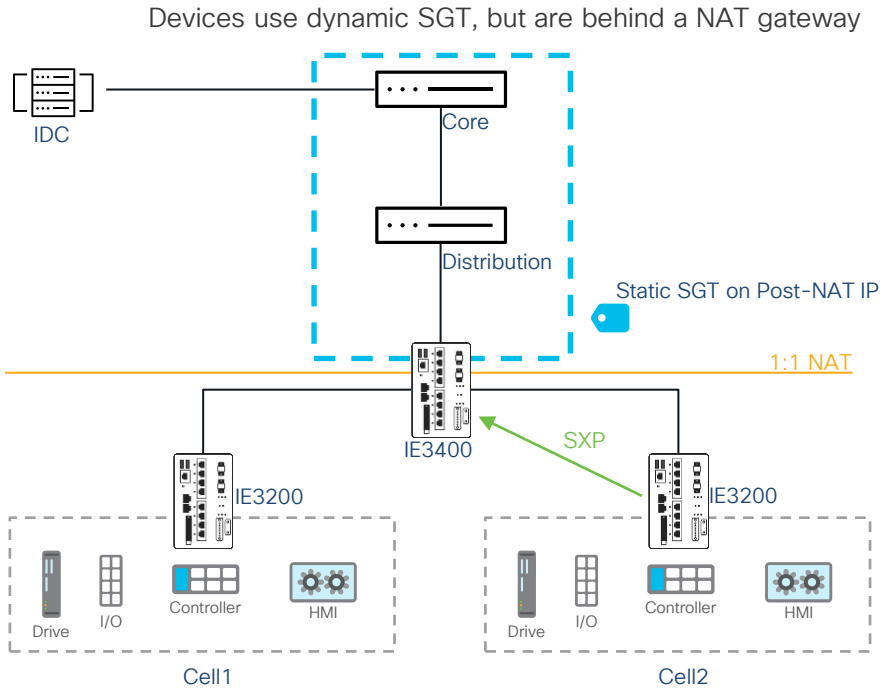
	Cell/Area Zones	Infrastructure Services
Cell/Area Zones		
Infrastructure Services		

How a ring topology effects your enforcement strategy



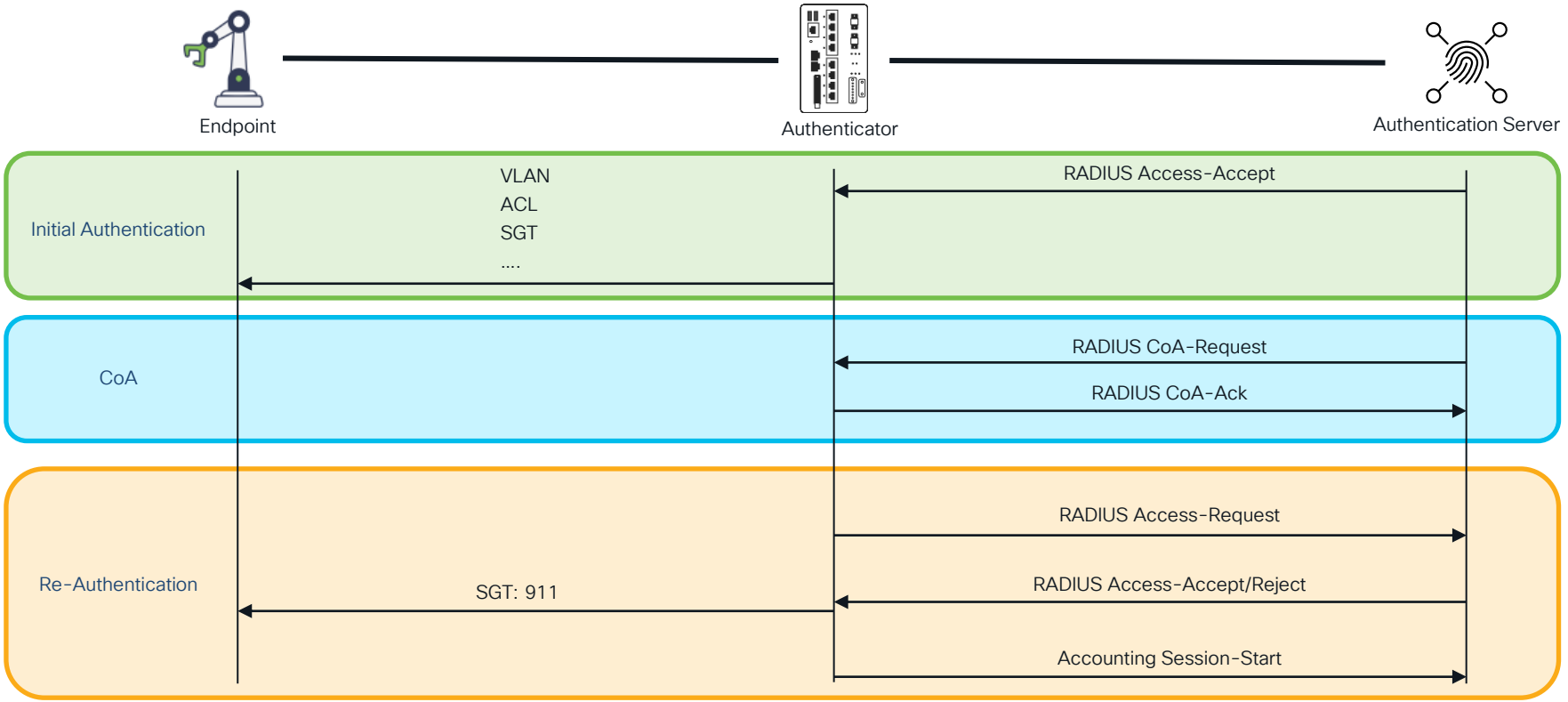
- In this case, aggregation of the SGT does NOT work
- TrustSec domain is part of the ring
- Each ring must have its own SGT so traffic can be permitted through

