

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC



Digitisation of OT

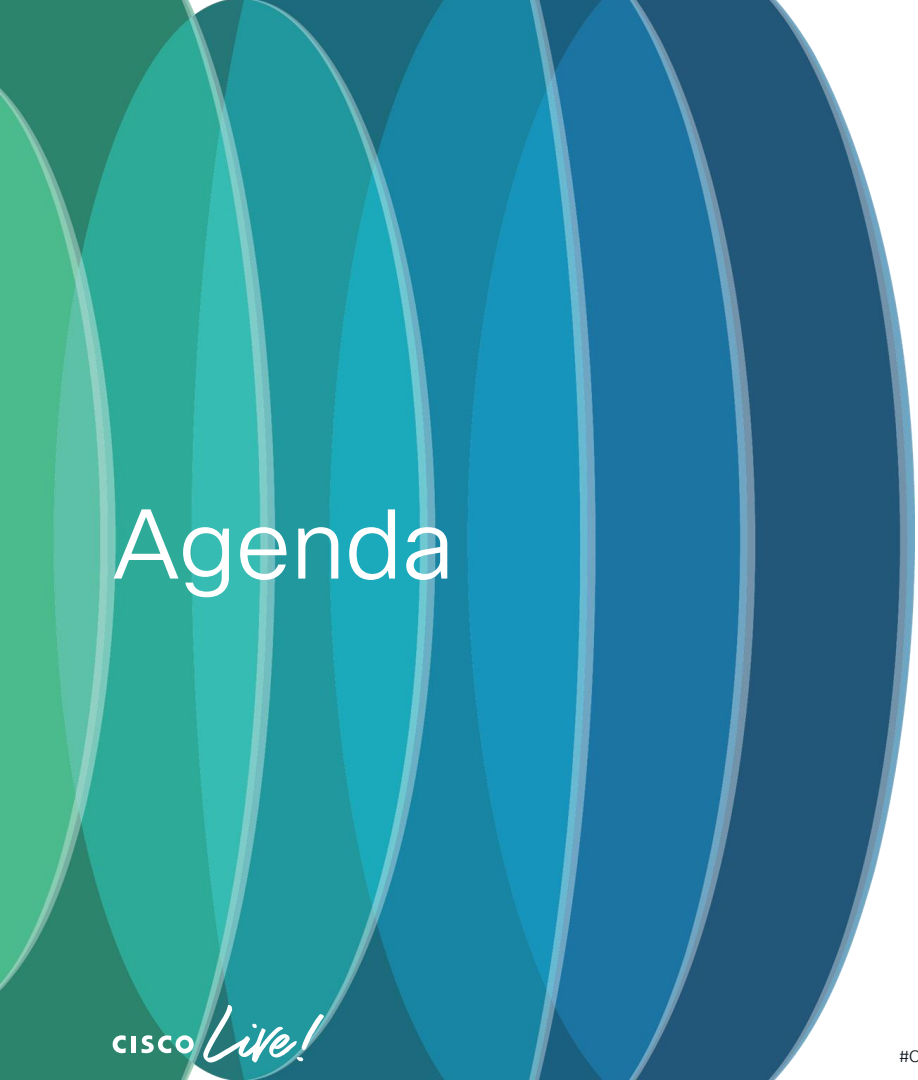
Increasing visibility, scalability and simple secure remote access

Alex Lynn, System Engineer
Industrial IoT, Cisco Systems

BRKIOT-2081



#CiscoLiveAPJC



Agenda

- Challenges with Digitisation and Remote Access
- How Cyber Vision can help with visibility
- How Secure Equipment Access can help with secure remote access
- IOS + Linux -> Containers
- Leverage IEC62443-3-3 with Cyber Vision for Segmentation

Cisco Webex App

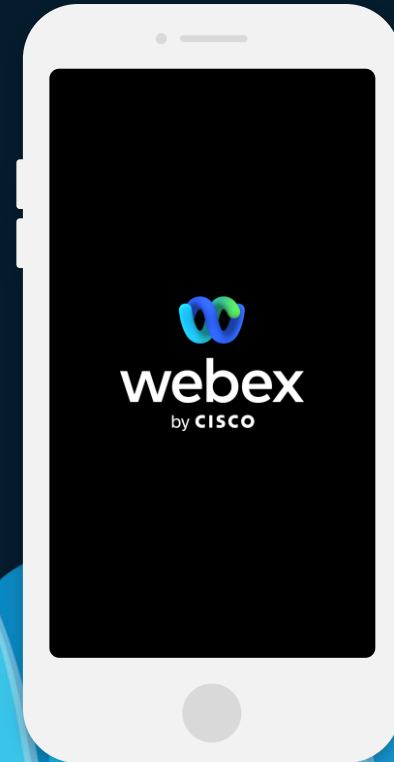
Questions?

Use Cisco Webex App to chat with the speaker after the session

How

- 1 Find this session in the Cisco Live 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 November 15, 2024.

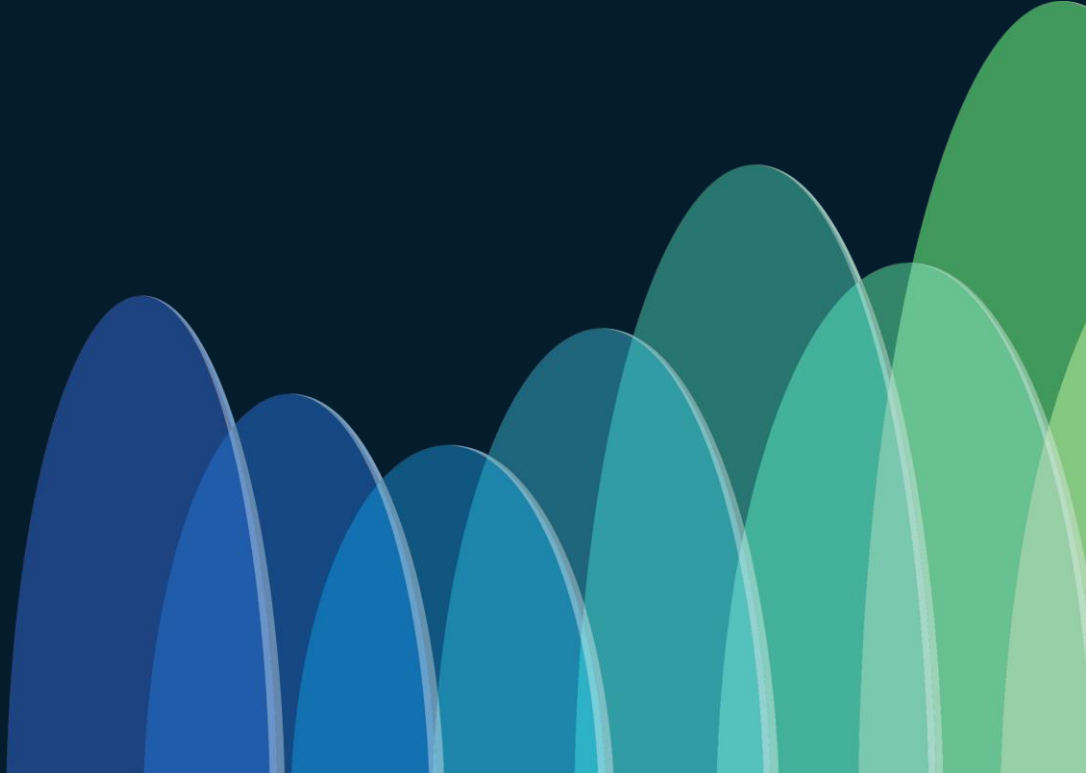


Industrial IoT Summit@Cisco Live APJC Wed 14th

Time	Eureka 1	Eureka 2	Eureka 3
11:45 – 12:20	Lunch & Networking inside the Room	Lunch & Networking inside the Room	Lunch & Networking inside the Room
12:20 – 12:45	Utilities Cisco Executive Welcome Vikas Butaney, Senior Vice President, Cisco Ross Delacour, IIoT APJC Regional Director	Mining Cisco Executive Welcome Dave West, Senior Vice President Samuel Pasquier, Vice President, IIoT Product Management	Transportation Cisco Executive Welcome Stefan Leitl, Vice President, Global IIoT Sales Bryan Tantzen, Sr. Director, IIoT Solutions
12:45 – 4:30	<u>Utilities Summit Breakout</u>	<u>Mining Summit Breakout</u>	<u>Transportation Summit Breakout</u>
	Industry breakout sessions bring focused dialogue to the key topics you care about: Breakout sessions include curated presentations by industry leaders including an industry panel discussion with Q&A. These meaningful conversations related to current and emerging trends will empower you to navigate the ever-changing IT/OT landscape with actionable takeaways you can bring back to your environment.		
4:30 – 5:15	Cocktail Reception Interact with your Industry peers and Cisco Industrial IoT Executives		

Contact Alex Lynn (alelynn@cisco.com) or
Andrew Johnstone (ajohnst3@cisco.com) for admission

Define Inevitable



Adjective:

Certain to happen; unavoidable.

"Digitsation was inevitable"

Noun:

A situation that is unavoidable.

"By the morning, we had accepted the inevitable"

Digitisation has become a necessity

Digitisation requires increased connectivity, and increased connectivity leads to challenges

Expanded Threat Surface

- Increasing number of endpoints
- Devices beyond traditional network perimeter
- Different ways of accessing assets
- [Point products and solutions](#)

Lack of Visibility

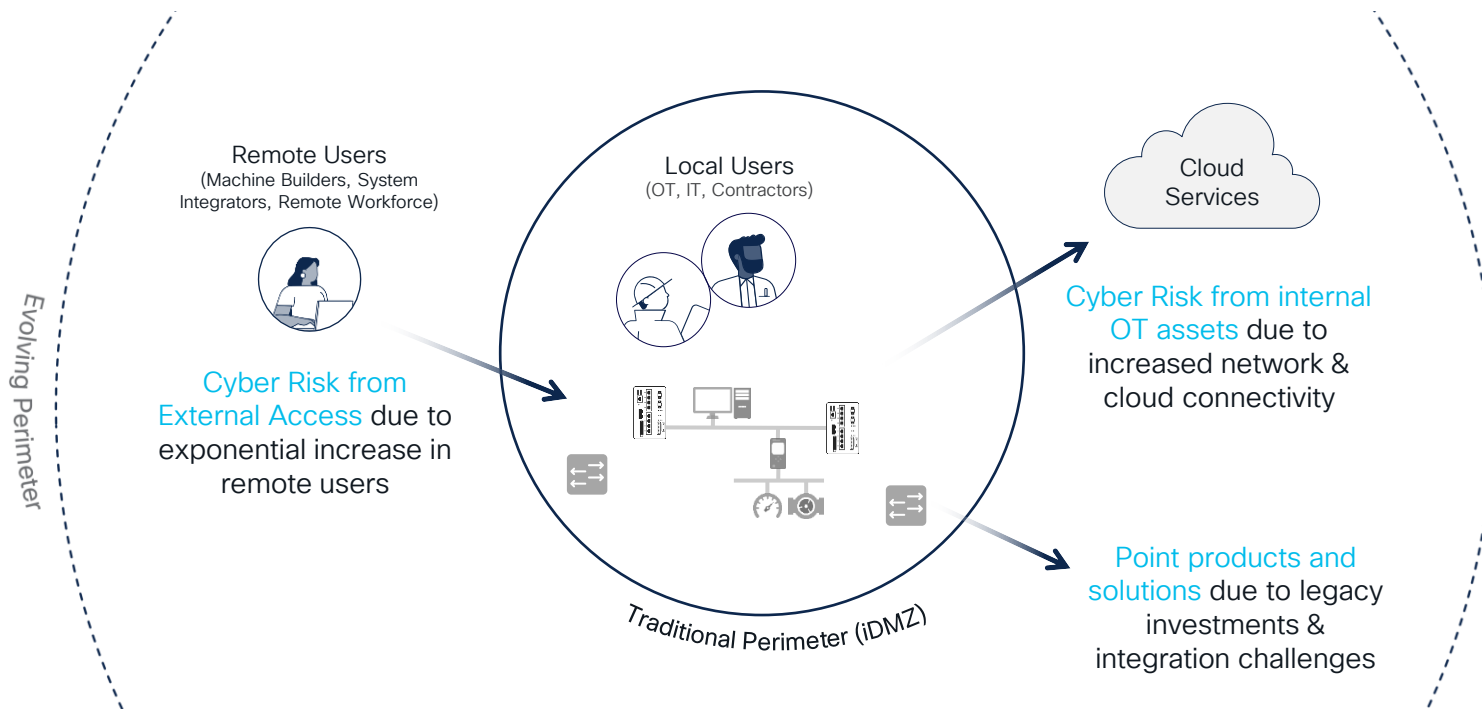
- Heterogenous protocols and devices
- Lack of holistic view
- [Traditional IT tools won't help in industrial environments](#)

Poor Cyber Security Hygiene

- Not compliant with government regulations
- Inability to handle vulnerabilities
- [Lack of IT/OT collaboration](#)

Expanded threat surface

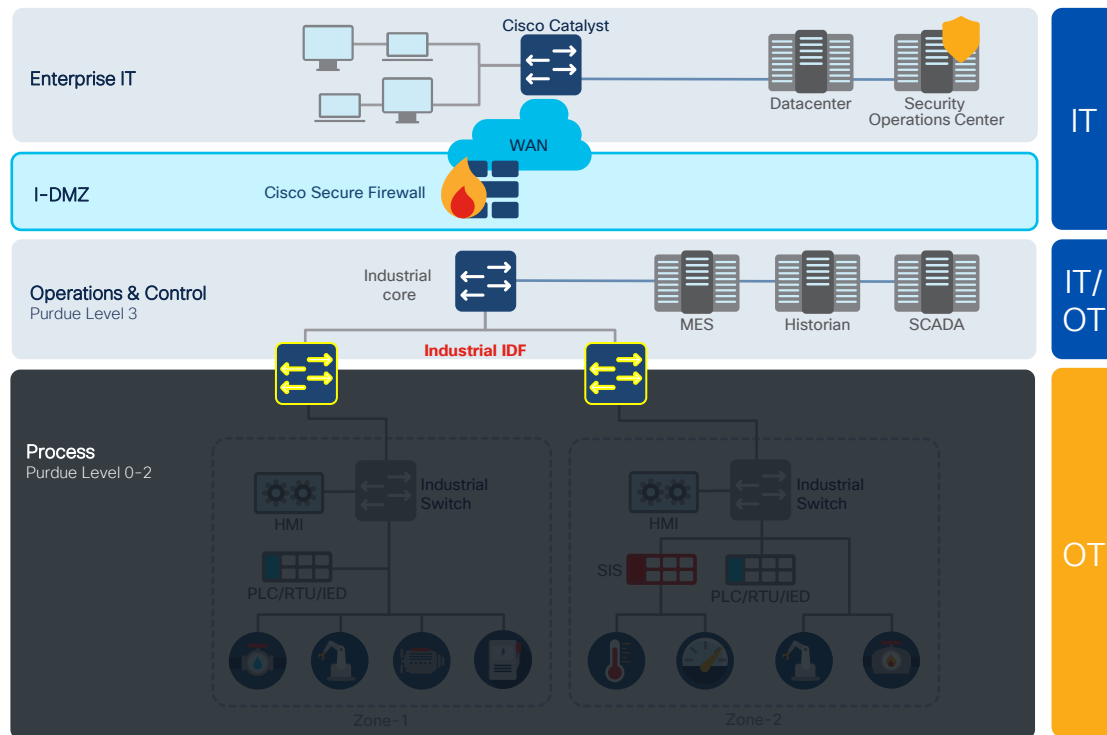
Point Products & Solutions



A larger industrial digital footprint results in increased cyber risk exposure

Lack of visibility

Limited visibility into OT assets



How can IT leverage network equipment it owns to gain visibility into OT?

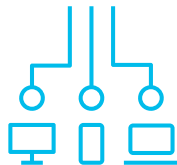
Poor Cybersecurity hygiene

Ineffective workflow

Problem



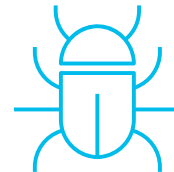
Ineffective workflow
between OT and IT



Limited visibility
of OT assets



Lack of
Segmentation



Malware
is the killer

Many roadblocks towards success. Industrial organisations need guidance.

Is Security really top of mind?



Between 2019 and 2023, attacks causing physical consequences to OT networks are almost doubling every year¹



Yet, malware free activity (such as identity attacks) represented 75% of detections in 2023 – up from 71% in 2022²

VPN with no MFA

Colonial Pipeline hack explained: Everything you need to know

A ransomware attack brought a major gas pipeline to a standstill in May. Here's what happened and who was behind the hack.