How L2NAT effects your enforcement strategy

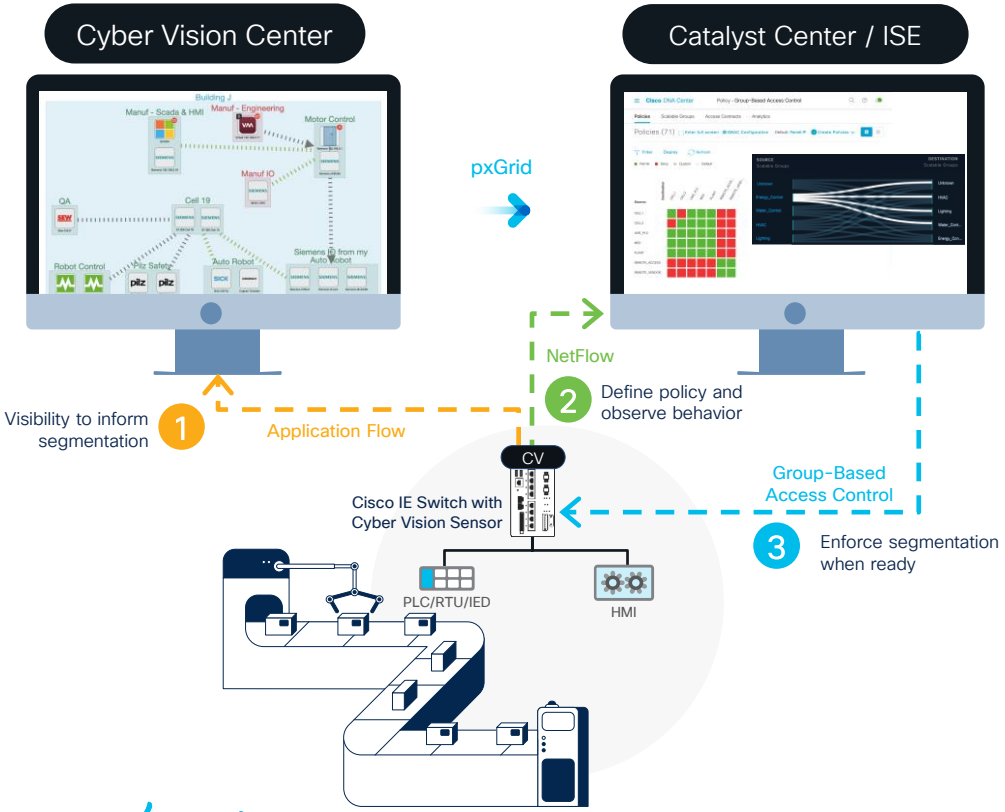


- **Problem Statement**: IP to SGT mapping will be on private IP address. This address does not exist in the TrustSec domain
- **Solution**: L2NAT Gateway is added to TrustSec Domain
  - Static SGT on Post-NAT IP
  - Dynamic SGT is shared to L2NAT device via SXP
  - L2NAT device does inline tagging on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

Change of Authorization (CoA)



Recap: Use visibility to influence segmentation



Visualize Zones & Conduits

visualize aggregated flows as conduits to inform segmentation policy

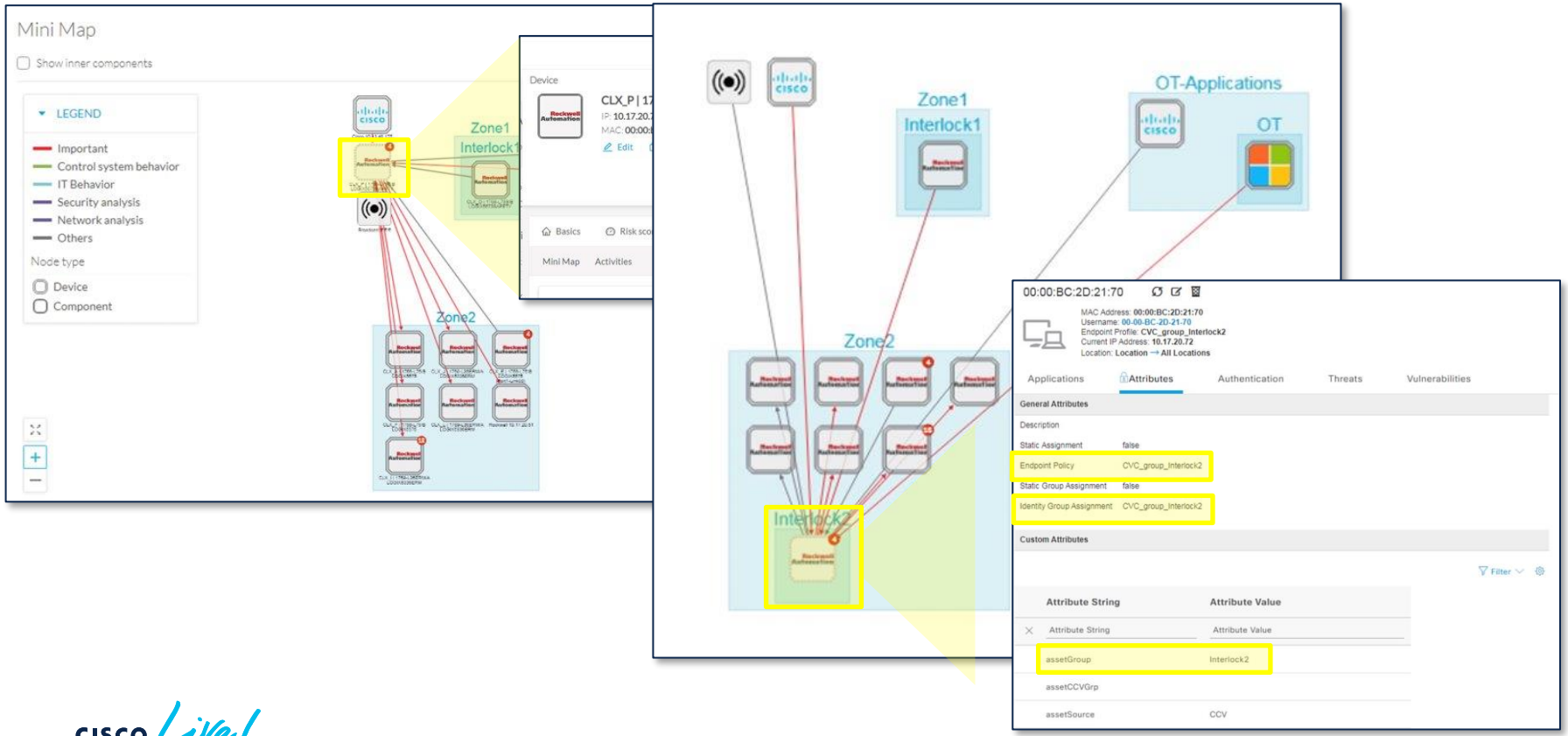
Dynamic SGT Mapping

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

Monitor Before Enforcement

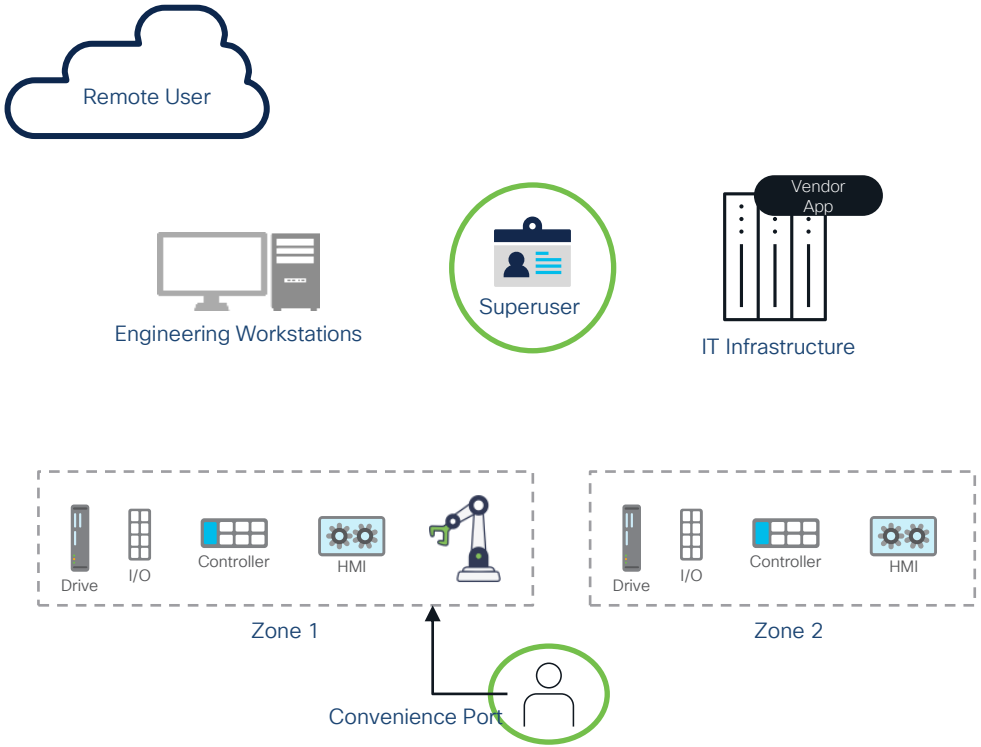
Visualize Group-based network behavior in Catalyst Center and enable enforcement when confident after monitoring