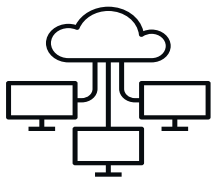
By [Sean Michael Kerner](#)

Published: 26 Apr 2022

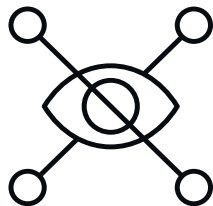
1. Waterfall 2024 Threat Report – OT Cyberattacks with Physical Consequences

2. CrowdStrike 2024 Global Threat Report

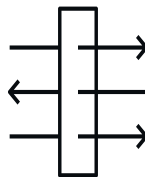
Problems with our existing remote access solutions



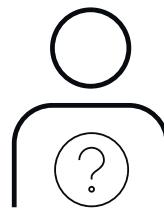
Unknown remote access gateways



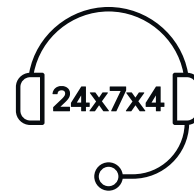
No visibility into user activity



VPN / Jump servers with full plant access



No Multi-Factor Authentication (MFA)



24/7 availability

For many, these are not new problems, and an attacker just needs a single entry to cause damage

SOCI/ESS8



Mandates must be implemented to drive change

NIS2

the use of *multi-factor authentication* or continuous authentication solutions

NIST

MFA is an accepted best practice for remote access to OT applications

ISA/IEC-62443

SR 1.1 RE 2 – *MFA for untrusted networks*

SR 1.1 RE 3 – *MFA for all networks*

NERC CIP

005-7 – Remote Access Management: *Require MFA*

TSA

MFA, or other logical and physical security controls that *supplement password authentication*

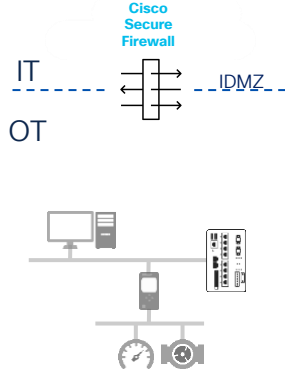
SOCI/ESS8

Phishing-resistant multi-factor authentication should be implemented for all services

4 Stages to Industrial Security Solution

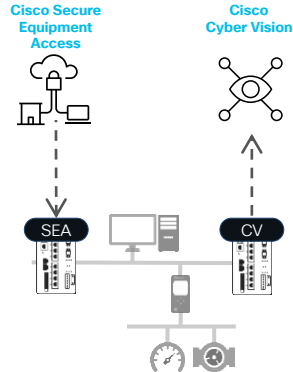
1

Build a Security Foundation



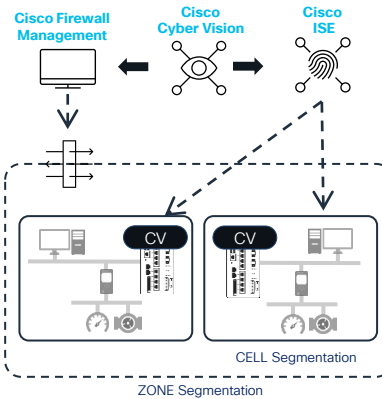
2

Security Posture & ZTNA of OT Assets



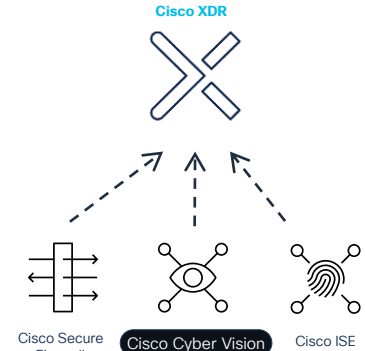
3

Segment Network into Smaller Trust Zones



4

Develop Incident Investigation & Response



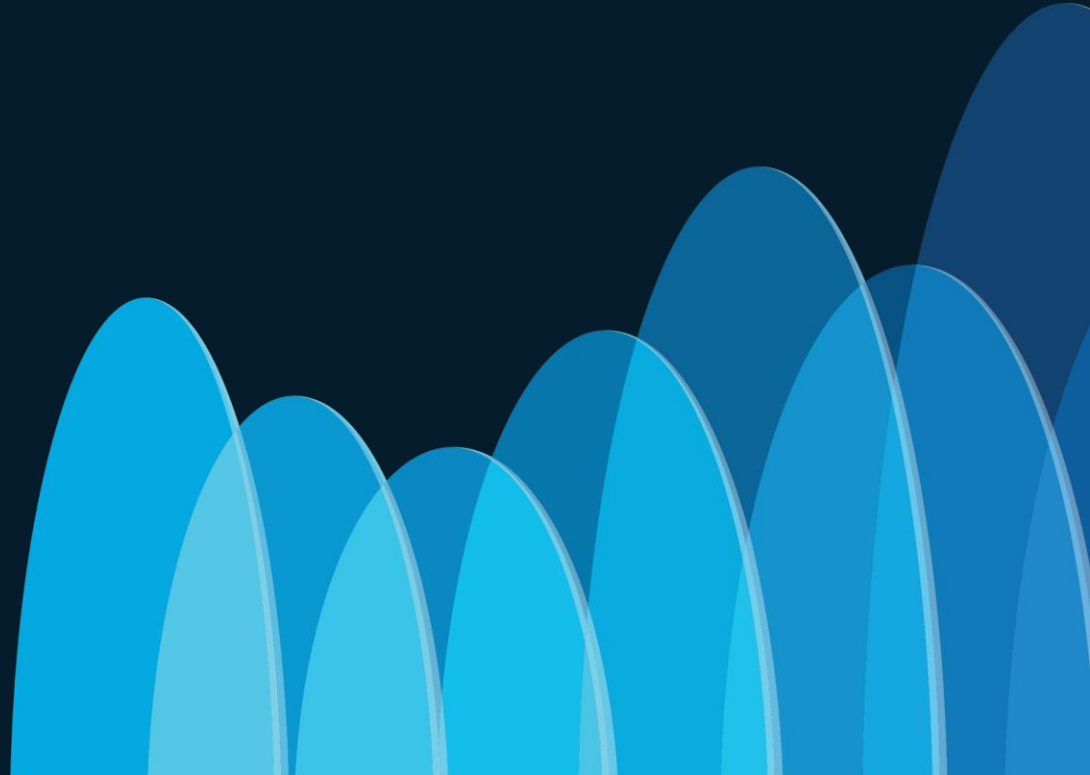
Talos Threat Intelligence

+



Talos Incident Response

Cyber Vision



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
- ✓ Short Threat Detection
- ✓ Talos Threat Intelligence
- ✓ On-prem & Cloud offers

CISCO *Live!*

Cyber Vision Center



Metadata

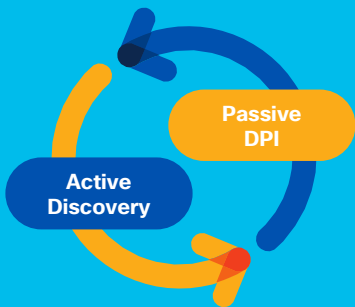
1 0 0 1
0 0 1

Cyber Vision Sensors

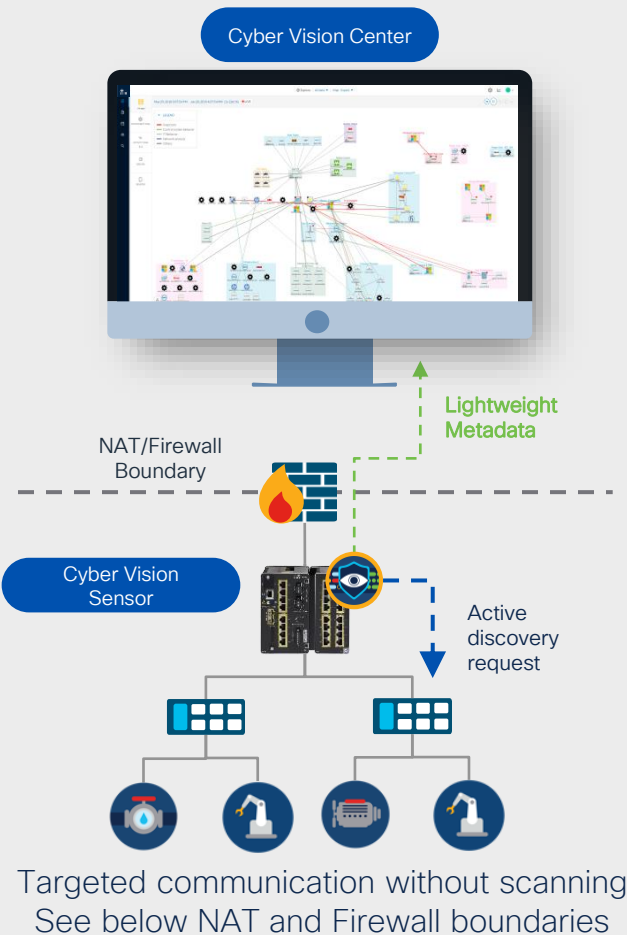


Deep Packet Inspection & Active Discovery
built into your network infrastructure

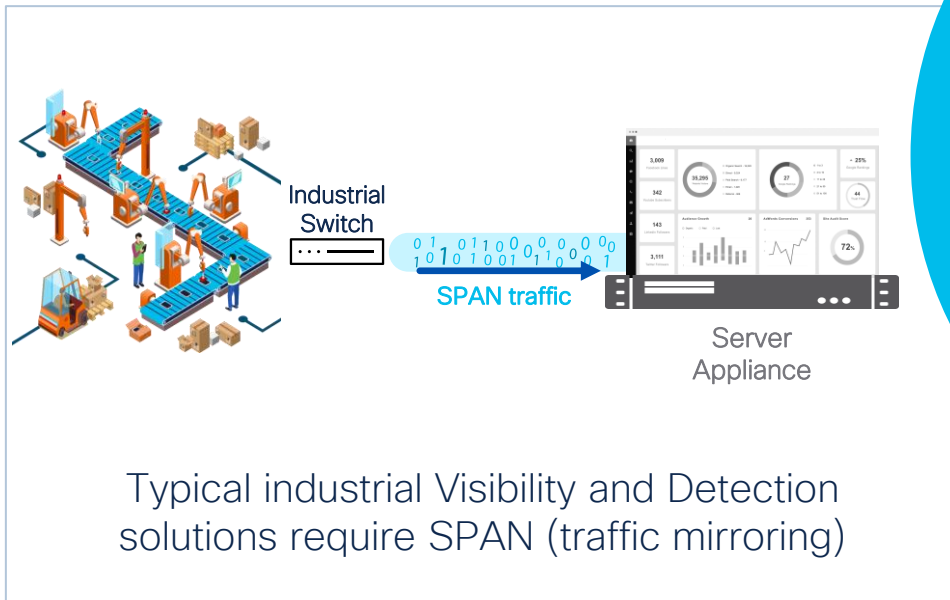
Distributed Edge Active Discovery



Closed-loop control between Passive DPI and **Active Discovery by Distributed Sensor** provides **100% Visibility**



Security Starts with Visibility But Beware of Hidden Costs!



Additional switches
for SPAN collection



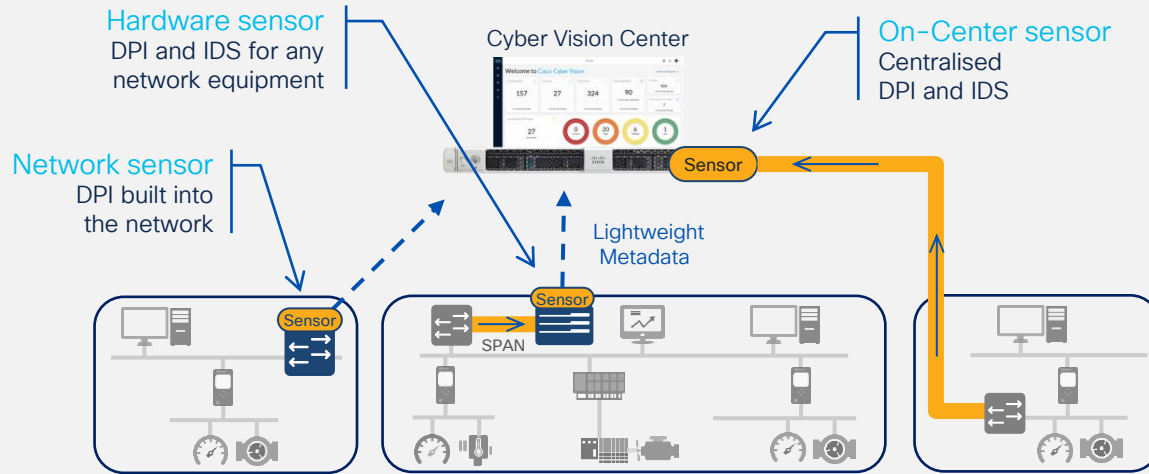
Expensive cabling
for collection network



**Exponential
increase in traffic**
due to SPAN

TCO of SPAN based solutions is **not** sustainable over long-term growth

Cyber Vision offers flexible deployment options



Network-sensors embedded in Cisco networking for simple and highly scalable deployments

Hardware-sensors capturing traffic on any switch with a single hop SPAN

On-Center sensor to leverage existing SPAN infrastructures, or collect traffic within the datacenter

SPAN option and Hardware sensors to support brownfield

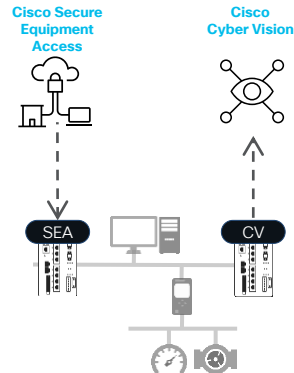
Network embedded sensors as you evolve and grow your operations

How Cyber Vision Can Help

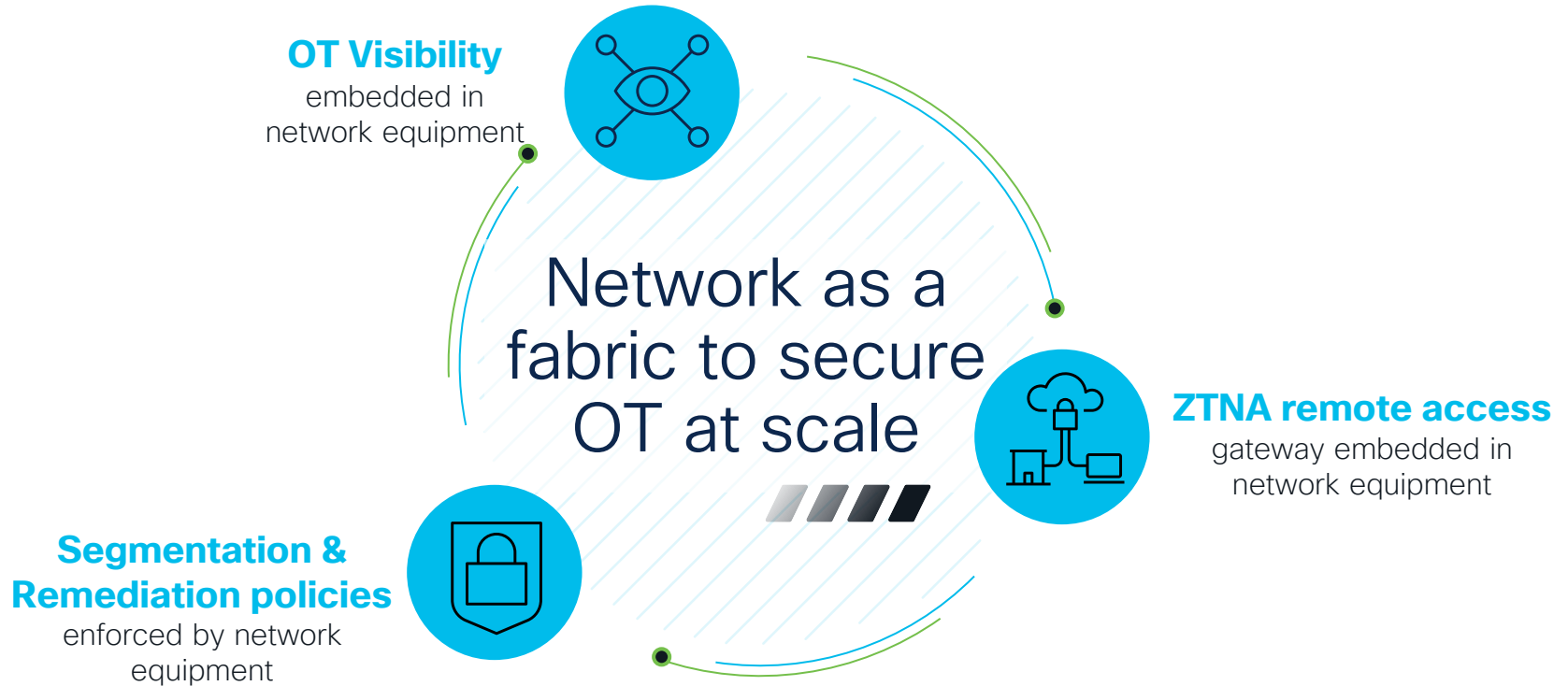
Point Product & Solution problem

2

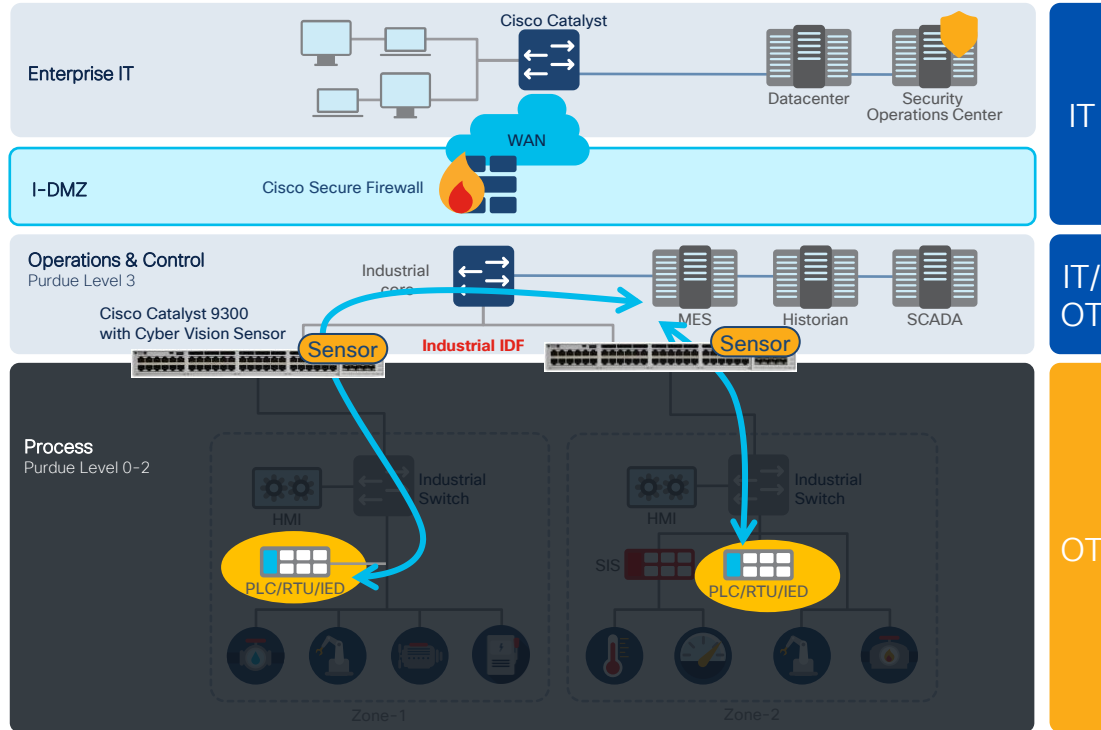
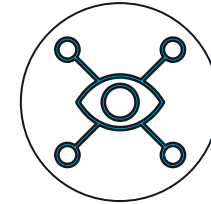
Security Posture & ZTNA of OT Assets



The Cisco Industrial Security Differentiation

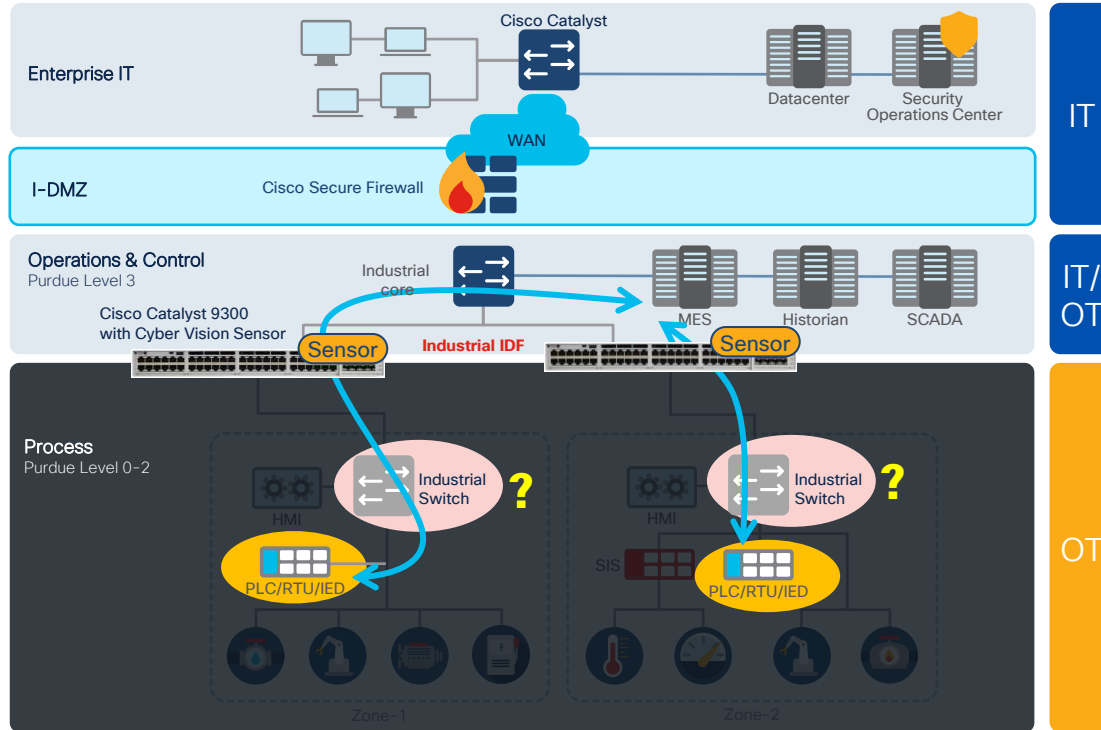
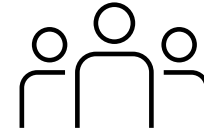


Your Catalyst switches let you turn on the lights



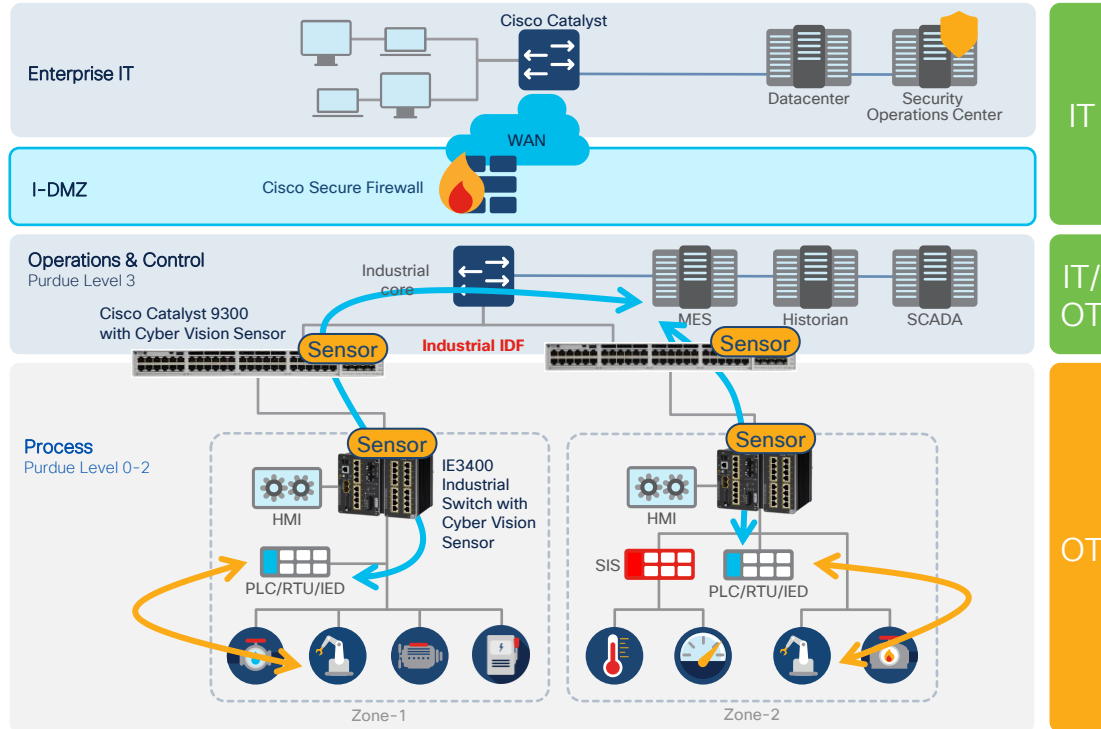
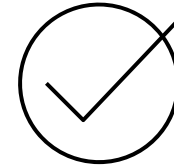
Step-1: Cyber Vision Sensor on Catalyst 9300 gives you visibility to North-South communications to identify key assets

Get OT buy-in by showing the benefits of visibility



Step-2: Work with OT to identify the critical industrial switches that connect these key assets

Gain full visibility to improve your security posture



Step-3: Replace critical switches with Cisco IE Switch running Cyber Vision sensor to see the entire OT network

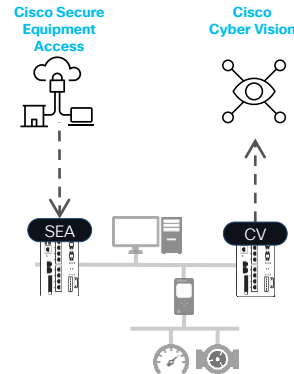
Note: You don't need to replace all industrial switches, just the ones connecting to PLC's

How Cyber Vision Can Help

Poor Cybersecurity hygiene problem

2

Security Posture & ZTNA of OT Assets



Use Risk Scoring to assess your security posture

Identify Riskiest Operations

Preset	Risk score	Last precomputation	Devices	Vulnerabilities
All Controllers	36.5	Jun 17, 2021 9:46:41 AM	14	94
Broadcast traffic only	12	Jun 17, 2021 9:46:47 AM	30	158
IT Activities	16	Jun 17, 2021 9:46:47 AM	36	169
IT Devices	25	Jun 17, 2021 9:46:49 AM	23	94
Internet Activities	12	Jun 17, 2021 9:46:45 AM	0	0
OT Devices	28	Jun 17, 2021 9:46:46 AM	21	128

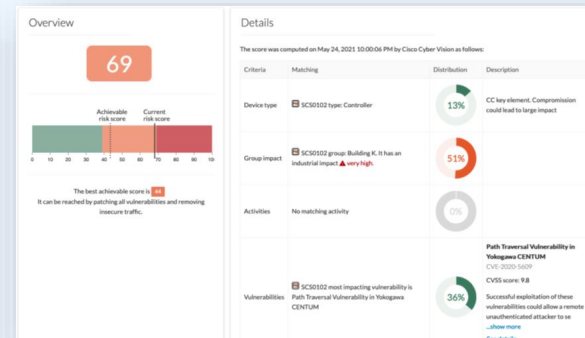
Preset widgets help identify operations at highest risk

Identify Riskiest Endpoints within operations

Device	Group	First activity	Last activity	IP	NAC	Risk score	Tags
SC50102	Building K	Oct 11, 2019 11:06:52 AM	May 24, 2021 12:30:15 PM	192.168.1.123	0000:64:8b:3c:15 (1 other)	69	# Controller - # Time Server
Falser 10.5.0.22	Emerson Process	Oct 11, 2019 11:03:46 AM	May 24, 2021 12:30:15 PM	10.5.0.22	00:22:45:3f:90:10	69	# Controller - # Default
Falser 10.4.0.14	Emerson Process	Oct 11, 2019 11:03:46 AM	May 24, 2021 12:30:15 PM	10.4.0.14	00:22:45:3f:90:10	69	# Controller - # Default
10.4.0.30	Emerson Process	Oct 11, 2019 11:03:46 AM	May 24, 2021 12:30:15 PM	10.4.0.30	00:22:45:21:0a:90	69	# Controller - # Time Server - # Default
Yokogawa 192.168.1.124	Yokogawa	Oct 11, 2019 11:06:52 AM	May 24, 2021 12:30:15 PM	192.168.1.124	0000:64:8b:3c:15 (1 other)	69	# Controller
Falser 10.5.0.18	Emerson Process	Oct 11, 2019 11:03:46 AM	May 24, 2021 12:30:15 PM	10.5.0.18	00:22:45:3f:90:20	69	# Controller - # Default
Falser 10.4.0.29.2	Emerson Process	Oct 11, 2019 11:03:46 AM	May 24, 2021 12:30:15 PM	10.4.0.29.2	00:22:45:04:45:40	69	# Non Management Server
Falser 10.4.0.29.1	Emerson Process	Oct 11, 2019 11:03:46 AM	May 24, 2021 12:30:15 PM	10.4.0.29.1	00:22:45:12:4c:90	69	# Non Management Server
192.168.1.123	Yokogawa	May 11, 2020 6:21:58 PM	May 24, 2021 12:30:15 PM	192.168.1.123 (1 other)	4c:12:62:33:95:20	69	# Email Server
Hirschmann 192.168.1.254	Building K	Oct 11, 2019 11:06:52 AM	May 24, 2021 12:30:15 PM	192.168.1.254	ec:74:ba:03:99:40	69	# Time Server
Yokogawa 192.168.1.128	Yokogawa	Oct 11, 2019 11:06:52 AM	May 24, 2021 12:30:15 PM	192.168.1.128	0000:64:8b:3c:15 (1 other)	69	# Time Server

Sort and Filter Risk scores of endpoints to identify riskiest devices

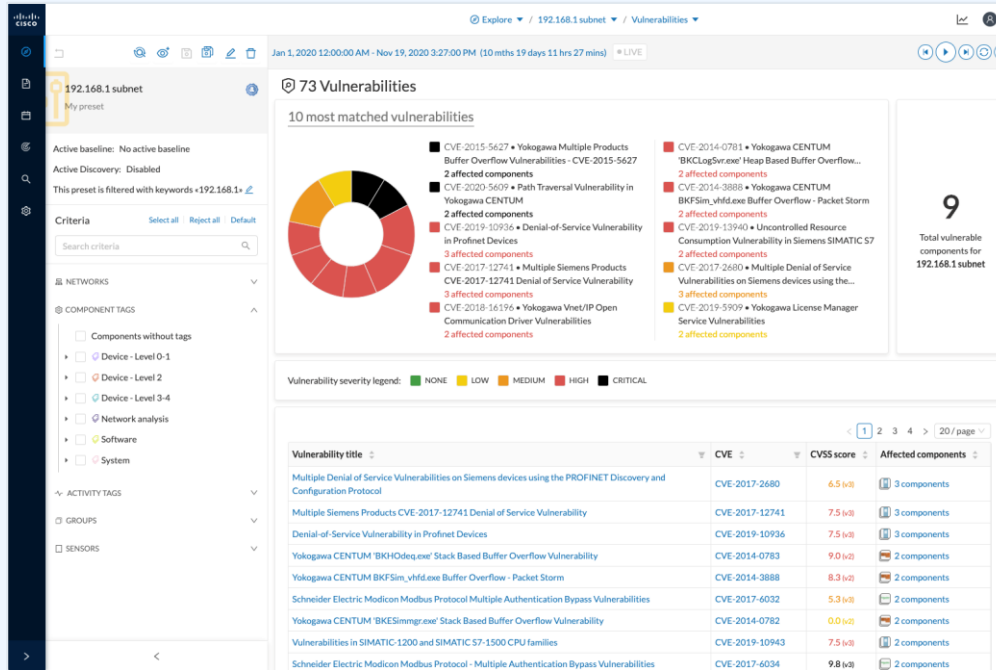
Understand Scoring to Reduce Risk



See what impacts endpoint risk score
See where you are, and where you could be

Build an action plan to to reduce risk

Improving Your Security Posture



- Identify most matched vulnerabilities based on severity
- Easily identify affected endpoints
- Build a remediation plan to patch or implement security controls

Identify and stop malicious traffic

Explore / 192.168.0 subnet / Activity list

Last 1 day (May 23, 2021 11:43:26 PM — May 24, 2021 11:43:26 PM) Refresh

30 Activities [New data](#) [Export to CSV](#)

1 2 > 20 / page

Device	Device	First activity	Last activity	Tags	Flows	Packets	Volume
STATION	VM-XP-PRO	Oct 11, 2019 11:39:57 AM	May 24, 2021 12:32:16 PM	Program Download, Start CPU, Stop CPU, Unite	-10	91036	6.59 MB
Virtual 192.168.0.77	Siemens 192.168.0.1	Oct 11, 2019 10:59:49 AM	May 24, 2021 12:32:16 PM	ARP, 57	-10	1255	109 kB
IE11WIN7	DESKTOP-GBJUF2N	May 26, 2021 12:14:06 AM	May 26, 2021 12:19:04 AM	Insecure, Authentication, Procedure Call, Exception, Low Volume, Netbios, Netbios Name Service, SMB, SNORT Policy Violation	-20	234	35.6 kB
1756-L55/A 1756-M12 (A LOGIX5555 (Port1-L ink00))	STATION-WINCC	Oct 11, 2019 11:23:14 AM	May 24, 2021 12:32:16 PM	Read Var, Write Var, ARP, EthernetIP	-10	29239	1.46 MB
192.168.0.255	VM-XP-PRO	Oct 11, 2019 11:39:57 AM	May 24, 2021 12:32:16 PM	Insecure, Broadcast, Low Volume, Netbios, SMB	-10	4	972 B

Security analysis

- ☐ DDOS
- ☐ Insecure
- ☐ Port Scan Activity
- ☐ Snort Alert
- ☐ Snort Browser
- ☐ Snort Deleted
- ☐ Snort Experimental-DoS
- ☐ Snort Experimental-Scada
- ☐ Snort Exploit-Kit
- ☐ Snort File
- ☐ Snort Malware-Backdoor
- ☐ Snort Malware-CNC
- ☐ Snort Malware-Other
- ☐ Snort Misc
- ☐ Snort OS-Other
- ☐ Snort OS-Windows
- ☐ Snort Server-Other
- ☐ Snort Server-Webapp

Activity tags associated with events detected by the Snort IDS provide context to understand malicious activities

Segmenting with Visibility & Policy Analytics

Visualize → Dynamically Assign Tags → Monitor Policy → Enforce



Visualise Zones & Conduits



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

Dynamic SGT Mapping



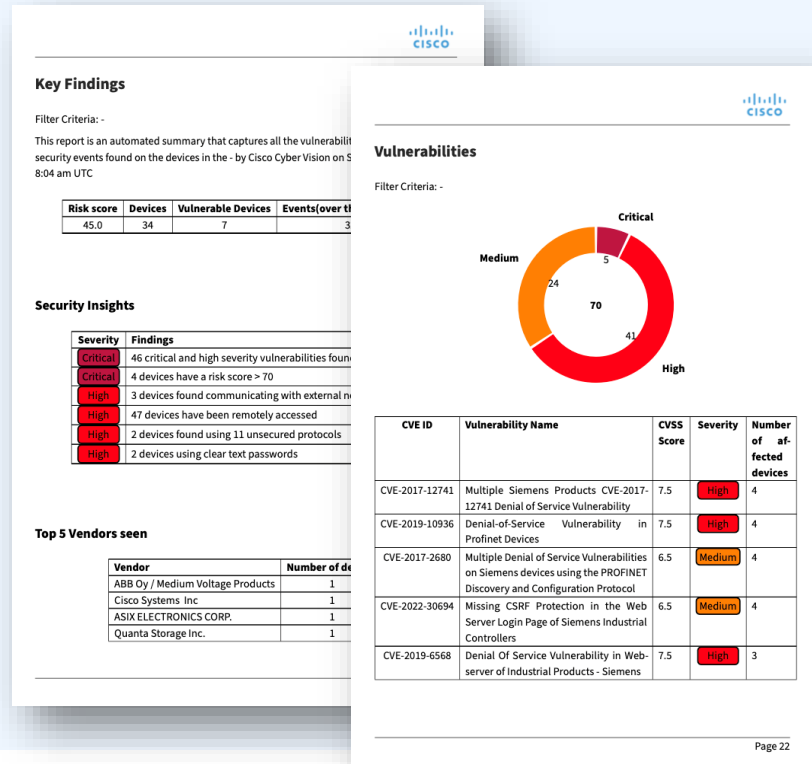
Cyber Vision grouping results in dynamic Group-based policy assignment to endpoints through ISE

Monitor Before Enforcement



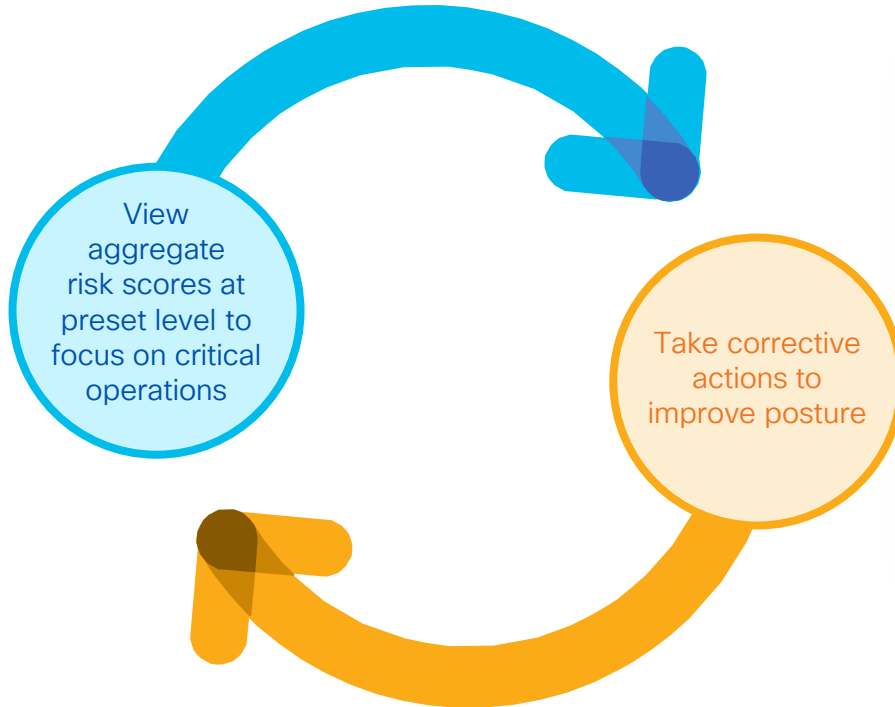
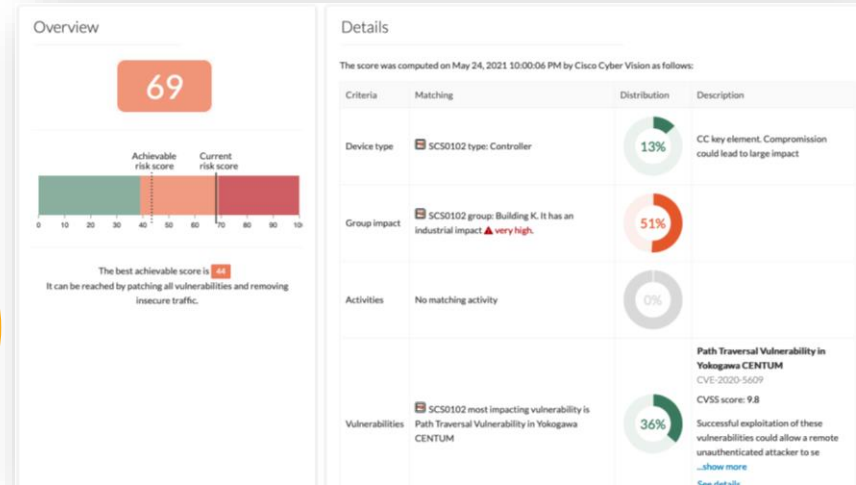
Visualize Group-based network behavior in Catalyst Center and enable enforcement when confident after monitoring