Using Cyber Vision to Initiate a CoA



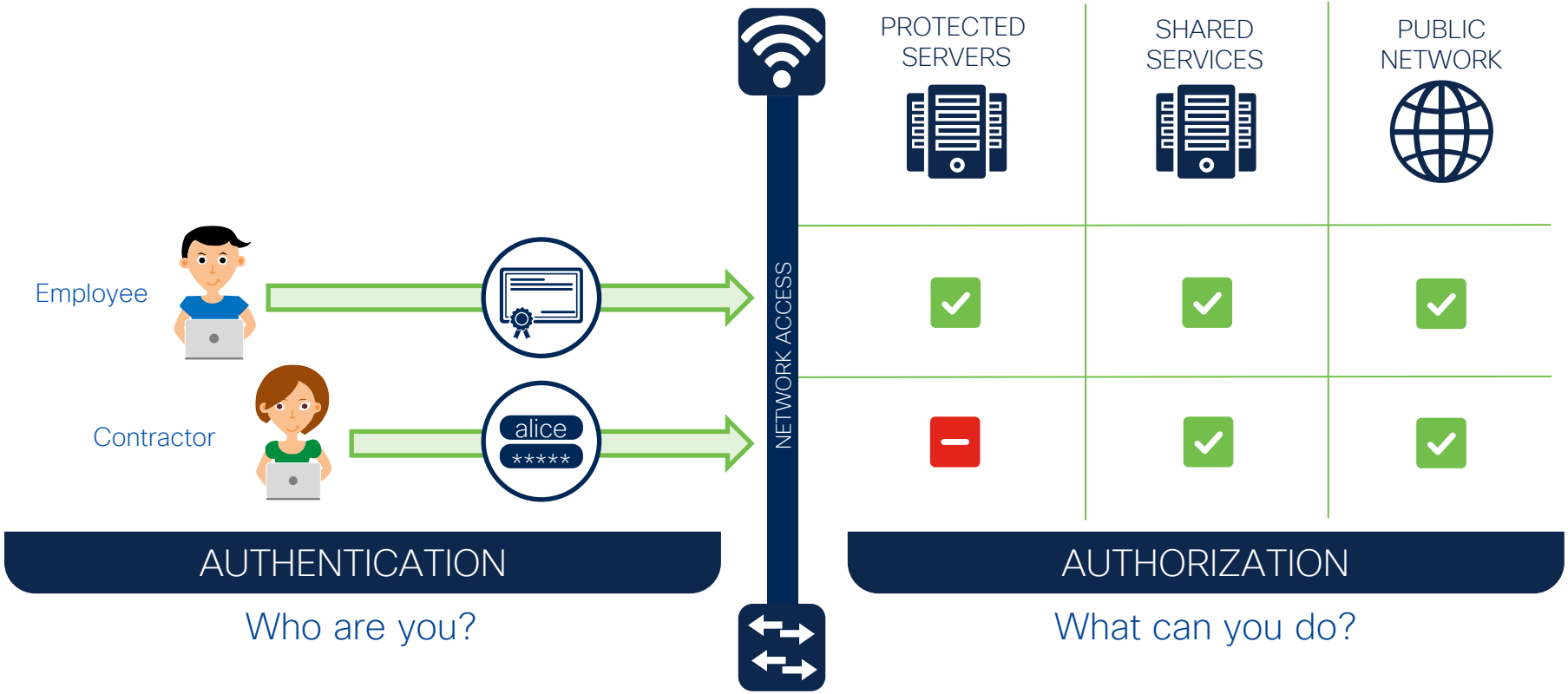
What about Users in OT networks?

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

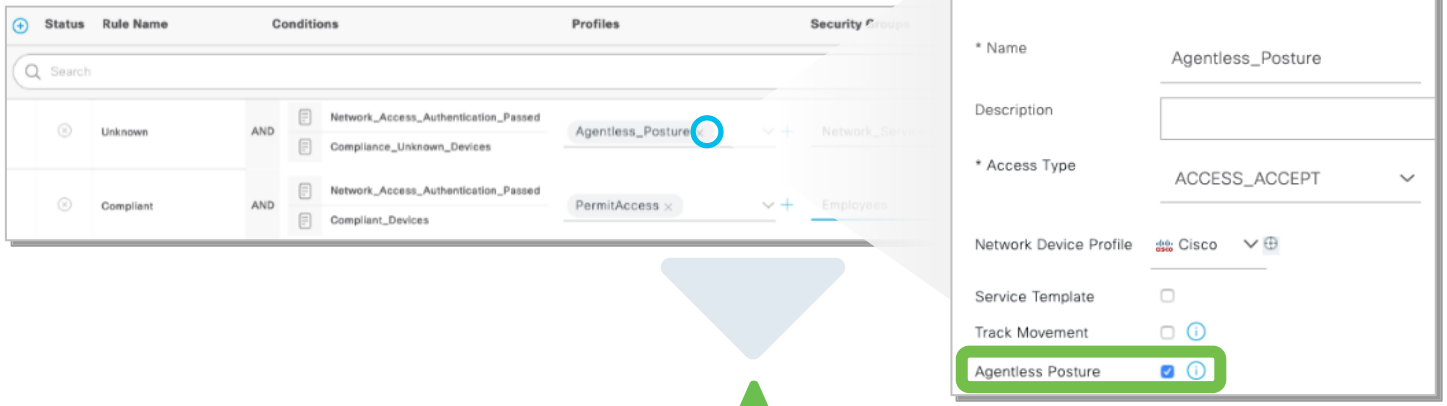


Posture & Compliance

MDM Attributes

ActivityType
AdminAction
AdminActionUUID
AnyConnectVersion
DaysSinceLastCheckin
DetailedInfo
DeviceID
DeviceName
DeviceType
DiskEncryption
EndPointMatchedProfile
FailureReason
IdentityGroup
IMEI
IpAddress
JailBroken
LastCheckInTimeStamp
MacAddress
Manufacturer
MDMCompliantStatus
MDMFailureReason
MDMServerName
MEID
Model
OperatingSystem
PhoneNumber
PinLock
PolicyMatched
RegisterStatus
SerialNumber
ServerType
SessionId
UDID
UserName
UserNotified