Measure progress with security posture reports



- Demonstrate you have a handle on risk for cyber insurance and standard compliance purposes
- Track risk management improvements through historical reports
- Show progress to management with customizable reports

Iterate until your posture is where it needs to be

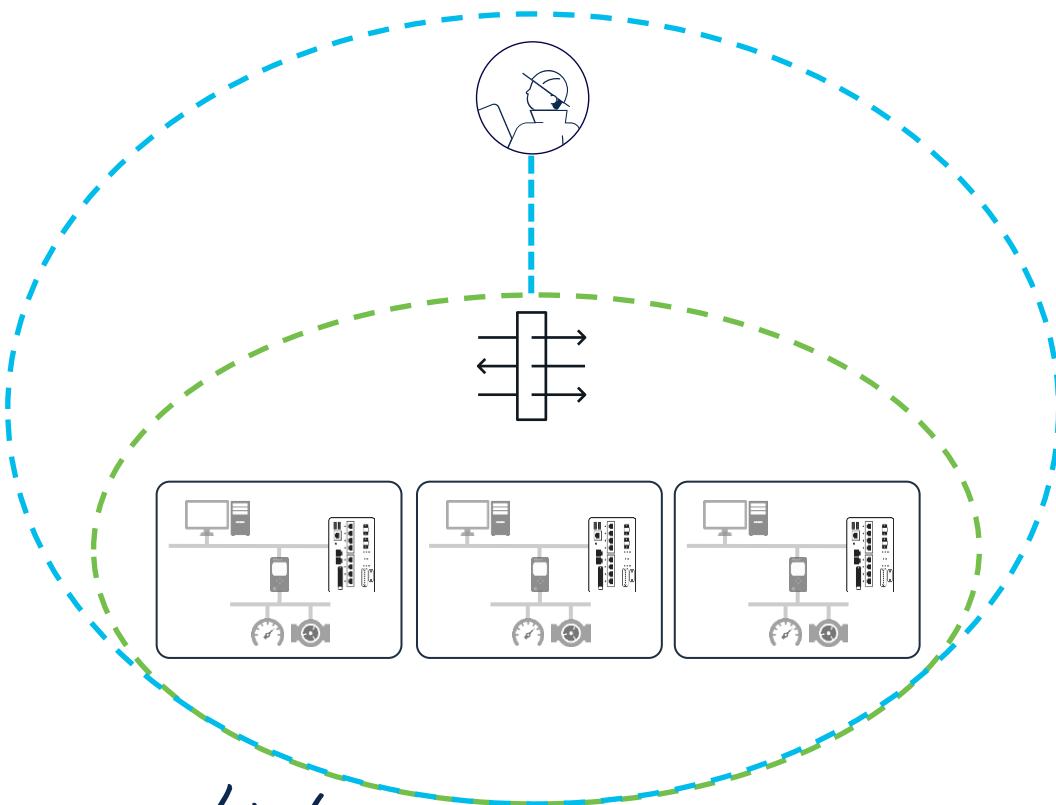


Endpoint risk score indicates what is impacting the current scoring, and shows the best achievable score

Remote Access Technologies



Virtual Private Network (VPN)



- Extends the network to remote users

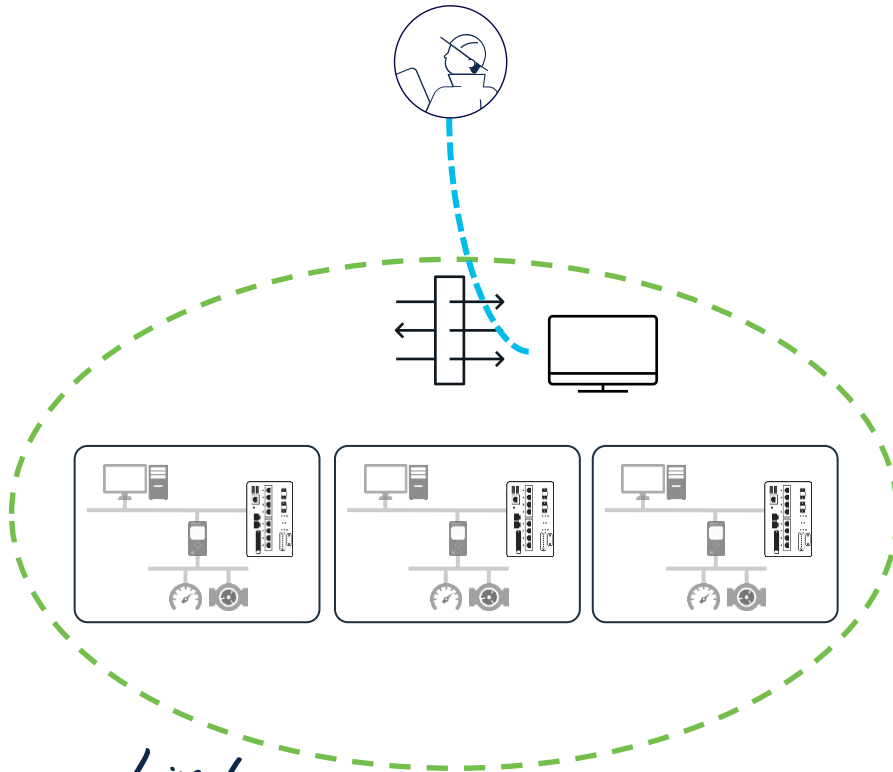
Pros

- Users can use applications hosted natively on their devices
- Minimal friction from end user experience

Cons

- Users have an IP address on your network
- Additional steps for lateral movement and reconnaissance to be prevented
- VPN headend has public IP that will be targeted
- Client can sometimes be a burden
- MFA an additional add-on

Jump Servers



- Users do all their tasks from a trusted device hosted in the network

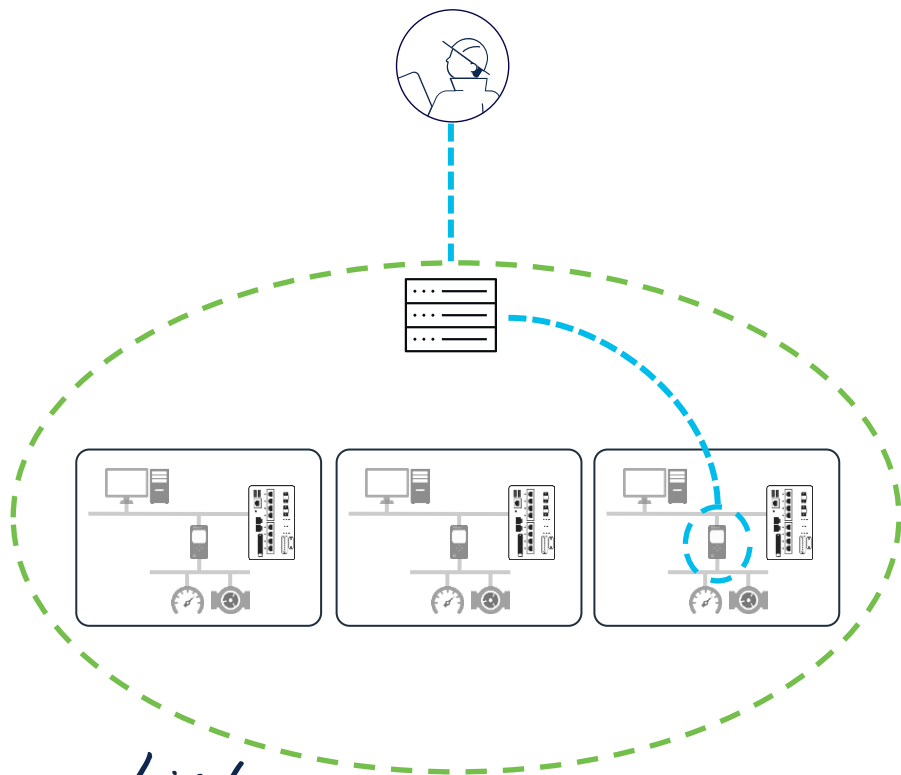
Pros

- Minimize the risk of introducing malware from client device
- Devices can be locked down to only permitted applications
- Jump servers can reside in isolated state until needed

Cons

- Additional overhead often leads to over privileged jump servers
- Must maintain vendor applications
- MFA still not a hard requirement

Shift to Zero Trust Network Access (ZTNA)



- Users have proxied access to specific endpoints / applications

Pros

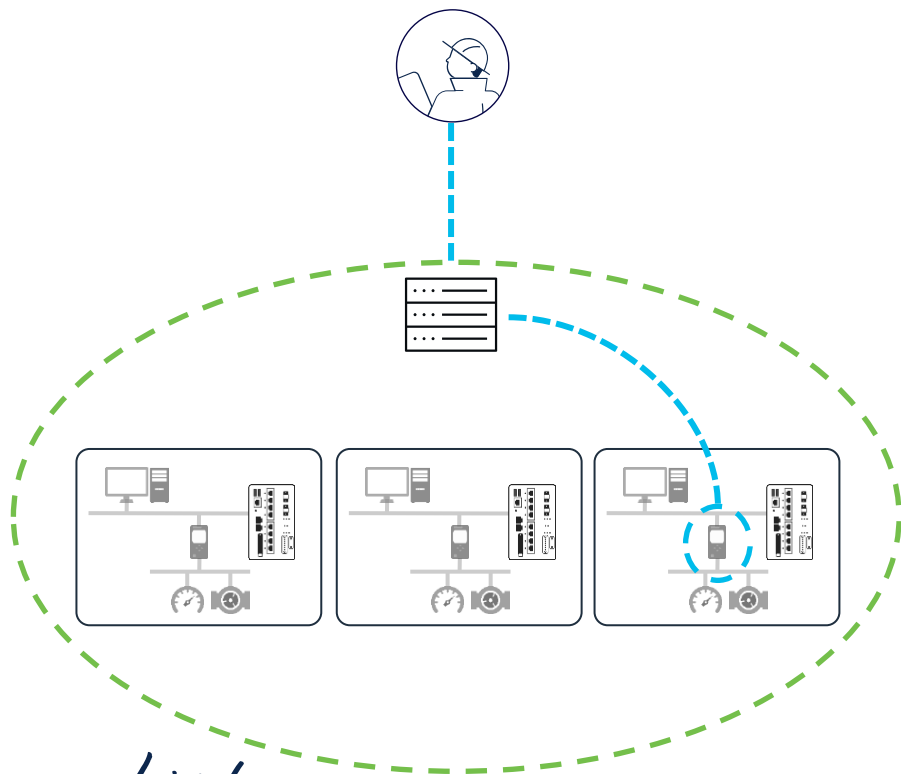
- Users only have access to what they need
- MFA is natively built in
- Clientless connectivity
- ZTNA gateway establishes outbound connection to a trusted cloud*

*some solutions can offer ZTNA gateway to be first point of entry

Cons

- Clientless connectivity does not cover every protocol
- Clients will be needed in some cases

Remote Privileged Access Management (RPAM)



- Very similar to ZTNA, but with extended features

Pros

- Users only have access to what they need
- MFA is natively built in
- Scheduled Access
- Session Monitoring and Recording
- Session Approval flows

Cons

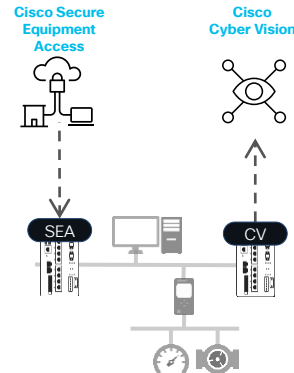
- Clientless connectivity does not cover every protocol
- Clients will be needed in some cases

How SEA Can Help

ZNTA access into OT
assets problem

2

Security Posture & ZTNA of OT Assets



Remote access to OT assets is key for operations

Secure Remote Access for OT

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

What do IT and OT users want?

Secure Remote Access for OT



Operational Efficiency

- ✓ Gain instant access to remote assets from anywhere in case of emergencies
- ✓ Be capable of easily creating remote access credentials when needed
- ✓ Be able to use any remote access protocol depending on the need
- ✓ Access to audit trails to understand what changes have been made to an asset



Cybersecurity

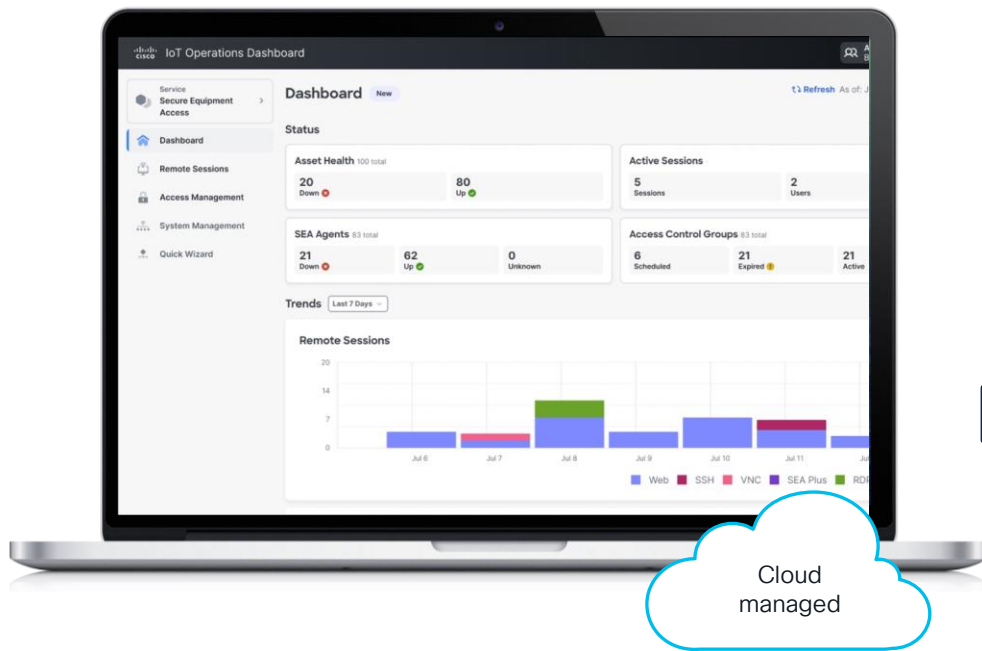
- ✓ Ensure only legitimate users can connect, and never to the entire network
- ✓ Verify remote computers' posture to avoid malware
- ✓ Simplify architecture to lower costs and avoid complex DMZ/firewall setups
- ✓ Have access to audit trails for regulatory compliance and investigations

Modern industrial operations require both OT agility and IT security

Cisco Secure Equipment Access

Purpose-built for Industrial and OT

IoT Operations Dashboard



Centralised cloud enforced policy
Define and enforce ZTNA controls with a cloud-based trust broker



Install and scale with ease
Deploy and monitor network embedded ZTNA gateway agents at scale from the cloud

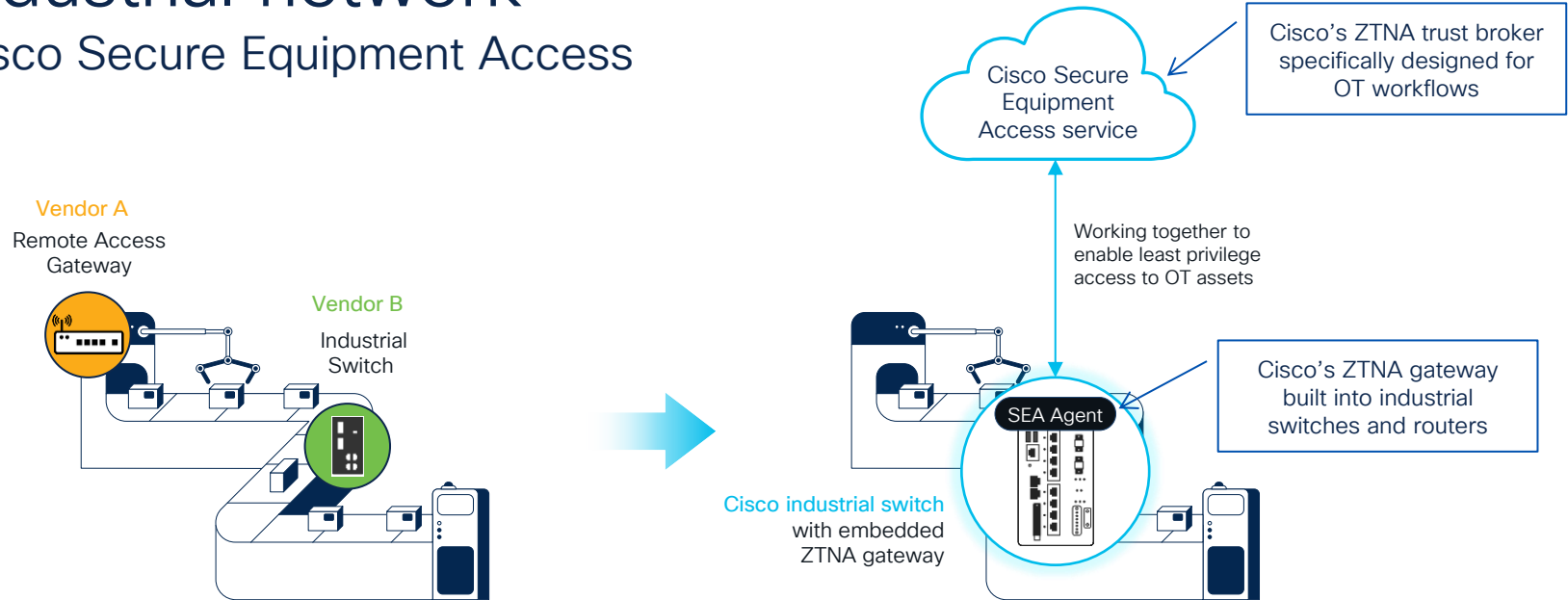


Access any remote asset the way you want
Connect any OT asset to a Cisco IE switch or IR router and securely access it from anywhere in the world

Cloud managed

Zero Trust Network Access (ZTNA) built into your industrial network

Cisco Secure Equipment Access



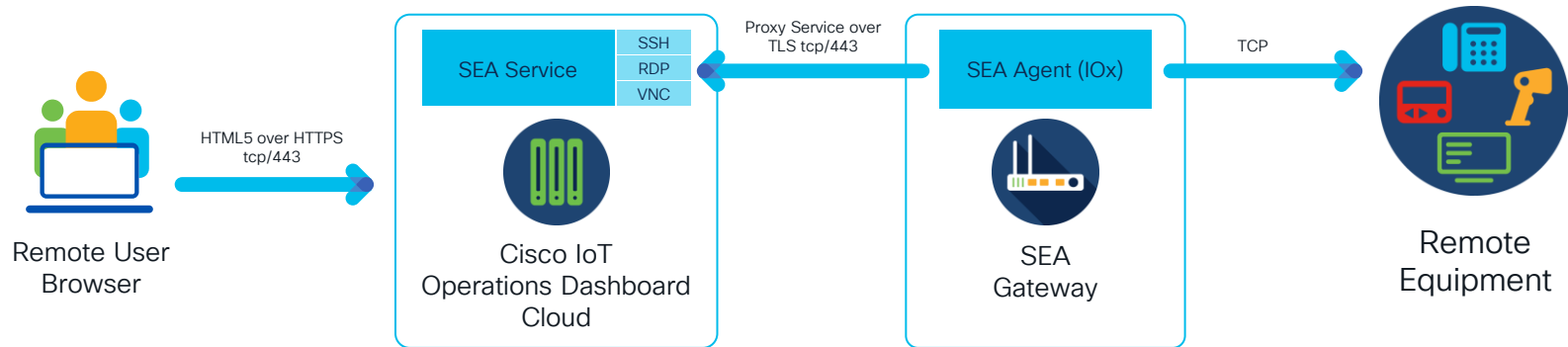
Eliminating complexity by converging functionalities as software features on Cisco's industrial network

Cisco Secure Equipment Access SEA and SEA Plus

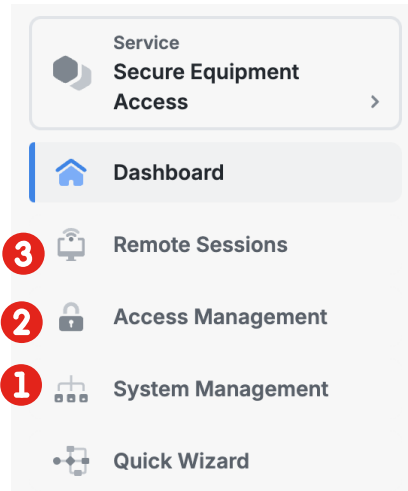
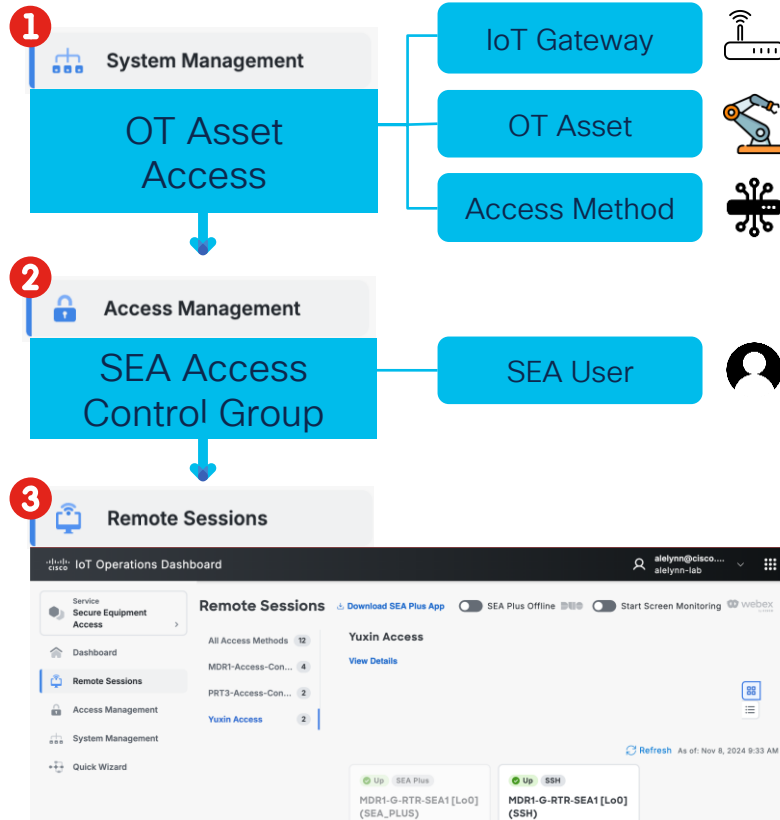


SEA Flow

- No installation required: equipment access through browser
- Proxy: SEA Agent on Gateway is a proxy over TLS/443
- Isolation: remote user is never directly connected to remote network

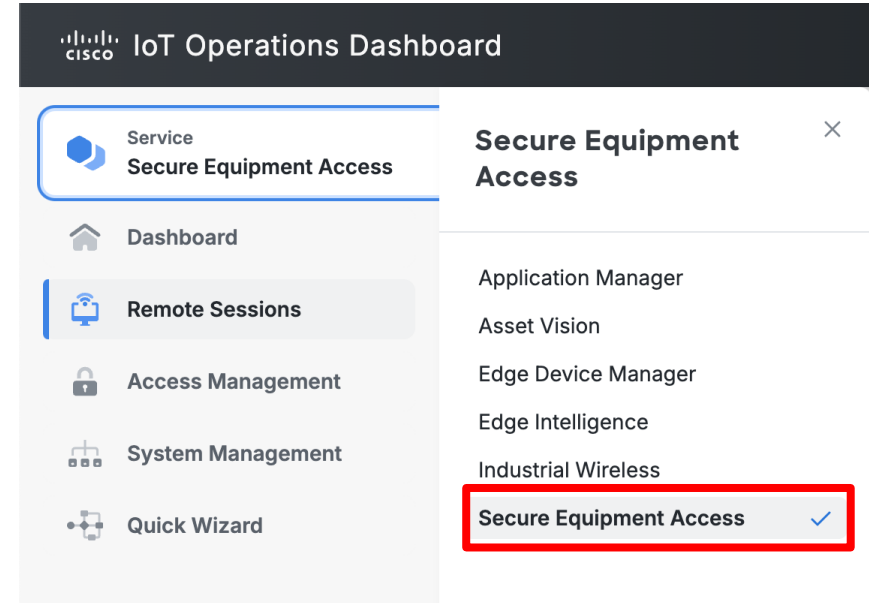


SEA Configuration Overview



How to access SEA Service ?

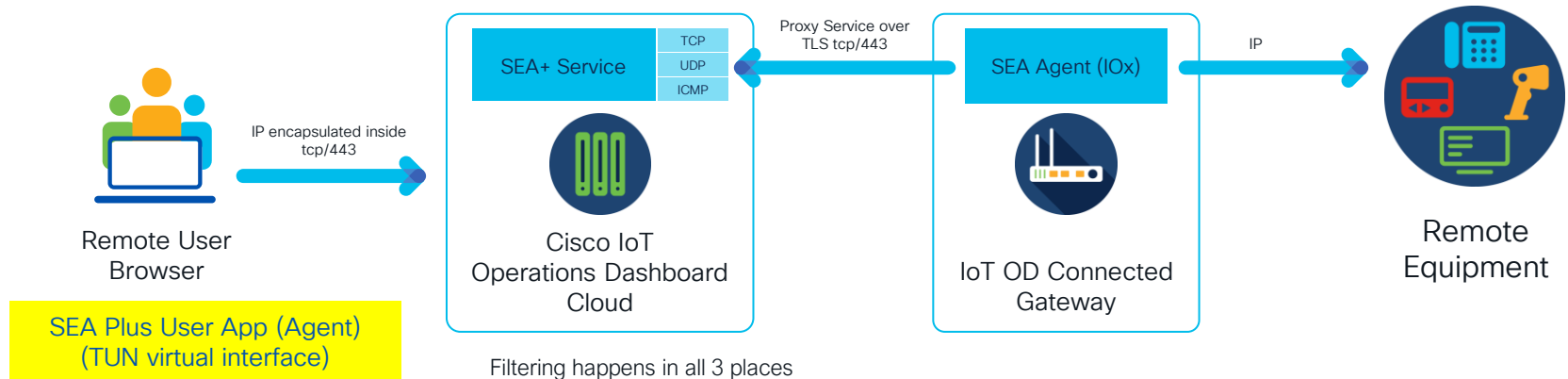
- Login to Cisco IoT Operations Dashboard
EU cluster <https://eu.ciscoiot.com>
US cluster <https://us.ciscoiot.com>
- On the left panel, in Services, switch to “**Secure Equipment Access**”
- If you don't see Secure Equipment Access, you may need to purchase an additional license. Contact your account team.



This view can be different based on your license

SEA Plus Flow

- Agent installation is **required** – creates TUNTAP virtual network device
- TUN devices runs inside SEA TLS/443
- Remote user computer routes changed to use TUN device
- Remote user is **directly connected** to remote network – with ZTNA therefore only allowing what's been explicitly permitted



- Filtering happens in all 3 places
1. in Windows SEA Plus app,
 2. in Cloud, and
 3. in IOx SEA app.

SEA Plus Creates on virtual TUN interface

```
PS C:\Users\Emmanuel Tychon> ipconfig /allcompartments

Windows IP Configuration

=====
Network Information for Compartment 1 (ACTIVE)
=====

Unknown adapter sea:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::5055:0370:2a6a:717%40
    IPv4 Address. . . . . : 169.254.65.176
    Subnet Mask . . . . . : 255.255.255.255
    Default Gateway . . . . . : 

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : local
    IPv6 Address. . . . . : 2a02:2788:925:e359:c98f:b501:8201:2188
    Temporary IPv6 Address. . . . . : 2a02:2788:925:e359:b94d:9c77:c6bb:d7f7
    Link-local IPv6 Address . . . . . : fe80::c98f:b501:8201:2188%9
    IPv4 Address. . . . . : 192.168.2.29
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : fe80::46ae:25ff:fea0:f774%9
    192.168.2.1
```

```
PS C:\Users\Emmanuel Tychon> route print -4

=====
Interface List
40.....WireGuard Tunnel
 9...c8 5b 76 dd c1 0a .....Realtek PCIe GBE Family Controller
 2...f0 d5 bf aa f5 00 .....Intel(R) Dual Band Wireless-AC 8260
 1.....Software Loopback Interface 1
11...00 00 00 00 00 00 e0 Microsoft Teredo Tunneling Adapter
=====

IPv4 Route Table
=====
Active Routes:
Network Destination        Netmask          Gateway          Interface        Metric
0.0.0.0                    0.0.0.0          192.168.2.1      192.168.2.29     25
10.10.20.50                255.255.255.255  On-link          169.254.65.176   261
127.0.0.0                  255.0.0.0        On-link          127.0.0.1        331
127.0.0.1                  255.255.255.255  On-link          127.0.0.1        331
127.255.255.255            255.255.255.255  On-link          127.0.0.1        331
169.254.65.176             255.255.255.255  On-link          169.254.65.176   261
169.254.88.31              255.255.255.255  169.254.65.176  169.254.65.176   261
192.168.2.0                255.255.255.0    On-link          192.168.2.29     281
192.168.2.29               255.255.255.255  On-link          192.168.2.29     281
192.168.2.255              255.255.255.255  On-link          192.168.2.29     281
224.0.0.0                  240.0.0.0        On-link          127.0.0.1        331
224.0.0.0                  240.0.0.0        On-link          192.168.2.29     281
224.0.0.0                  240.0.0.0        On-link          169.254.65.176   261
255.255.255.255            255.255.255.255  On-link          127.0.0.1        331
255.255.255.255            255.255.255.255  On-link          192.168.2.29     281
255.255.255.255            255.255.255.255  On-link          169.254.65.176   261
=====
Persistent Routes:
None
```

SEA Plus Access Control Lists

IoT Operations Dashboard | alelynn@cisco... | alelynn-lab

System Management [Refresh](#) As of: Nov 06 2024 04:25 PM

Network Devices | Assets | **SEA Plus Protocols** | More ▾

Protocol Definition Details

Name * Tag Description

Allowed Protocols [+ Add Protocol](#) As of: Nov 6, 2024 4:25 PM

Protocol ▾	Port(s)	Actions
ICMP	-	...
TCP	502	...

[Save](#) [Cancel](#)

IoT Operations Dashboard | alelynn@cisco... | alelynn-lab

MDR1-G-RTR-SEA1

Asset Details

[Edit](#) [Delete](#)

IP Address/Host Name
172.20.12.239

Network Device
MDR1-G-RTR-SEA1

Description
—

Edit Access Method ✕

Access Method Details

Access Method SEA Plus

Add Protocol Definitions & Port Configuration

[All](#) [Custom](#) [Predefined](#)

Protocol Definition *

▾

☐ Advanced Settings

Access Name

Name *

Description

SEA vs SEA Plus

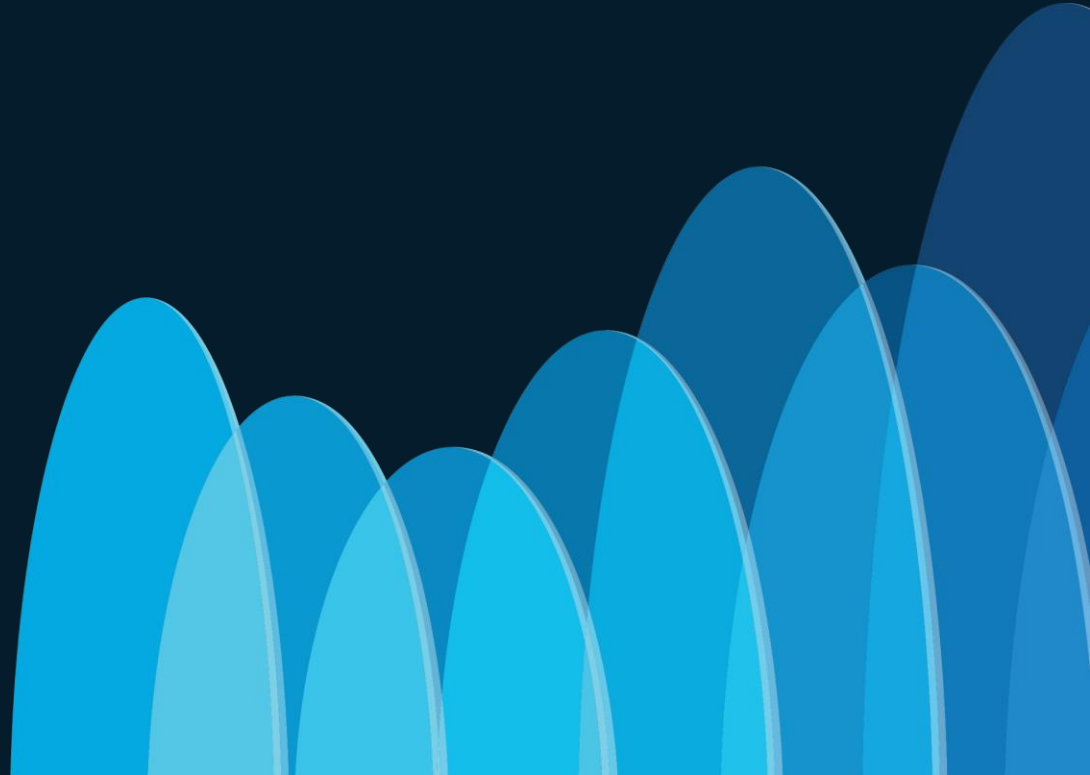
- SEA is **easier** to use
- **More secure** with IP isolation
- To be used, when possible, for:
 - SSH
 - VNC
 - RDP
 - Telnet
 - Web
- SEA Plus requires Windows installation of the SEA Plus User Application, and Windows admin privileges to do so
- SEA Plus is **more flexible**
- Can provide **direct IP connectivity** (ie. to a native client such as Profinet programmer)
- Allows file transfer (ie. with SFTP)

Use both SEA and SEA Plus for different use cases
It always follows the ZTNA principles

SEA Support Matrix

Platform	IoT OD Application Manager (externally managed)	SEA Support	Recommended Minimum IOS-XE Release
IR18xx	Yes	Yes	17.15.1
IR1101	Yes	Yes	17.15.1
IE3400H	Yes	Yes	17.15.1
IE3400	Yes	Yes	17.15.1
IE3300	Yes	Yes <small>(4GB of RAM models)</small>	17.15.1
IE31xx	Yes	Yes	17.15.1

Cisco Secure Equipment Access Session Management



Features for Session Monitoring

- SEA Admin can:
 - join active sessions to monitor activity in real time
(Only for RDP, VNC, SSH and Telnet)
 - immediately terminate an active session
 - see Session History
 - view inline session recordings stored on AWS S3
 - see audit information
- Logs can be seen, but cannot be exported to any Security Information and Event Management (SIEM) system

Accessing and Terminating Sessions

The screenshot displays the Cisco IoT Operations Dashboard. The top navigation bar includes the Cisco logo, the title "IoT Operations Dashboard", and a user profile for "alelynn@cisco...." with a dropdown arrow and a grid icon. The left sidebar contains a "Service Secure Equipment Access" menu item and a list of navigation options: Dashboard, Remote Sessions, Access Management (highlighted), System Management, and Quick Wizard. The main content area is titled "Access Management" and includes a "Refresh" button and a timestamp "As of: Nov 08 2024 09:38 AM". Below the title are tabs for "Access Control Groups", "Users", "Active Sessions" (selected), "Session History", "Pending Requests", and "Request History". A search bar labeled "Search Table" is positioned above a table. The table has columns for "Asset", "Access Method", "User", "Session Start", "Schedule Duration", "Monitor", and "Security". A single record is shown for the asset "MDR1-G-RTR-SEA1 [Lo0]" with access method "MDR1-G-RTR-SEA1 [Lo0] (SSH)" and user "alelynn@cisco.com". The session started "a minute ago" and is "Unscheduled". In the "Monitor" column, there are two buttons: a green "Join Session" button and a red "Terminate" button. Below the table, it indicates "1 Records" and a pagination control showing "Show Records: 10" and "1 - 1".

Asset	Access Method	User	Session Start	Schedule Duration	Monitor	Security
MDR1-G-RTR-SEA1 [Lo0]	MDR1-G-RTR-SEA1 [Lo0] (SSH)	alelynn@cisco.com	a minute ago	Unscheduled	Join Session	Terminate

Join Session

Terminate Session

Session History

IoT Operations Dashboard

alelynn@cisco...
alelynn-lab

Service Secure Equipment Access

Dashboard

Remote Sessions

Access Management

System Management

Quick Wizard

Access Management

Access Control Groups

Users

Active Sessions

Session History

Pending Requests

Request History

Refresh As of: Nov 08 2024 09:38 AM

Start date → End date ☐ Only Show Recorded Sessions

Download

Search yuxinzha

Session Start	Session End	Asset	Access Method	User	Total Bytes	Terminated	Recorded	Actions
Sep 10, 2024 2:16 PM	Sep 10, 2024 2:20 PM	MDR1-G-RTR-SEA1 [Lo0]	MDR1-G-RTR-SEA1 [Lo0] (SSH)	yuxinzha@cisco.com	16.90 KB	No	No	...
Sep 5, 2024 10:41 AM	Sep 5, 2024 10:45 AM	MDR1-G-RTR-SEA1 [Lo0]	MDR1-G-RTR-SEA1 [Lo0] (SSH)	yuxinzha@cisco.com	19.14 KB	No	No	...
Aug 16, 2024 4:05 PM	Aug 16, 2024 4:07 PM	MDR1-G-RTR-SEA1 [Lo0]	MDR1-G-RTR-SEA1 [Lo0] (SSH)	yuxinzha@cisco.com	4.46 KB	No	No	...
Aug 16, 2024 4:01 PM	Aug 16, 2024 4:26 PM	MDR1-G-RTR-SEA1 [Lo0]	MDR1-G-RTR-SEA1 [Lo0] (SEA_PLUS)	yuxinzha@cisco.com	0 Bytes	No	No	...
Aug 16, 2024 4:01 PM	Aug 16, 2024 4:03 PM	MDR1-G-RTR-SEA1 [Lo0]	MDR1-G-RTR-SEA1 [Lo0] (SSH)	yuxinzha@cisco.com	11.60 KB	No	No	...
Aug 16, 2024 3:56 PM	Aug 16, 2024 3:59 PM	MDR1-G-RTR-SEA1 [Lo0]	MDR1-G-RTR-SEA1 [Lo0] (SSH)	yuxinzha@cisco.com	4.37 KB	No	No	...