Agentless Posture

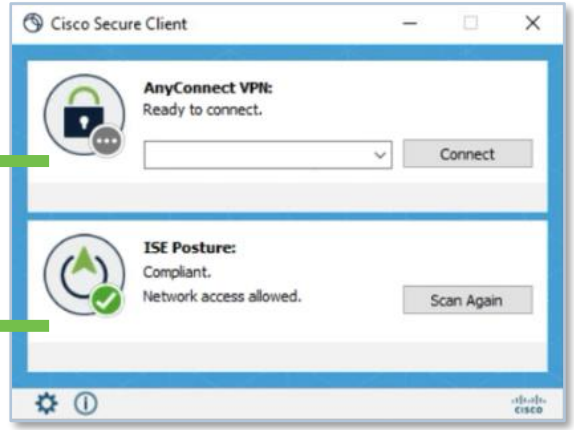


Linux Support added in ISE 3.1

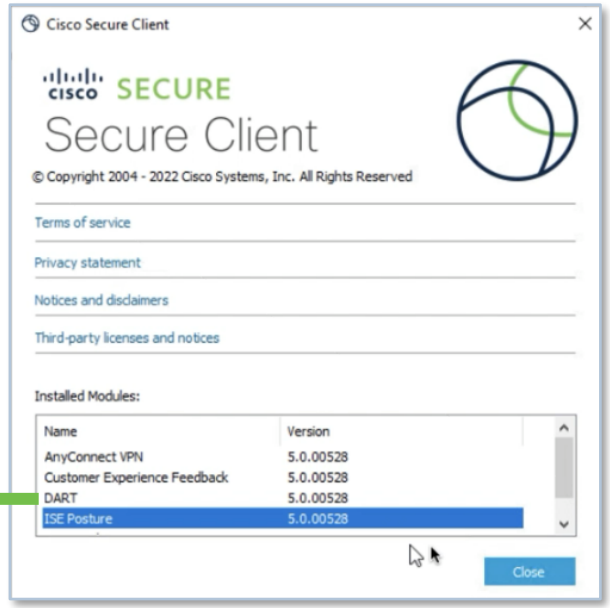
Cisco Secure Client (formerly AnyConnect)

VPN Module (Core)

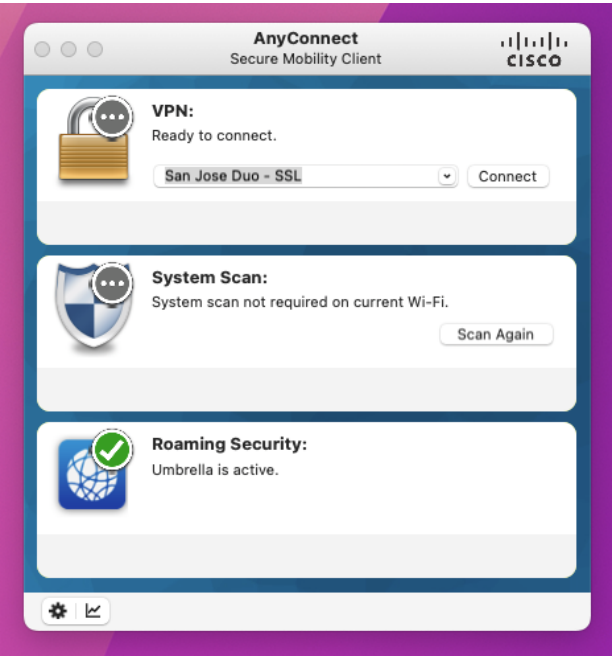
ISE Posture

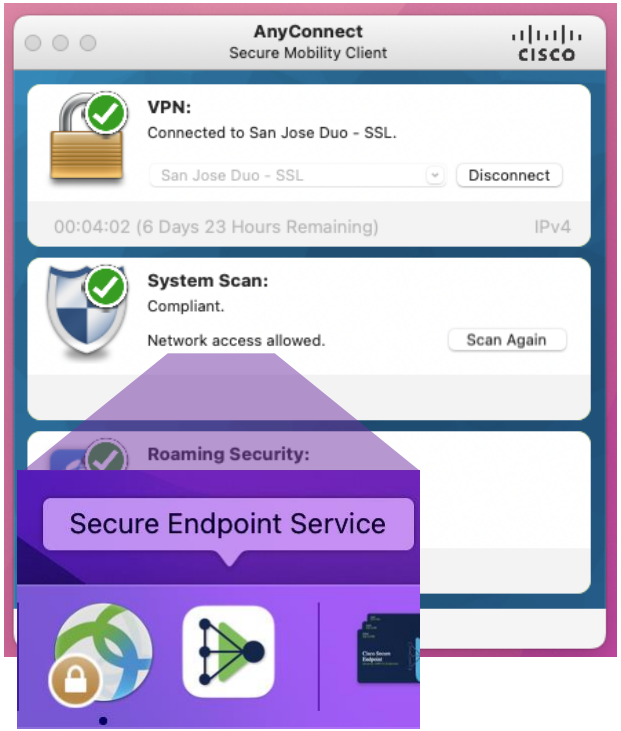


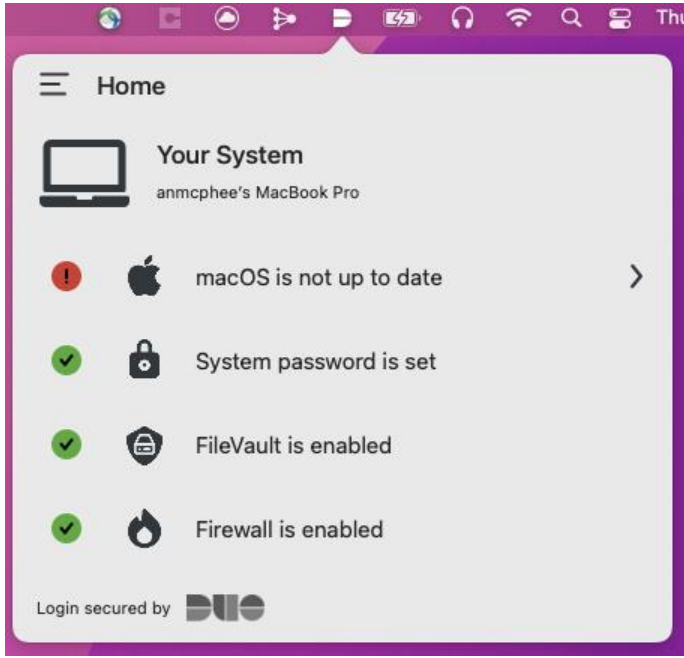
Diagnostics and Reporting Tool (DART)



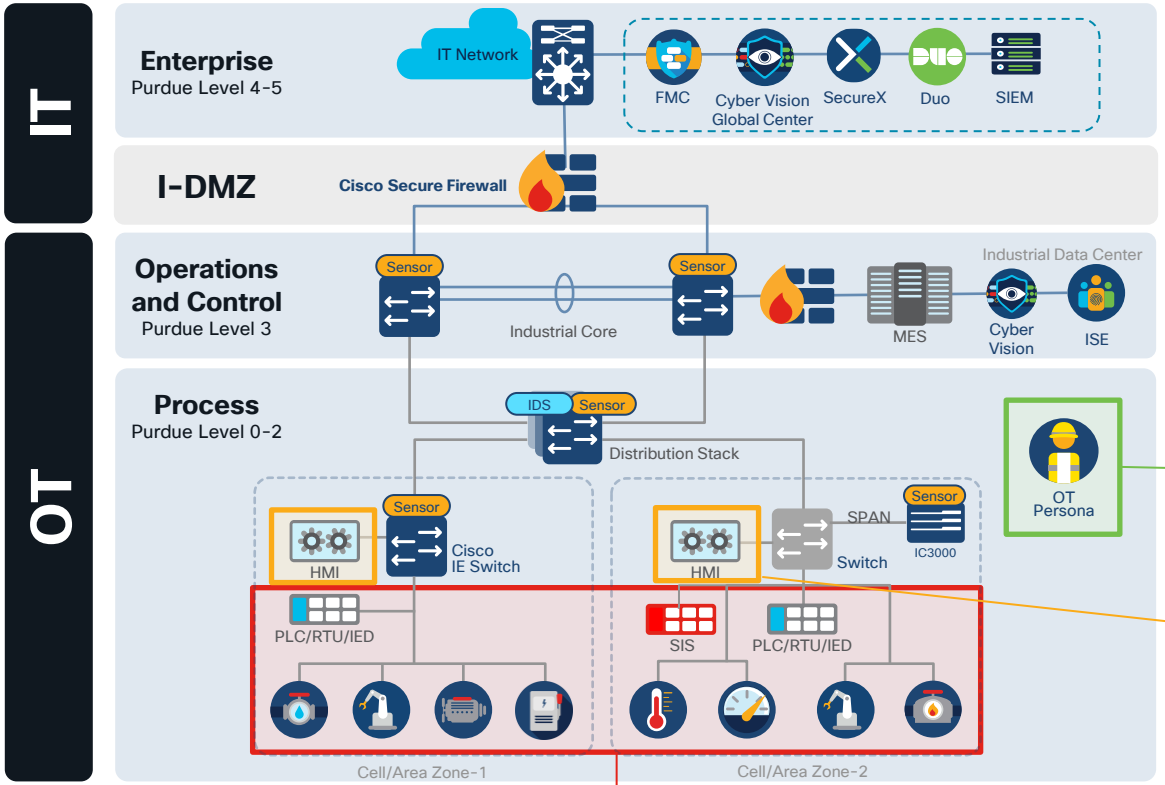
Endpoint Security is the Norm for IT systems