6 Records

Show Records: 10 1 - 6

CISCO Live!

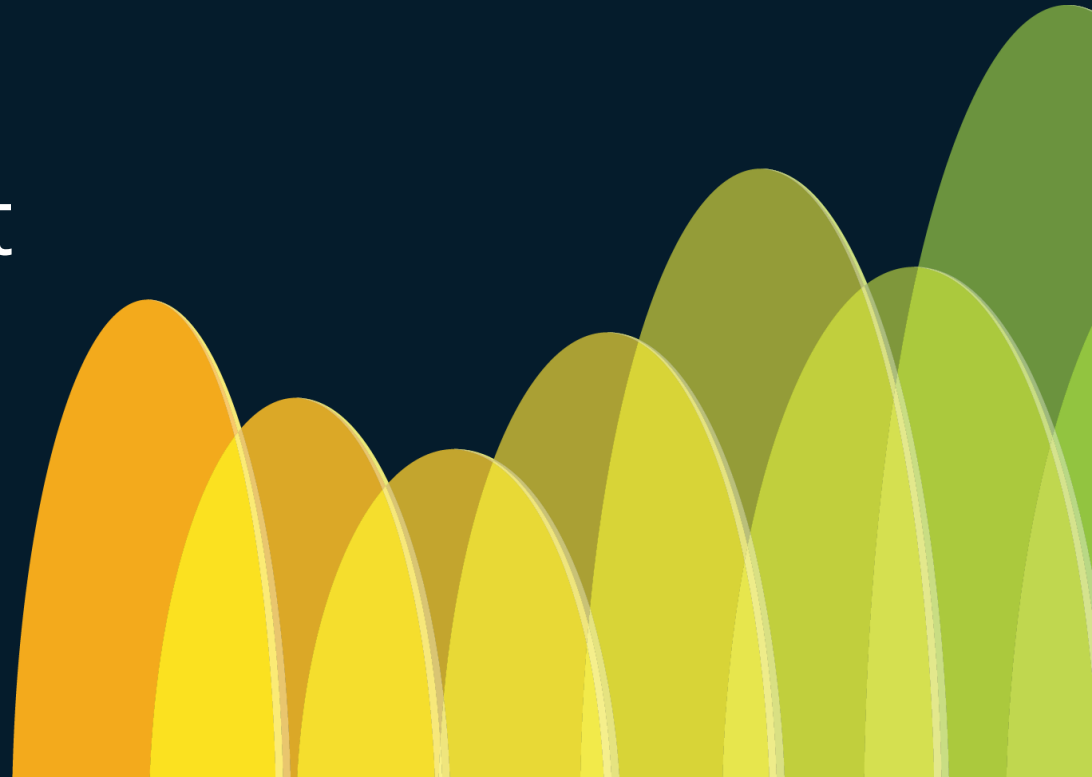
#CiscoLiveAPJC

BRKIOT-2081

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

57

Cisco Secure Equipment Access Session Request and Approval



Remote User Benefits

- Can **request access** to a remote asset
- Request is routed to a list of **approvers**
- Once approved – user gets **instant access** for the requested duration

Administrator Benefits

- No need to pro-actively add users to group – they request when needed
- Simple approve / deny / revoke action to be done by approvers
- Approvers and Administrators can be separate users

Simple "Remote User" workflow

- Request, approve, and access:



For maximum granularity and security, access is not granted to the whole group, but only to the specific asset(s) and access method(s) that have been requested and approved.

Cisco Secure Equipment Access VLAN Access



VLAN Access on IE Switches for SEA Agent

- For switches, when installing SEA, you can configure access to up to 9 VLANs.
- For each VLAN you can use a dynamic (DHCP address) or configure a static IP address.
- Multiple interfaces will be created inside IOx, each in their respective assigned VLAN
- No overlapping IP addresses between VLANs
- Note: the IOx port must be in trunking mode, for example:

```
interface AppGigabitEthernet1/1
switchport trunk native vlan 4094
switchport mode trunk
```

Edit Additional Configuration

☒ VLAN

Default VLAN

VLAN ID* IP Assignment

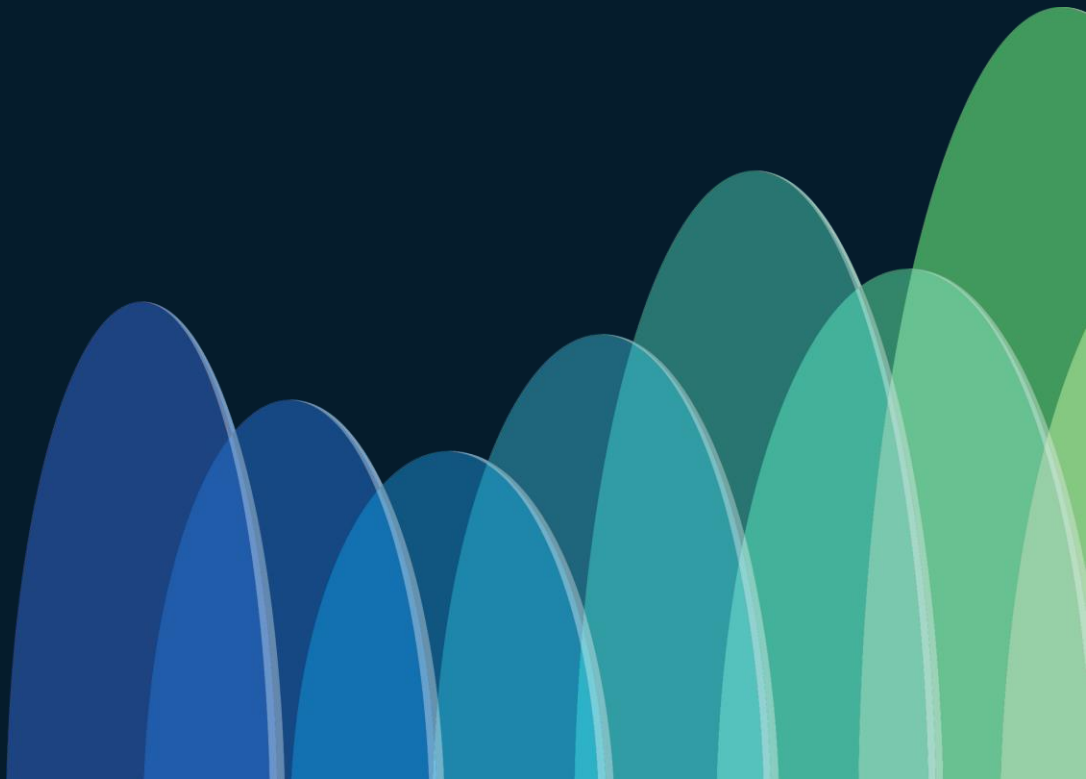
VLAN range: 1-4093

Add Up to 9 Additional VLANs

VLAN ID	IP Assignment	IP Address / Subnet Mask
☐ 10	Static IP	IP Address* <input type="text" value="10.10.10.10"/> / Subnet Mask* <input type="text" value="24"/>
VLAN range: 1-4093		
☐ 100	Dynamic IP	
VLAN range: 1-4093		
☐ 101	Dynamic IP	
VLAN range: 1-4093		
☐ 102	Dynamic IP	
VLAN range: 1-4093		
☐ 103	Dynamic IP	
VLAN range: 1-4093		
☐ 104	Dynamic IP	
VLAN range: 1-4093		
☐ 105	Dynamic IP	
VLAN range: 1-4093		

```
eth7:
  MAC address : 52:54:dd:bb:2b:f1
  IPv6 address : ::
  Network name : mgmt-bridge-v105
  Multicast : No
  Mirroring : No
eth6:
  MAC address : 52:54:dd:c6:fe:9c
  IPv6 address : ::
  Network name : mgmt-bridge-v104
  Multicast : No
  Mirroring : No
eth5:
  MAC address : 52:54:dd:cd:44:a5
  IPv6 address : 192.168.2.152
  Network name : mgmt-bridge-v1
  Multicast : No
  Mirroring : No
eth4:
  MAC address : 52:54:dd:d9:91:53
  IPv6 address : ::
  Network name : mgmt-bridge-v102
  Multicast : No
  Mirroring : No
eth3:
  MAC address : 52:54:dd:f6:84:fb
  IPv6 address : ::
  Network name : mgmt-bridge-v100
  Multicast : No
  Mirroring : No
eth2:
```

IOS + Linux, or IOx

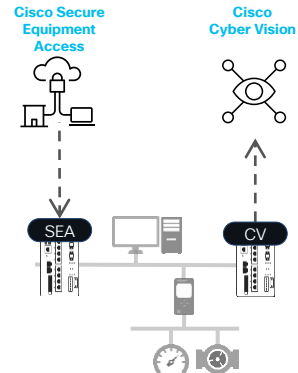


How IOx Can Help

The Network as a sensor,
or an access gateway

2

Security Posture & ZTNA of OT Assets



Application Hosting, What is it?

Local Compute



- At the edge of the network
- No dedicated server HW needed
- Fanless & I-Temp

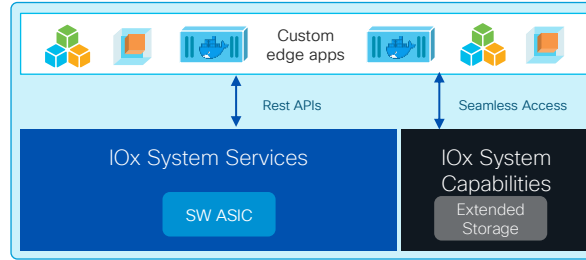
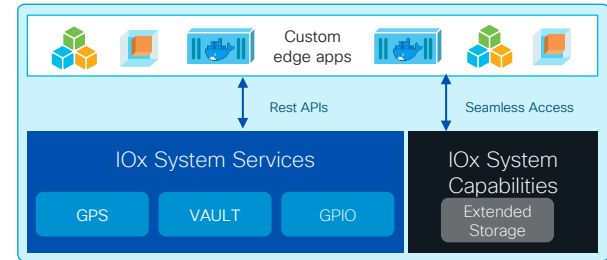
Docker support

- Uses lightweight containers
- Runs native docker images
- Provides familiar tooling



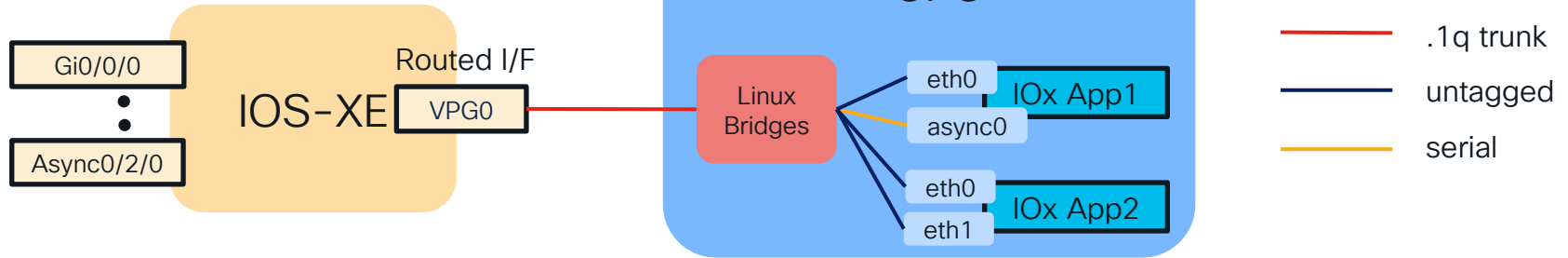
Developer Support

- Cisco DevNet Ecosystem

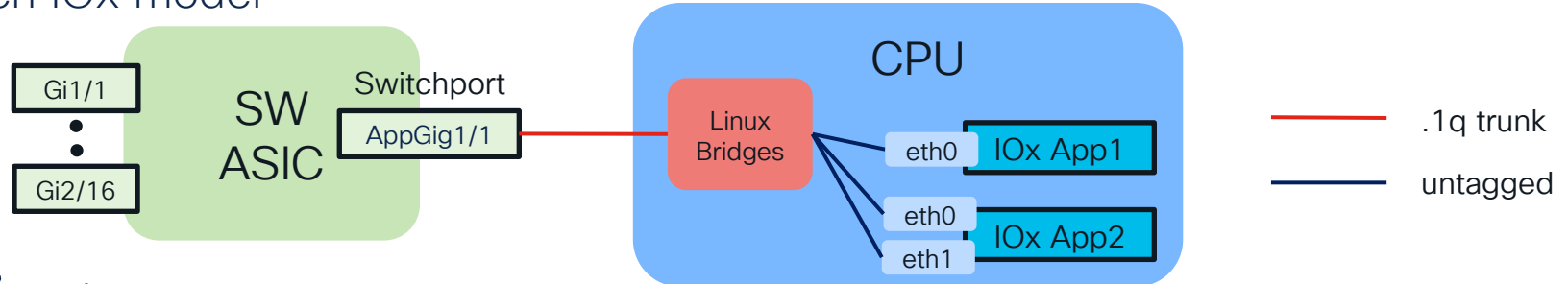


I/O Model Abstracts

Router IOx model



Switch IOx model



Platforms that support SEA Agent

SEA Agent is the ZTNA gateway function embedded in network platforms

Industrial Switches



IE3300, IE3400



IE3400H



IE3100



IE9300

Industrial Routers



IR1101



IR1800



IR8300

Turning the Network into an Asset Inventory Sensor



The Role of the Cyber Vision Sensor

Collects Industrial Network Traffic



Captures industrial network flows (passive) and queries devices (active). Stores data locally in case the Center is not accessible

Decodes Industrial Protocols (DPI)



Understands most OT and IT communication protocols to analyze packet payloads and extract meaningful information

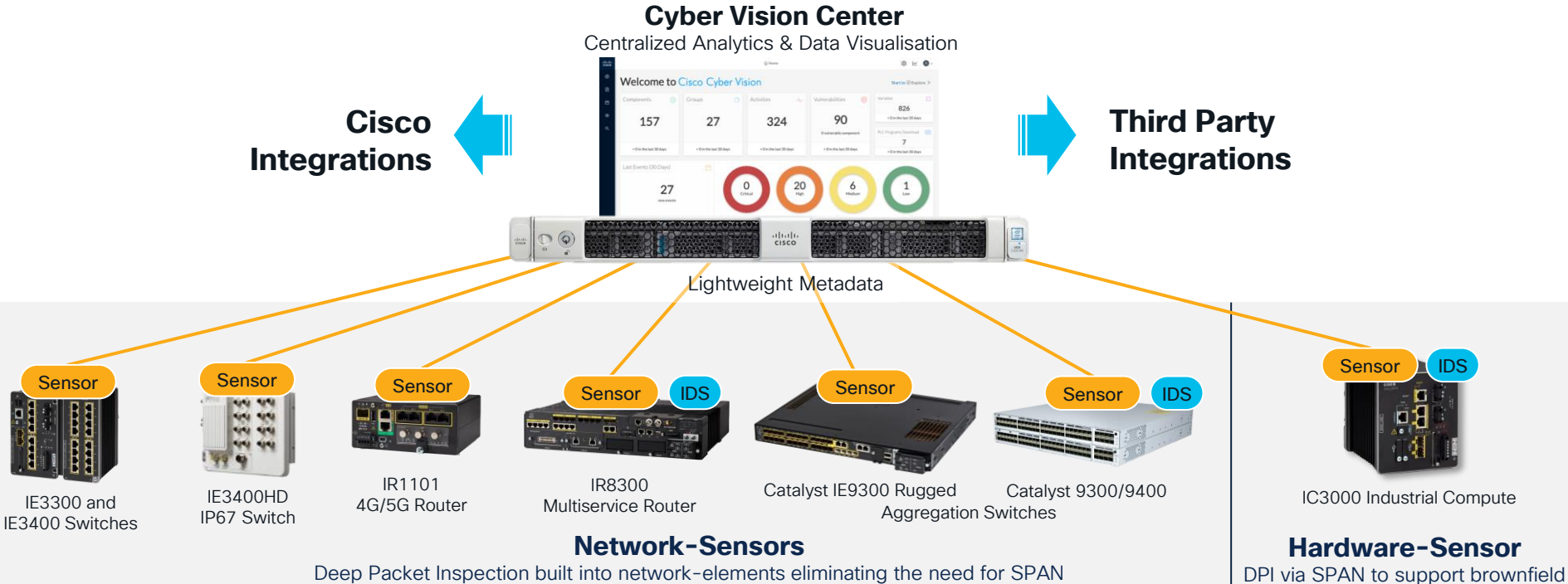
Sends Metadata to the Cyber Vision Center



Sends metadata to the Center for storage, analysis and visualisation. This only adds 2 to 5% extra traffic to the network

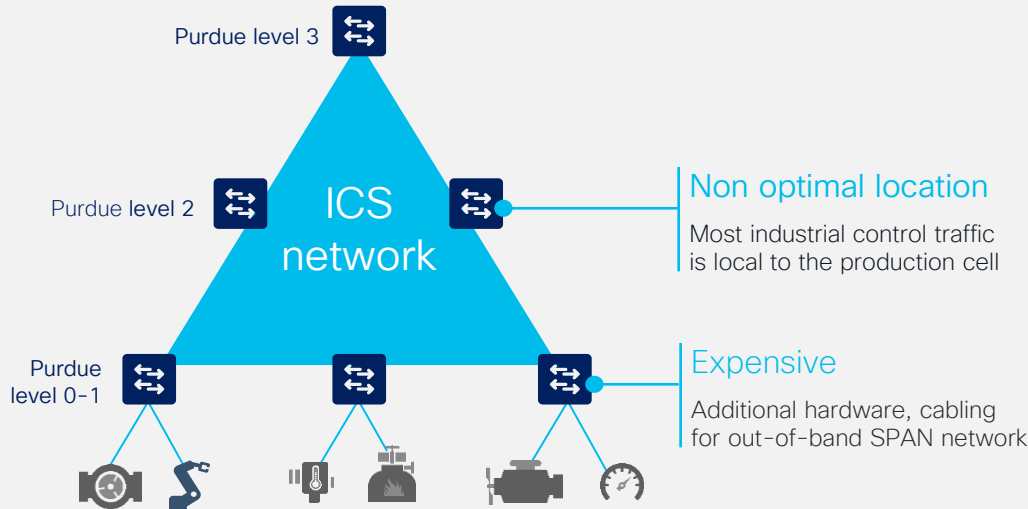
Security That Scales With Your Infrastructure

Visibility and threat detection built into your industrial network



Why is a network-sensor important?