Where do you install Endpoint Protection in the OT?



Employee laptops / tablets / mobiles should always have it

Possibly, but policy may not allow it

Devices wont support it

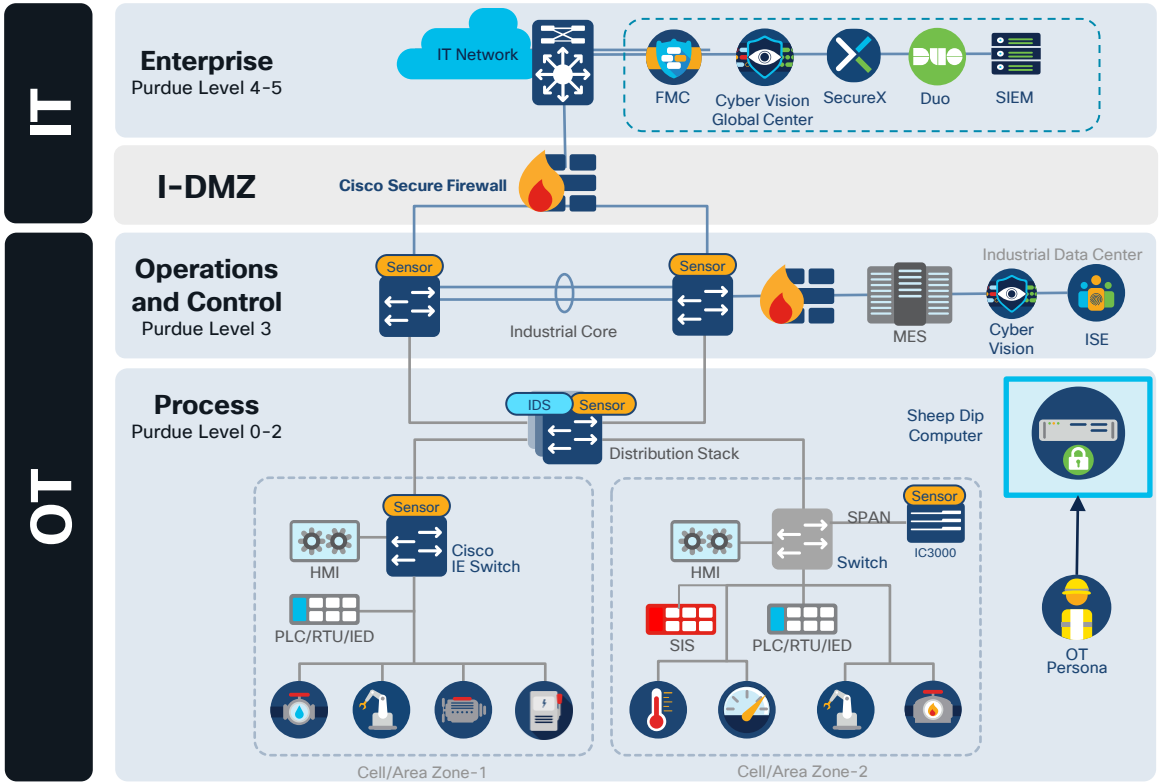
USB drives still pose a major concern for Industrial Networks

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



- 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

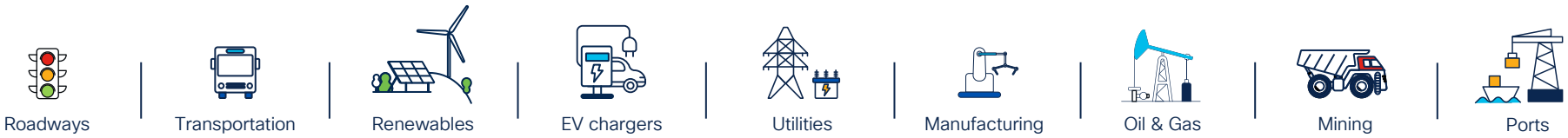
Remote configuration and maintenance by vendors and third-party technicians.

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.



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)

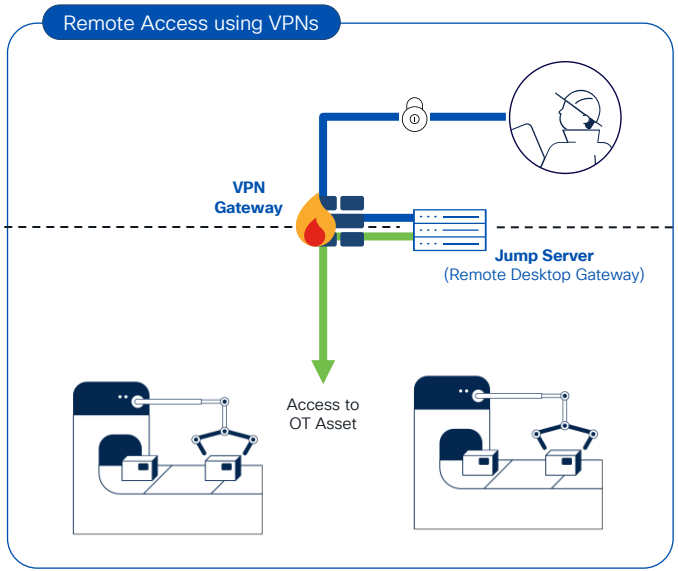
> ZTNA provides controlled **identity and context-aware** access to resources. It starts with a **default deny** posture and **adaptively offers the appropriate trust** required at the time. A **trust broker** mediates connections between applications and users. The result **reduces risk** and offers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

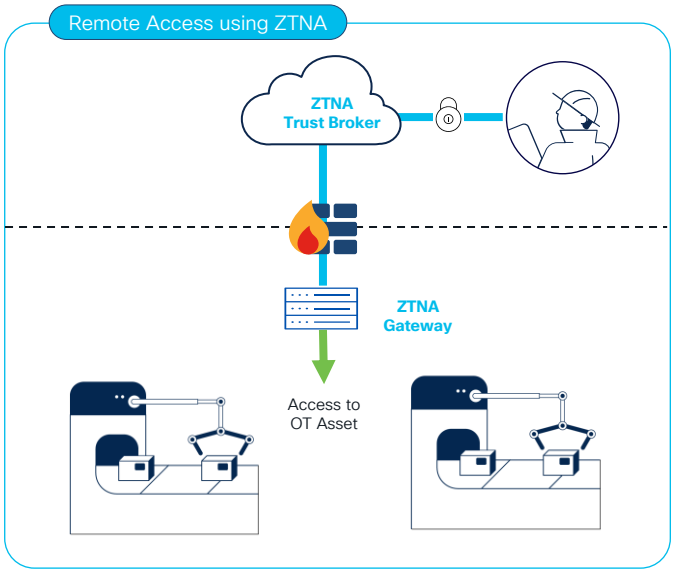
Gartner

Market Guide for Zero Trust Network Access, August 2023

- 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



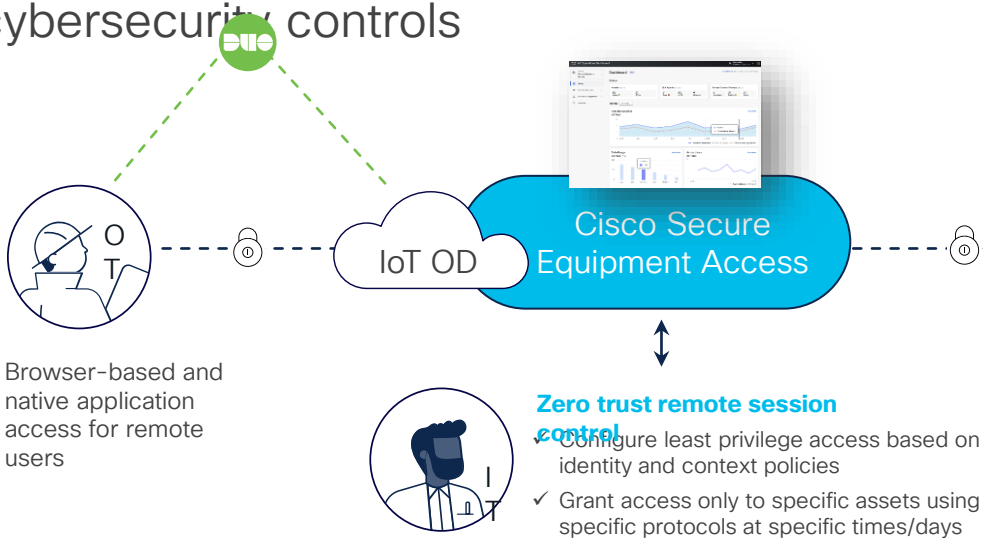


- Always-on solutions with all-or-nothing access
- Firewall rules need to be frequently updated
- Manual session management using jump servers

- 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

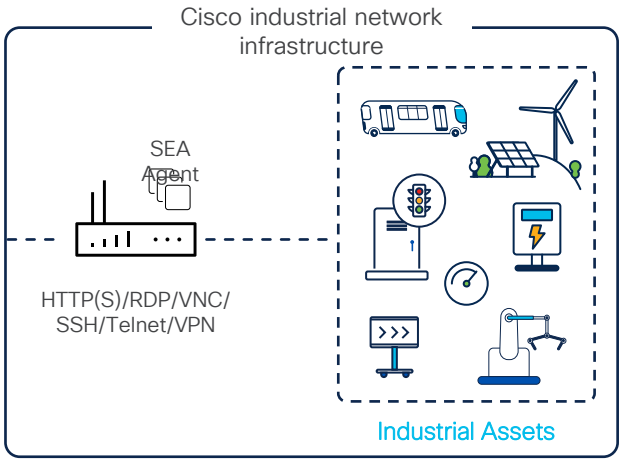
Zero Trust Network Access (ZTNA) for OT Assets

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



Zero trust remote session control

- ✓ Configure least privilege access based on identity and context policies
- ✓ Grant access only to specific assets using specific protocols at specific times/days
- ✓ Multi-factor authentication
- ✓ Remote user posture check
- ✓ Session recording, monitoring, termination



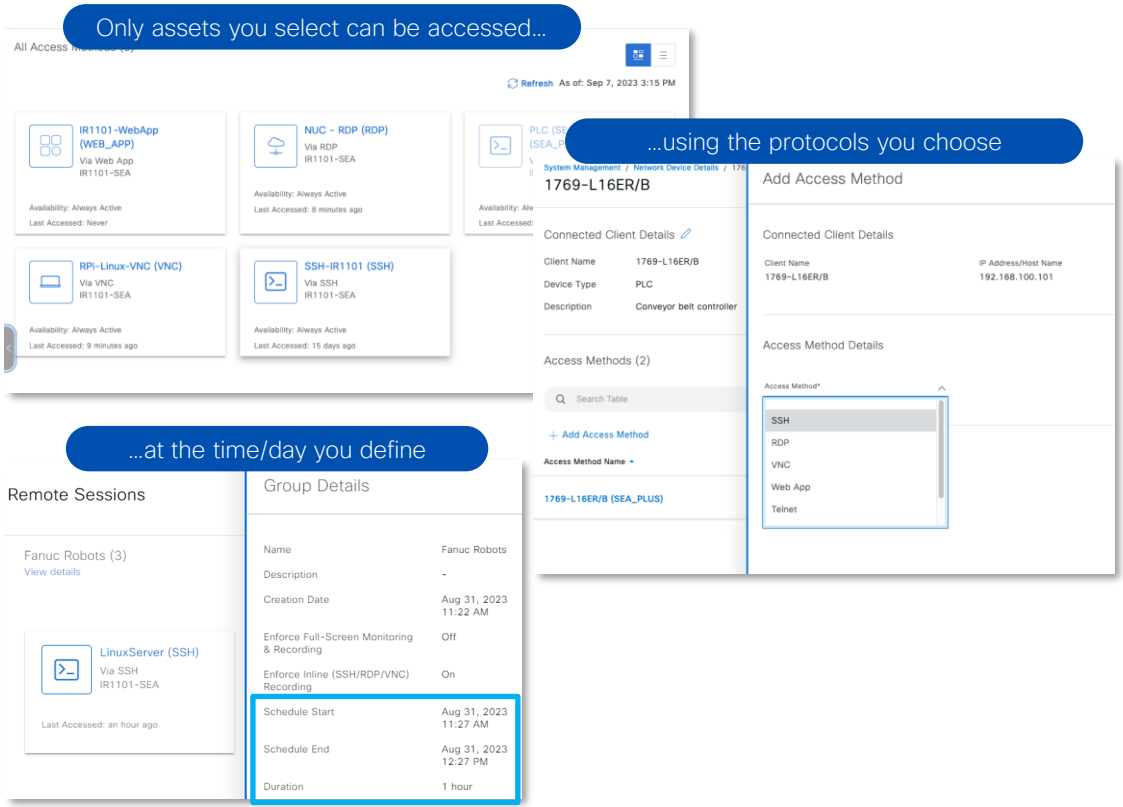
Cisco Secure Equipment Access

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.