Most industrial network traffic is East-West, not North-South



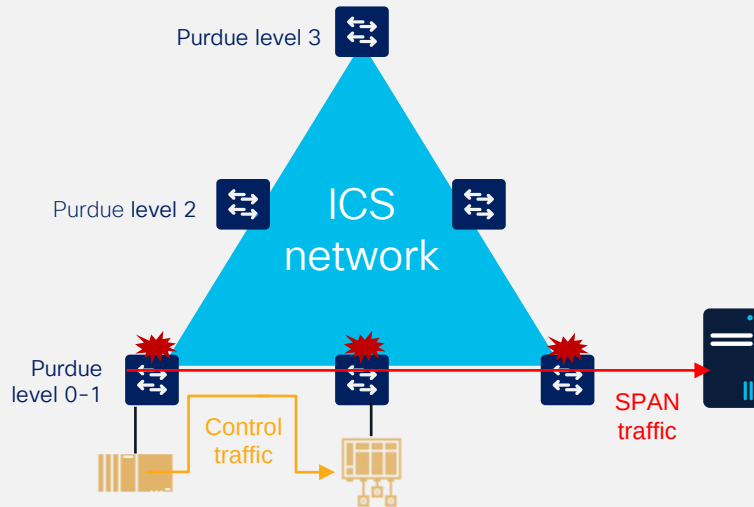
DPI location matters!

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

A sensor embedded in the network sees everything that attaches to it

Why is a network-sensor important?

RSPAN is not a viable option for control system networks



RSPAN introduces Jitter & Latency!

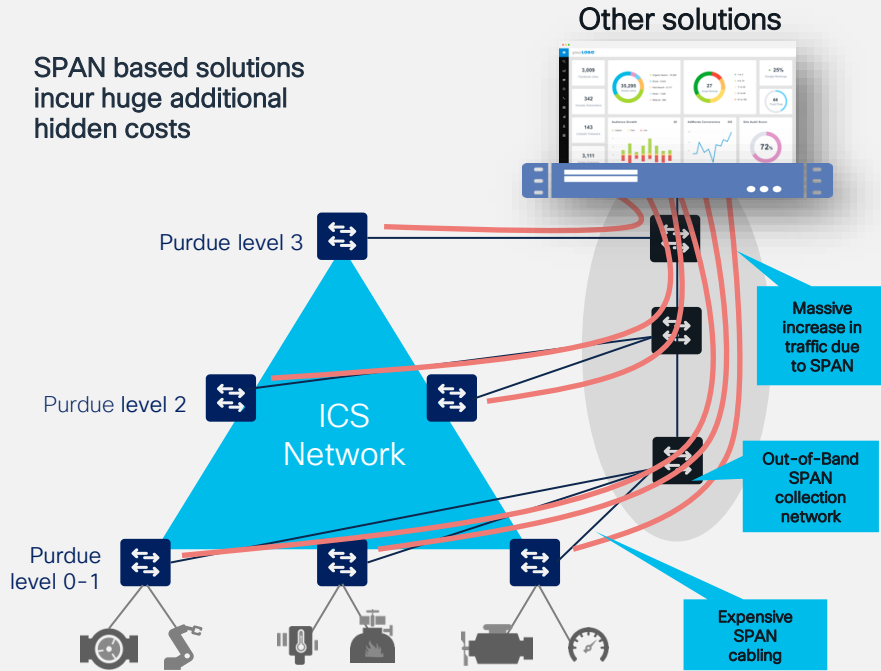
- Head-of-line blocking caused by Inline SPAN traffic negatively impacts time-sensitive control loop
- RSPAN in LANs is detrimental to control system performance

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

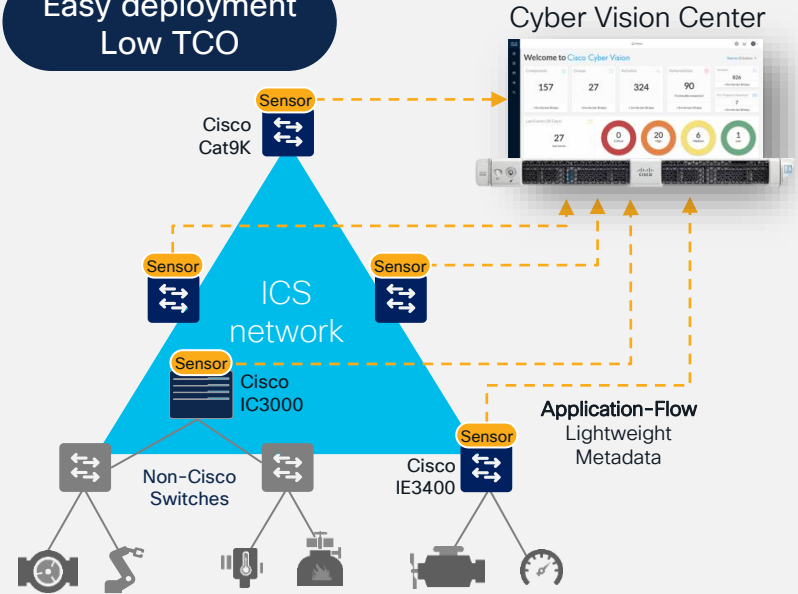
Why is a network-sensor important?

Visibility you can deploy at scale without the need for costly SPAN networks

SPAN based solutions
incur huge additional
hidden costs



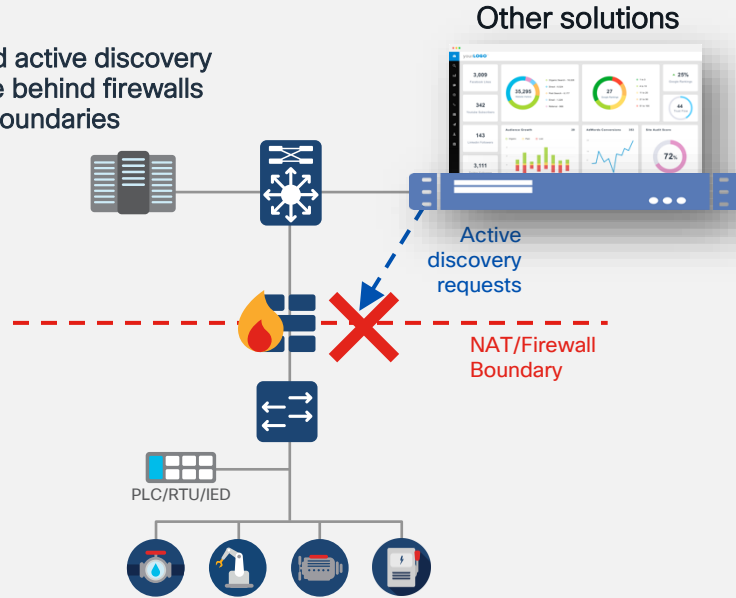
Easy deployment
Low TCO



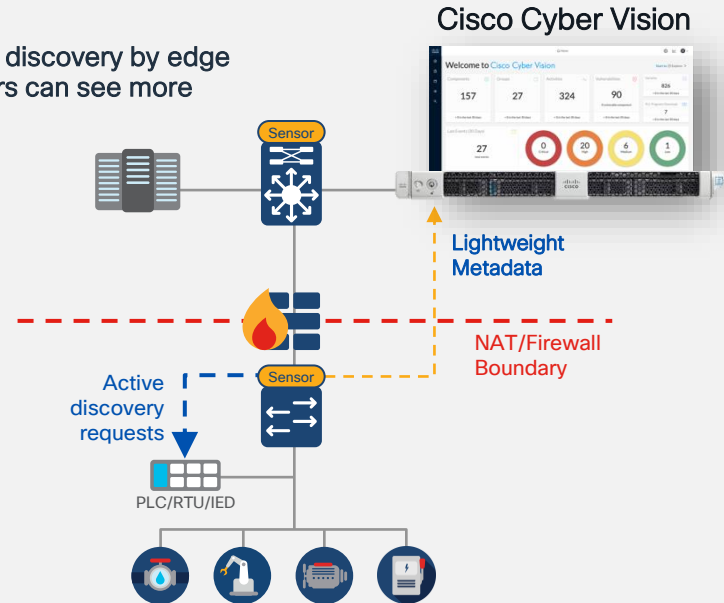
Network-sensor will solve architecture challenge

Distributed edge active discovery gives you 100% visibility

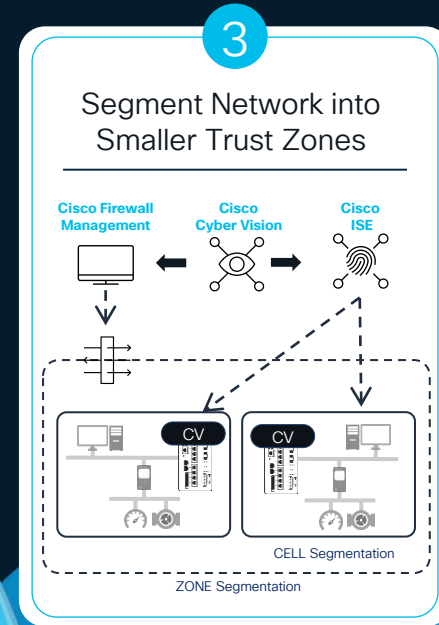
Centralised active discovery cannot see behind firewalls and NAT boundaries



Active discovery by edge sensors can see more

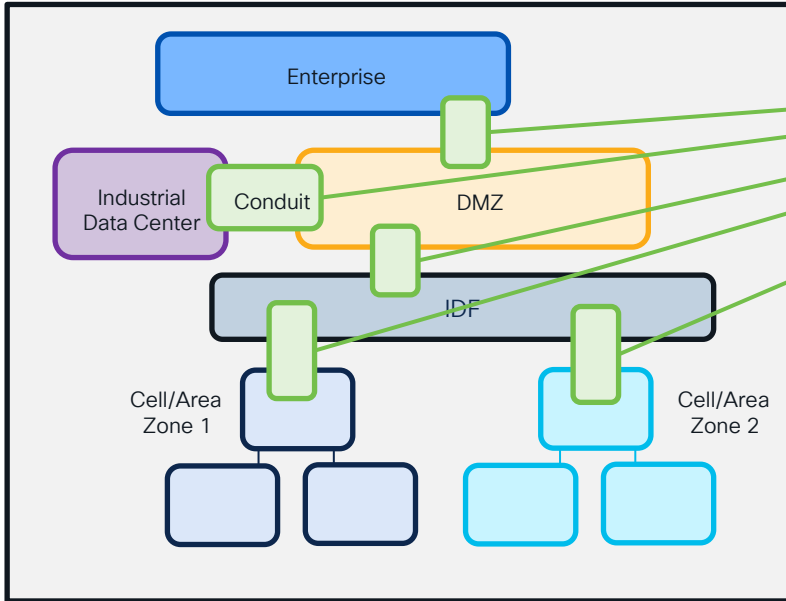
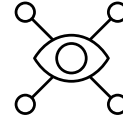


Network Segmentation



The Segmentation Journey – Virtual Segmentation

ISA/IEC 62443

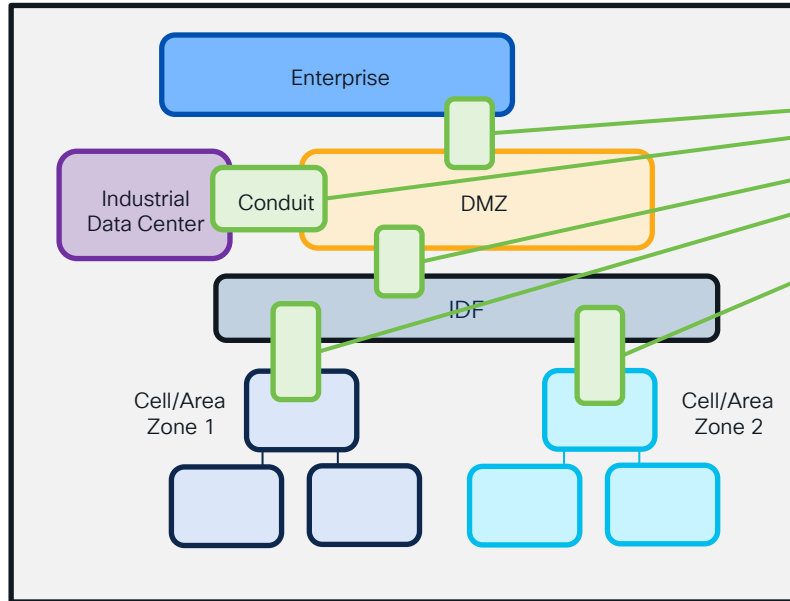


Virtual Segmentation

Visualising the zones and conduits model and reacting to data observed between zones

The Segmentation Journey – Macro Segmentation

ISA/IEC 62443

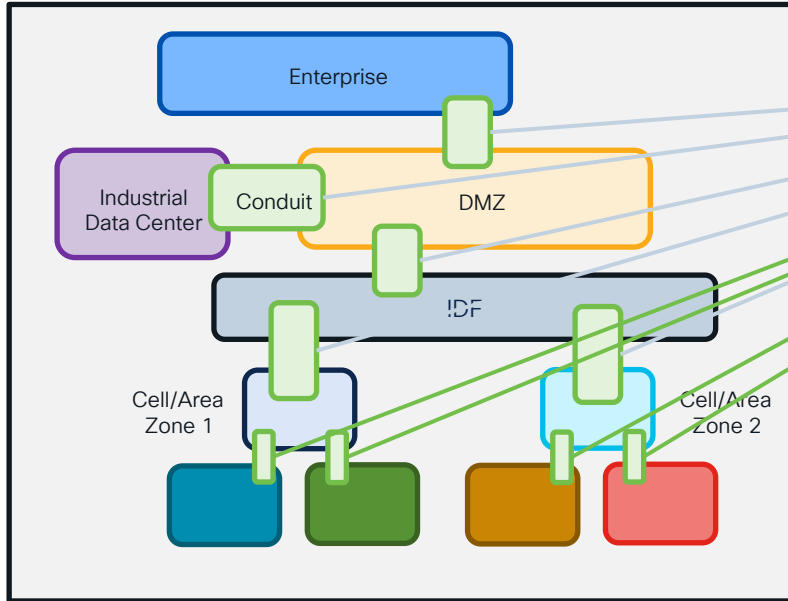


Macro Segmentation

- Pushing policy across “large” zones (between Cell/Area/Zones/Production Lines)
- IDF is typically point of VLAN termination and is a conditioned space

The Segmentation Journey – Micro Segmentation

ISA/IEC 62443

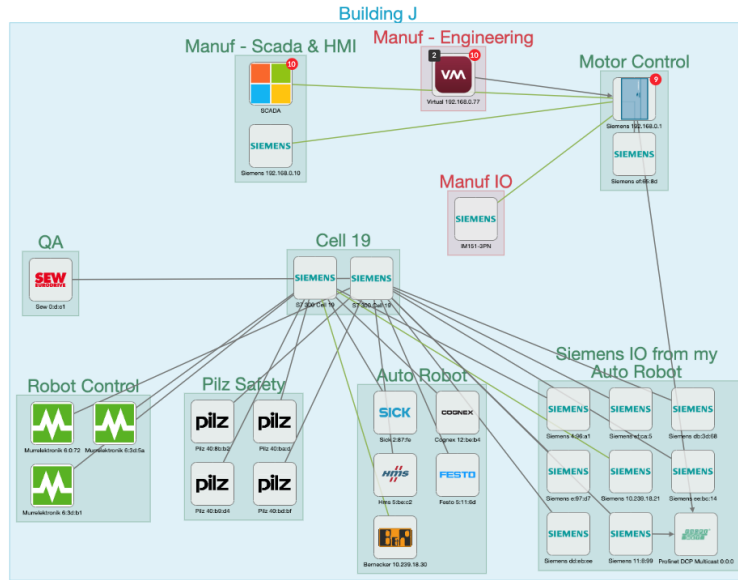


Micro Segmentation

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

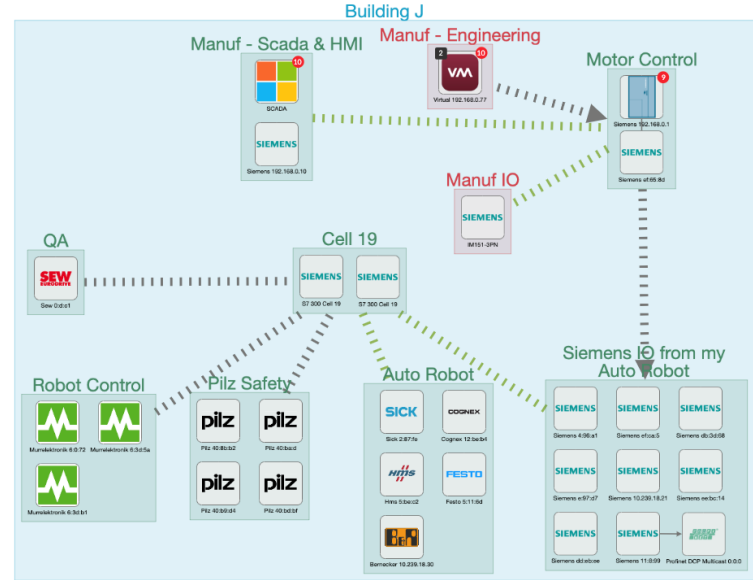
Aggregated activities match IEC62443 conduits

Unaggregated



[View all asset relationships](#)

Aggregated



[Easily browse through conduits](#)

Examine 'Conduits' between 'Zones' with Cyber Vision

Legend

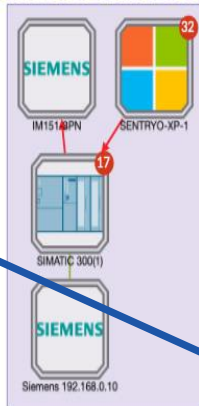
Emerson Vlan 222 - Cell3

PLC 3

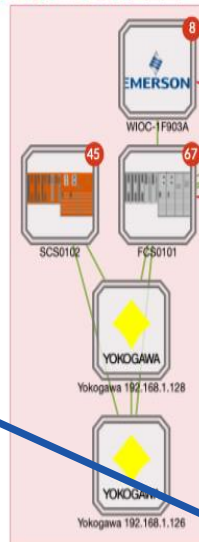
Options

☒ Show network activities

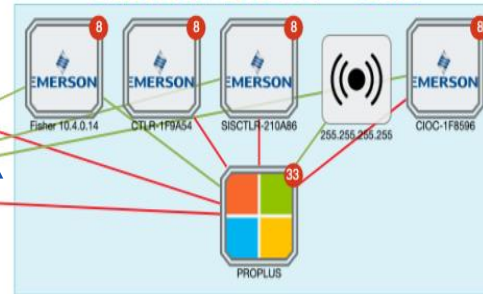
Siemens Vlan Cell 1



Emerson Vlan 222 - Cell3



Emerson Vlan 111 - Cell2



Specific inter-cell flows can be exposed.
If required build micro segmentation policy exceptions for these flows.