Cisco Secure Equipment Access

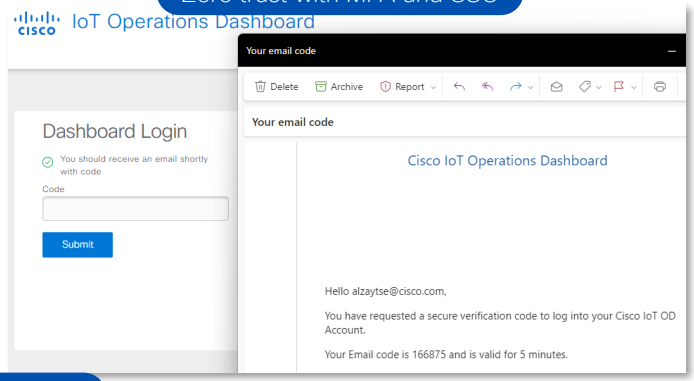
Identities and roles

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

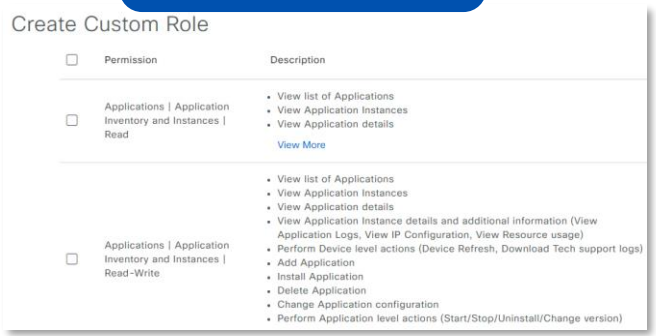
Security posture check

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

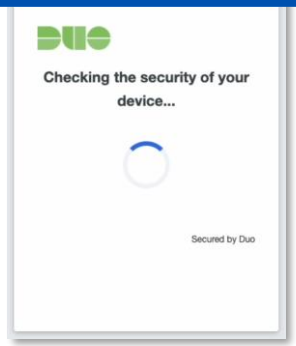
Zero trust with MFA and SSO



Custom user roles



Posture check with Duo



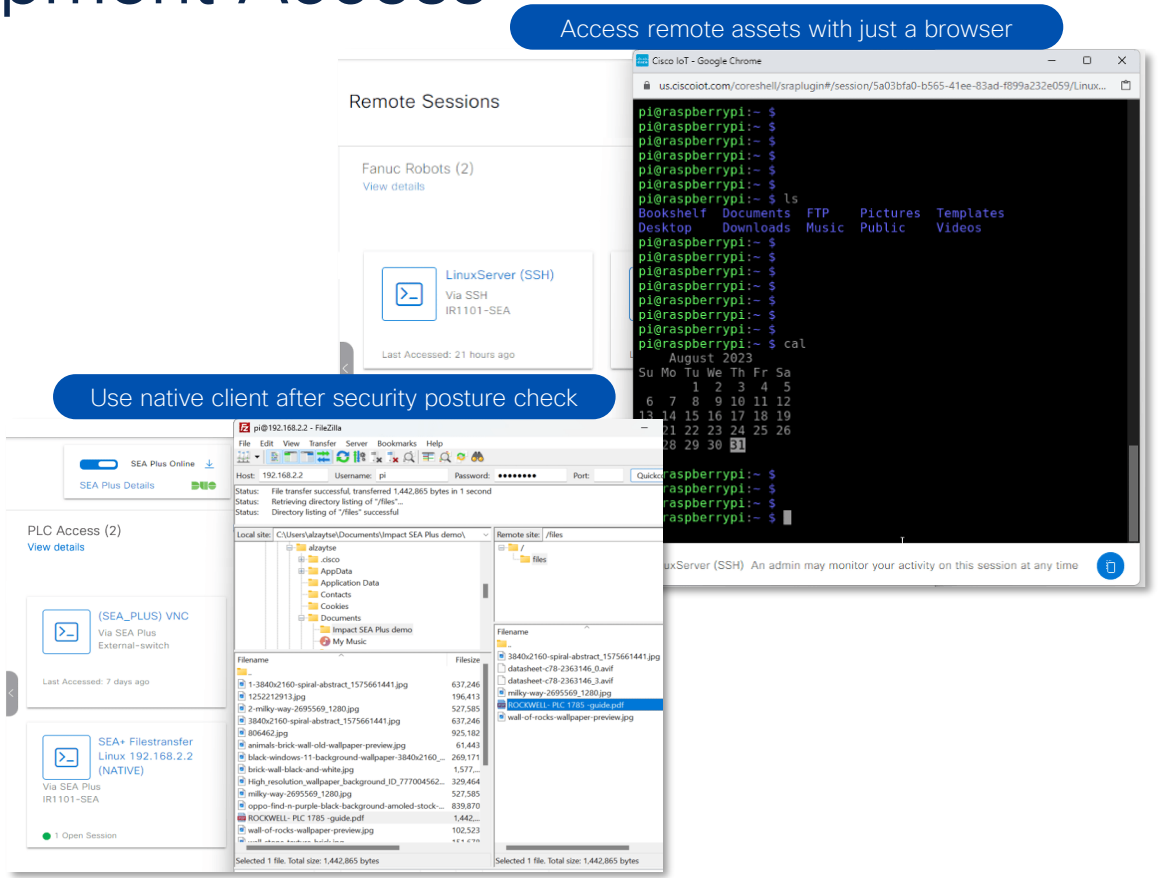
Cisco Secure Equipment Access

Clientless ZTNA

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

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.



Cisco Secure Equipment Access

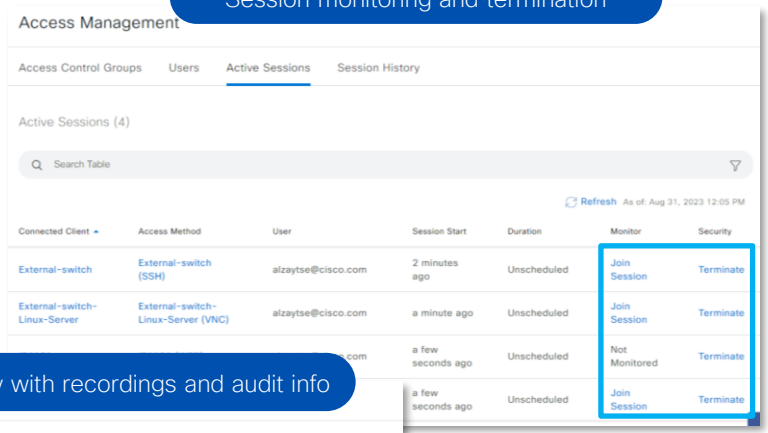
Session monitoring

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

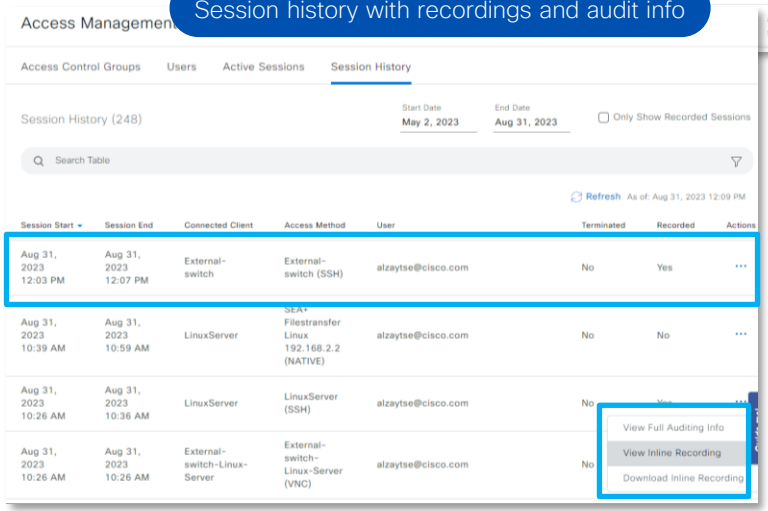
Session audit trails

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

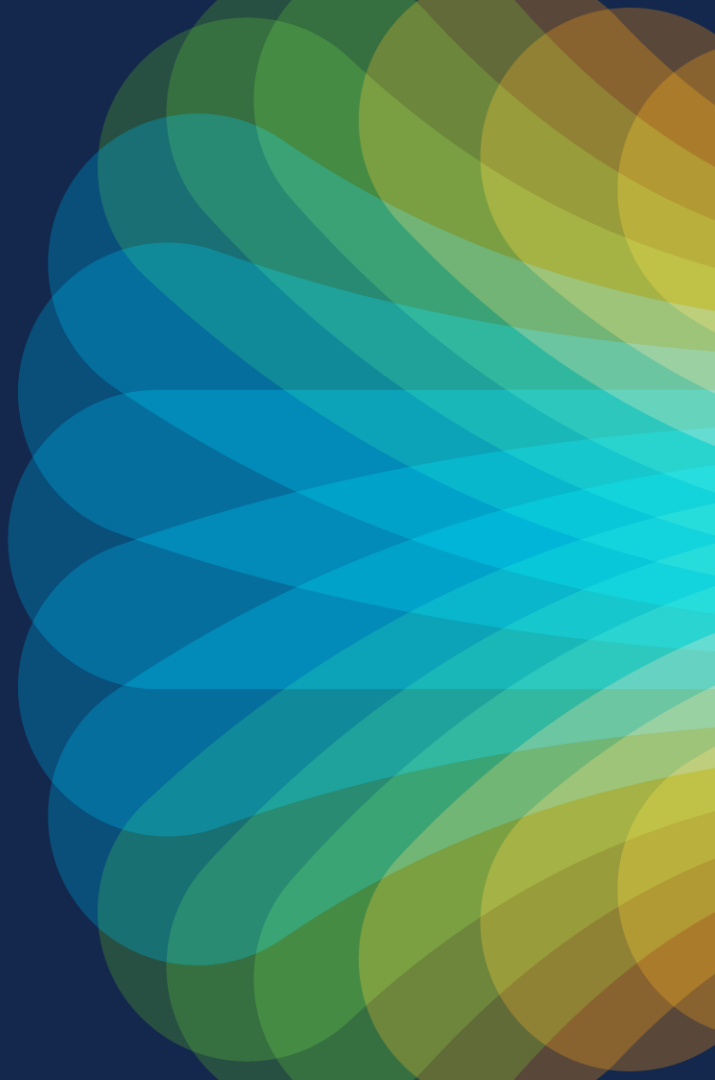
Session monitoring and termination



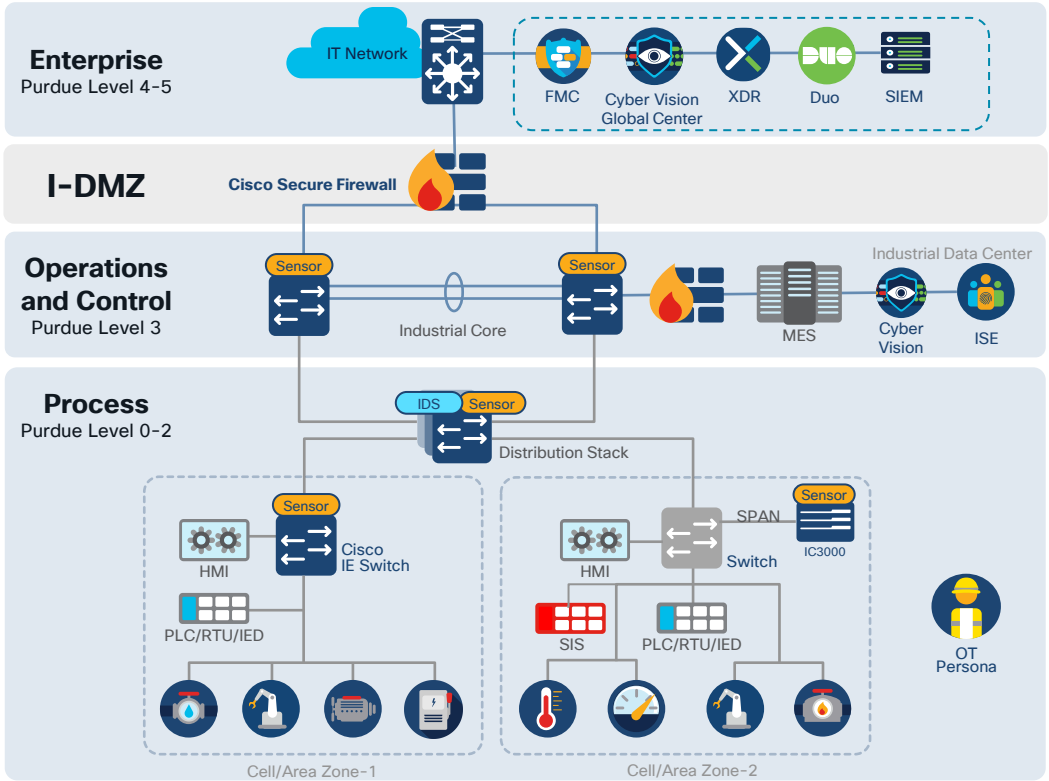
Session history with recordings and audit info



Pulling it all together



Let's put everything together

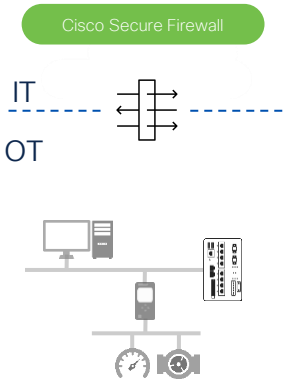


1. CyberVision discovers industrial assets and communications and groups it into Zones.
2. ISE implemented for visibility and CyberVision context is shared with ISE.
3. Components are dynamically classified in SGTs via group assignment directly from CyberVision
4. Visualize traffic activity between SGT 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.

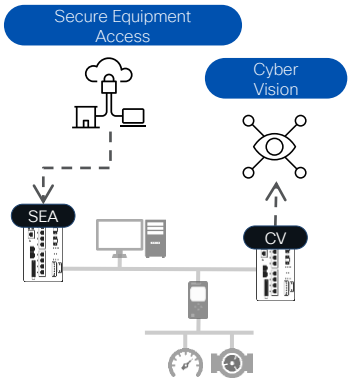
BRKIOT-2882

Cisco's Industrial Security Journey

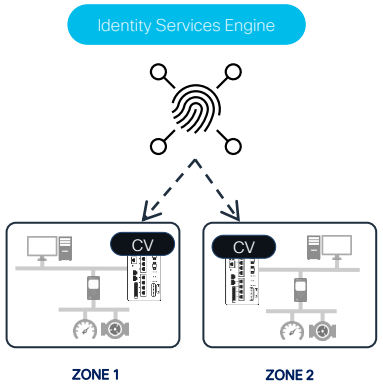
Build a Security Foundation



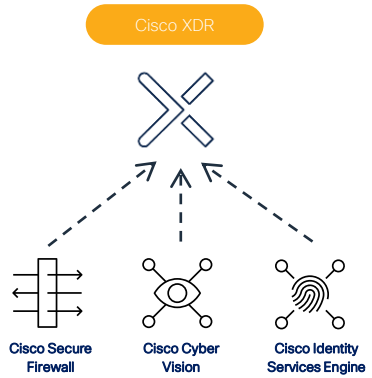
Security Posture & ZTNA of OT Assets



Segment Network into Smaller Trust Zones



Develop Incident Investigation & Response



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


cisco
The bridge to possible
Thank you
cisco Live!


cisco Live!
Let's go