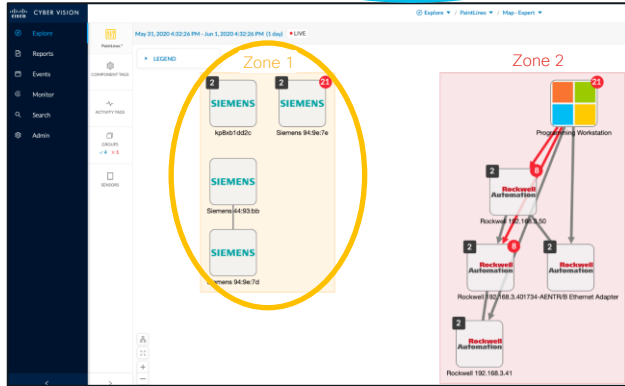
Cyber Vision + ISE Simplifies Segmentation



I can group assets into zones that match my industrial process



I can build security policies that will not disrupt production



Cyber Vision Map View

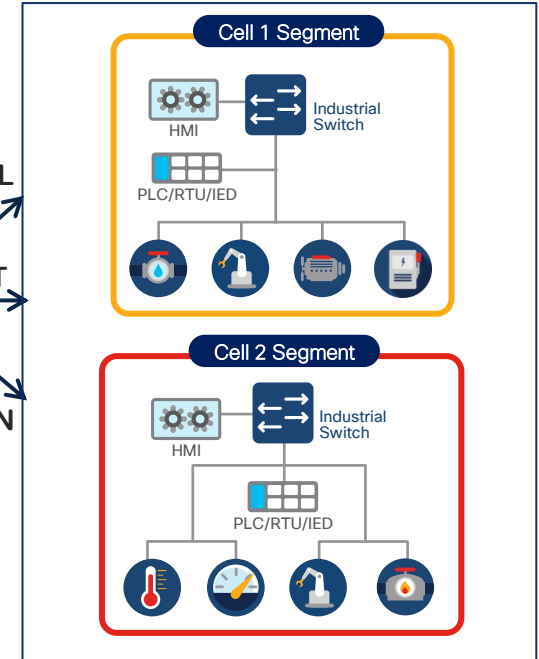
	Zone 1	Zone 2	PLC	MES
Zone 1	✓	✗	✓	✗
Zone 2	✗	✓	✓	✗
PLC	✓	✓	✓	✓
MES	✗	✗	✓	✓

pxGrid update with asset endpoint identities and group Cell1 as custom attribute

Cisco ISE Policy Matrix

dACL
SGT
VLAN

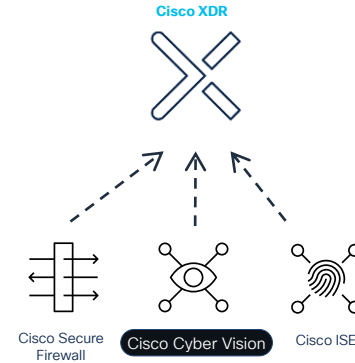
Segmentation of industrial network



Cisco XDR Integration

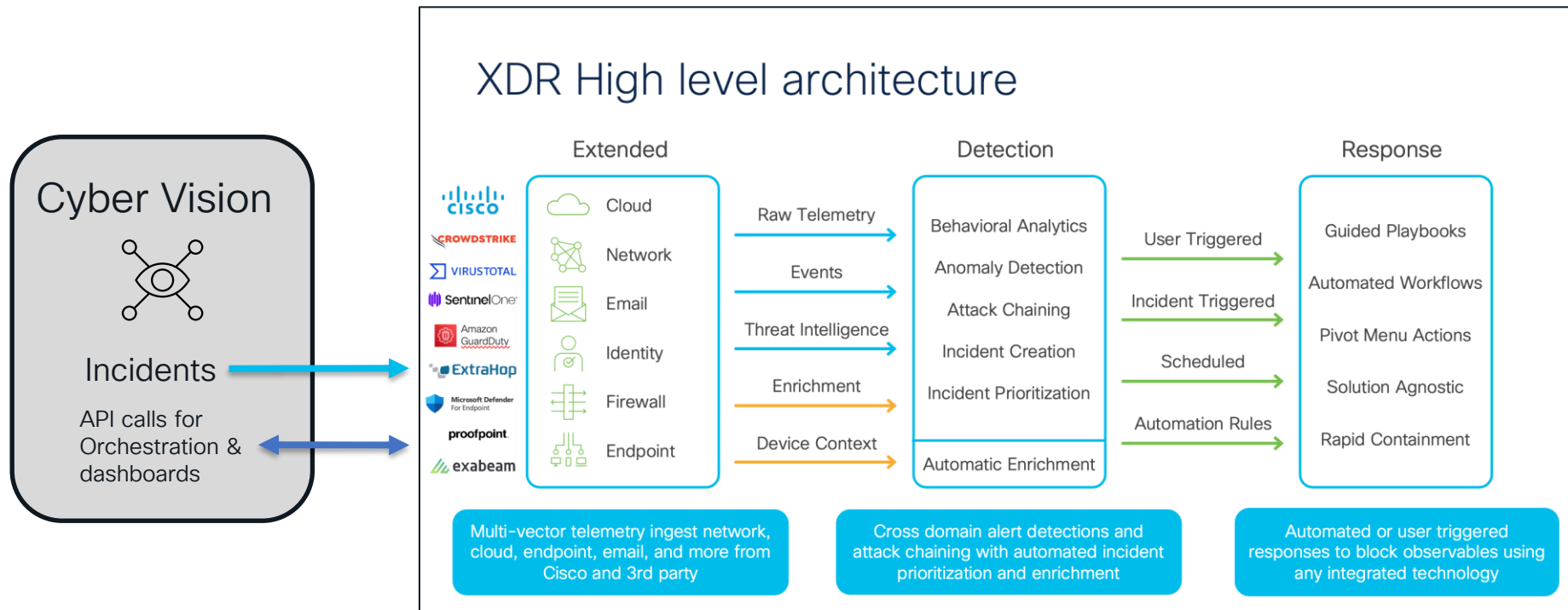
4

Develop Incident Investigation & Response



X(tended) D(etection) & R(espense) & Cyber Vision

Cloud based advanced Security Ops Centre Tool



XDR is a major enhancement to what was previously called 'secureX'

Promote Cyber Vision events to Cisco XDR

View events in Cyber Vision

Launch investigation in XDR

April 2, 2024 11:40:55 AM **critical** Control Systems Events

Stop CPU command has been detected from 192.168.105.241 (@ 192.168.105.241) | IP: 192.168.105.241 | MAC: 34:17:ebd1:c9:97 to 192.168.105.112 (@ 192.168.105.112) | IP: 192.168.105.112 | MAC: 28:63:36:85:b3:32

source	destination	Flow	Source component	Destination component
192.168.105.241	192.168.105.112	Source port: 1613 Destination port: 102	Device: 192.168.105.241 Name: 192.168.105.241 MAC: 34:17:ebd1:c9:97 IP: 192.168.105.241 Tag: Engineering Station	Device: 192.168.105.112 Name: 192.168.105.112 MAC: 28:63:36:85:b3:32 IP: 192.168.105.112 Tag: Controller Vulnerabilities detected: 32

[Report to XDR](#)

Threat Response Investigate Snapshots Incidents Intelligence

Create new incident Investigate This Incident Change Status Link Reference Download

Find ... Sort/Filter ...

Control system event: Stop CPU command has been detected from...

Control system event: Stop CPU command has been detected from 192.168.249.114:1110 to 192.168.249.50:502
New - Created by Cisco Cyber Vision on 2021-05-26T04:30:49.867Z

Summary Observables Timeline Signings Linked References (0)

Seen at 2021-05-26T04:30:27.661Z

Source: Cisco Cyber Vision
Sensor: Network Sensor
IP Address
Device

Confidence: High
Severity: High
Environment: Global
Resolution: N/A

KEY PROPERTIES

DESCRIPTION	Source	Destination
Name	DESKTOP-G8JUF2N	1789-L16EB18 LOGS316ER
Vendor	VMware, Inc.	Rockwell Automation
Mac	00:0c:29:c7:c8:76	14:54:33:91:cb:ee
IP	192.168.249.114	192.168.249.50
Tags	WINDOWS, ENGINEERING PLC, ROCKWELL, AUTOMATION	

TARGETS

IP Address 192.168.249.50

OBSERVABLES RELATED TO SIGNING (7)

IP Address 192.168.249.114

RELATIONS (1)

IP Address 192.168.249.114 Connected to IP Address 192.168.249.50

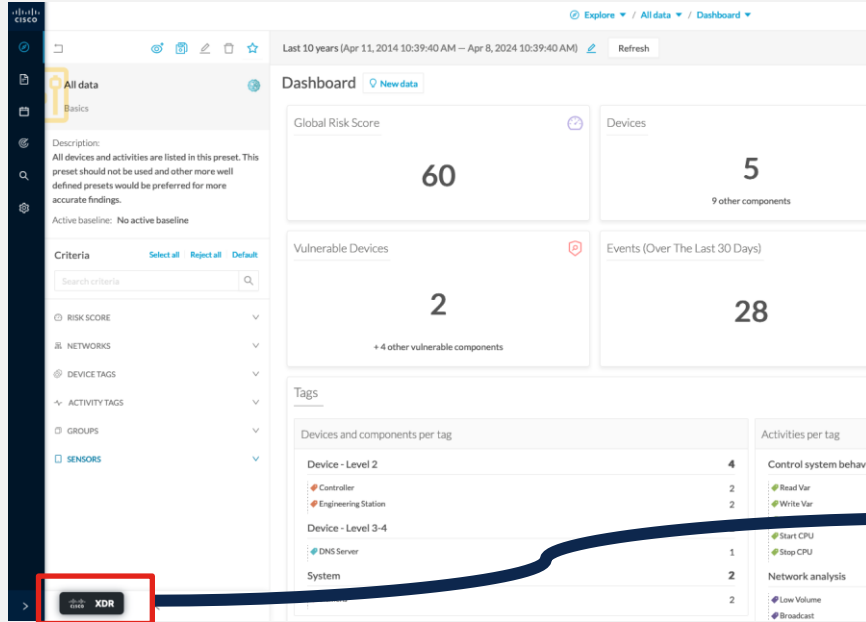
192.168.249.50
IP Address

Add to current investigation
Investigate in Threat Response
Create Judgement
Search for this IP
Umbrella
IP view for 192.168.249.50

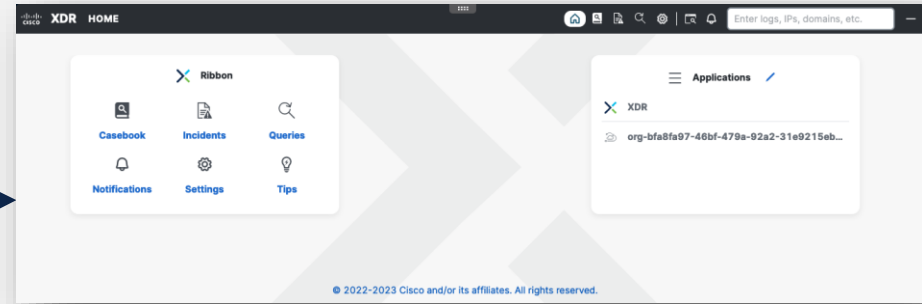
Events generated in Cyber Vision for process anomalies, signatures and control system can be promoted

Investigate the threat with enrichment from Cisco and 3rd party security products

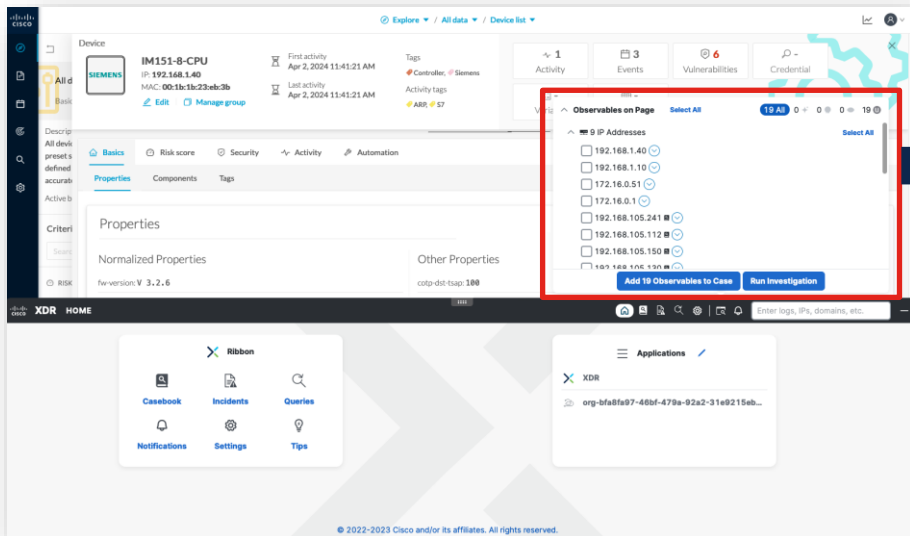
Cisco XDR Ribbon on Cyber Vision



Create and manage **incidents**,
Launch **investigations**,
Orchestrate **playbooks**...
...directly from Cyber Vision

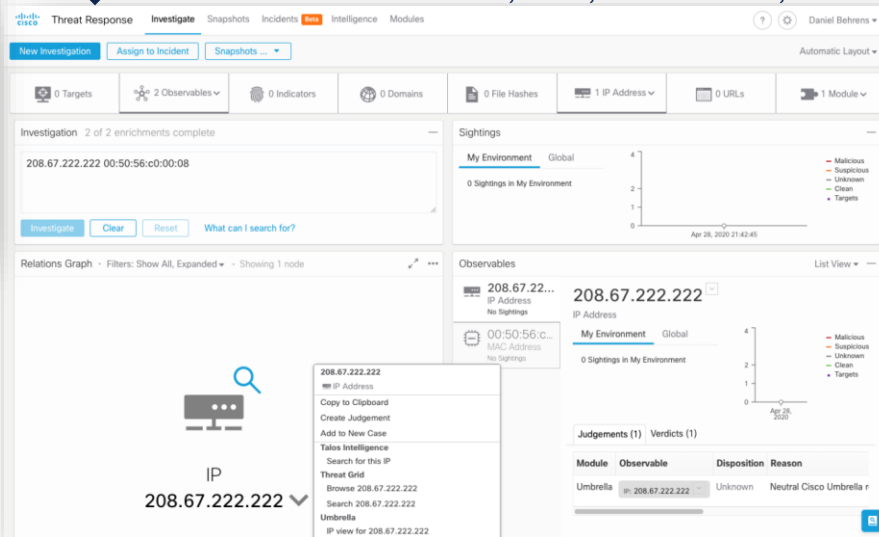


Investigate OT events with Cisco XDR



Pivot from Cyber Vision to XDR
to investigate observables...

...pull details from Umbrella, FTD,
Talos, AMP, Stealthwatch, etc.



Wrapping Up



*"You cannot protect
what you cannot
see"*

How Cyber Vision helps

Areas of concern



Risk analysis



Incident prevention



Incident detection & response



Vulnerability management



Cyber hygiene

Cyber Vision Capabilities



Risk scores, Security posture reports



IEC-62443 zone segmentation with Cisco ISE



Snort IDS with Talos Threat Intel, Cisco XDR



OT asset vulnerability, Cisco VM Risk scores



Asset inventory, Activities, Security insights

Assess OT cyber risks with Cyber Vision to implement best practices

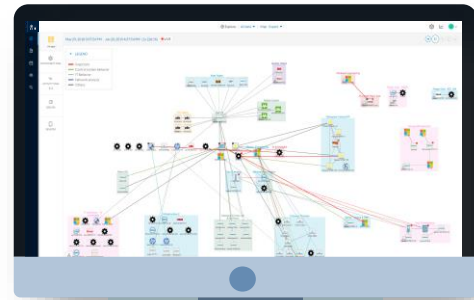
Enlist your OT network for security



Cisco Industrial switches and gateways **see everything** that attaches to them so you can gain **visibility at scale**

cisco *Live!*

Cyber Vision Center



1 0 0 1
0 0 1
Application Flow
Metadata
0 0
1 1 0

Cyber Vision Sensor



Deep Packet Inspection & Active Discovery
built into your network infrastructure

SEA Key takeaways

- Contemporary network access embraces ZTNA, not VPN
- SEA is built with ZTNA in mind, for OT networks
- SEA is embedded in your network – no additional equipment
- SEA is Cloud managed by Cisco – nothing to install

Industrial IoT Summit@Cisco Live APJC Wed 14th

Time	Eureka 1	Eureka 2	Eureka 3
11:45 – 12:20	Lunch & Networking inside the Room	Lunch & Networking inside the Room	Lunch & Networking inside the Room
12:20 – 12:45	Utilities Cisco Executive Welcome Vikas Butaney, Senior Vice President, Cisco Ross Delacour, IIoT APJC Regional Director	Mining Cisco Executive Welcome Dave West, Senior Vice President Samuel Pasquier, Vice President, IIoT Product Management	Transportation Cisco Executive Welcome Stefan Leitl, Vice President, Global IIoT Sales Bryan Tantzen, Sr. Director, IIoT Solutions
12:45 – 4:30	<u>Utilities Summit Breakout</u>	<u>Mining Summit Breakout</u>	<u>Transportation Summit Breakout</u>
	Industry breakout sessions bring focused dialogue to the key topics you care about: Breakout sessions include curated presentations by industry leaders including an industry panel discussion with Q&A. These meaningful conversations related to current and emerging trends will empower you to navigate the ever-changing IT/OT landscape with actionable takeaways you can bring back to your environment.		
4:30 – 5:15	Cocktail Reception Interact with your Industry peers and Cisco Industrial IoT Executives		

Contact Alex Lynn (alelynn@cisco.com) or
Andrew Johnstone (ajohnst3@cisco.com) for admission

Keynote Deep Dives

Wednesday
10:30am – 11:30am



Experiences Amplified:
How AI Can Fuel Better Employee and Customer Experiences

Level 1
Room 106



Smart, Secure, Seamless:
Transforming Experiences with Next-Generation Networking

Level 2
Room 204



Harness a Bold New Era:
Transform Data Centre and Service Provider Connectivity

Level 2
Room 203



Securing User to Application and Everything in Between

Level 2
Melbourne Room 2



Unlocking Digital Resilience through Unified Observability

The HUB
Centre Stage

Complete Your Session Evaluations



Complete a minimum of 4 session surveys and the Overall Event Survey to claim a **Cisco Live T-Shirt**.



Complete your surveys in the **Cisco Live mobile app**.



Continue your education



- Visit the Cisco Stand for related demos
- Book your one-on-one Meet the Expert meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand



Thank you

CISCO *Live!*

#CiscoLiveAPJC

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC