The bridge to possible

Bezpieczeństwo OT

Marcin Szreter
szreter@cisco.com

Industrial IoT networking portfolio Overview

Our solutions meet the needs of IT and operations

Industrial Ethernet switches

DIN-Rail, IP67, and Stackable Rackmount

IE3400

IE3300

IE3200

IE3100

IE3400H

IE9300

Industrial Cybersecurity

Cyber Vision, Secure Equipment Access

Industrial Wi-Fi and Ultra-reliable Wireless Backhaul

For outdoor conditions

IW9165E

IW9165D

IW9167i

IW9167E

IW9167E-HZ

Industrial Routers

Modular 4G/5G – for connecting remote and mobile assets

IR1100

IR1800

IR8300

IR8100

Data Control and Exchange

Edge Intelligence, IOx

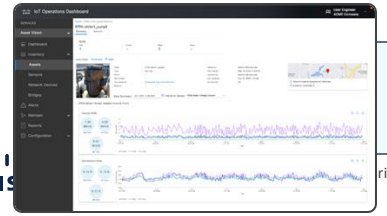
Embedded Networking

Embedded routers and switches for industrial Makers

ESR6300

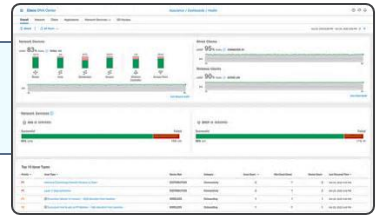
ESS3300

ESS9300



Management and Automation

Cisco Catalyst Center, Cisco Catalyst WAN Manager, Field Network Director



Securing Critical Infrastructure is a Key Priority

NERC CIP

Substations & Renewable Energy

CIP-005-7 — Cyber Security – Electronic Security Perimeter(s)

A. Introduction

1. **Title:** Cyber Security — Electronic Security Perimeter(s)
2. **Number:** CIP-005-7
3. **Purpose:** To manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.
4. **Applicability:**

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1. Balancing Authority

4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one

TSA Security Directives

Rail, Pipelines, Airports

U.S. Department of Homeland Security
Transportation Security Administration
6595 Springfield Center Drive
Springfield, Virginia 20598

NUMBER	Security Directive 1580/82-2022-01
SUBJECT	Rail Cybersecurity Mitigation Actions and Testing
EFFECTIVE DATE	October 24, 2022
EXPIRATION DATE	October 24, 2023
SUPERSEDES	Not Applicable
APPLICABILITY	Each freight railroad carrier identified in 49 CFR 1580.101 and other TSA-designated freight and passenger railroads
AUTHORITY	49 U.S.C. 114(d), (f), (*l*) and (m)
LOCATION	All locations within the United States

I. PURPOSE AND GENERAL INFORMATION

The Transportation Security Administration (TSA) is issuing this Security Directive due to the ongoing cybersecurity threat to surface transportation systems and associated infrastructure to mitigate the significant harm to the national and economic security of the United States that could result from the "degradation, destruction, or malfunction of systems that control this infrastructure."[1]

This Security Directive requires actions necessary to protect the national security, economy, and public health and safety of the United States and its citizens from the impact of malicious cyber-intrusions affecting the nation's railroads.[2] Even minor disruptions in critical rail systems may result in temporary product shortages that can cause significant harm to national security. Prolonged disruptions in the flow of commodities could lead to widespread supply

NIS2

Energy, Transport, Water, Manufacturing, …..

BRIEFING
EU Legislation in Progress

European Parliament

The NIS2 Directive

A high common level of cybersecurity in the EU

OVERVIEW

The Network and Information Security (NIS) Directive is the first piece of EU-wide legislation on cybersecurity, and its specific aim was to achieve a high common level of cybersecurity across the Member States. While it increased the Member States' cybersecurity capabilities, its implementation proved difficult, resulting in fragmentation at different levels across the internal market.

To respond to the growing threats posed with digitalisation and the surge in cyber-attacks, the Commission has submitted a proposal to replace the NIS Directive and thereby strengthen the security requirements, address the security of supply chains, streamline reporting obligations, and introduce more stringent supervisory measures and stricter enforcement requirements, including harmonised sanctions across the EU. The proposed expansion of the scope covered by NIS2, by effectively obliging more entities and sectors to take measures, would assist in increasing the level of cybersecurity in Europe in the longer term.

Within the European Parliament, the file was assigned to the Committee on Industry, Research and Energy. The committee adopted its report on 28 October 2021, while the Council agreed its position on 3 December 2021. The co-legislators reached a provisional agreement on the text on 13 May 2022. The political agreement was formally adopted by the Parliament and then the Council in November 2022. It entered into force on 16 January 2023, and Member States now have 21 months, until 17 October 2024, to transpose its measures into national law.

Proposal for a directive on measures for a high common level of cybersecurity across the Union

Committee responsible:	Industry, Research and Energy (ITRE)	COM(2020) 823 16.12.2021
Rapporteur:	Bart Groothuis (Renew, the Netherlands)	2020/0359(COD)
Shadow rapporteurs:	Eva Maydell (EPP, Bulgaria) Eva Kaili (S&D, Greece) Rasmus Andresen (Greens/EFA, Germany) Thierry Mariani (ID, France)	Ordinary legislative procedure (COD)

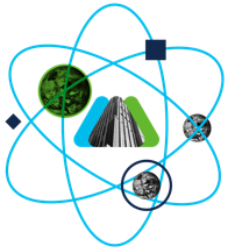
There are increasing demands on security teams

Business evolution

Unlimited devices

Transition to the cloud

Distributed workforces

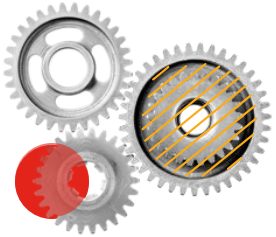


Digital transformation

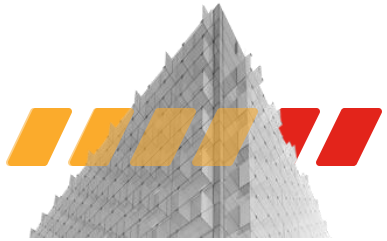
Security pressures

Too little visibility

Too few experts



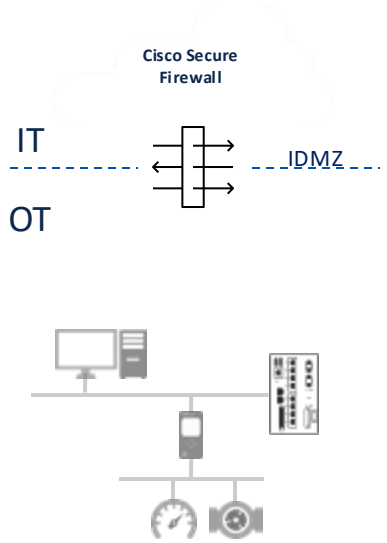
Too little integration



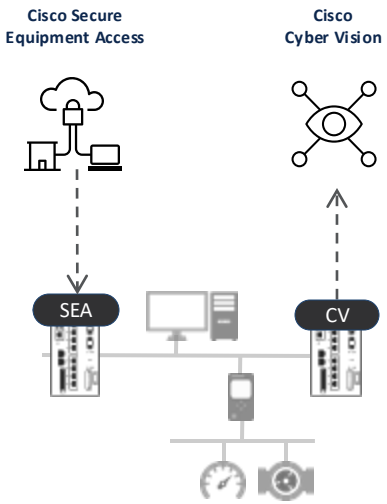
Too much exposure

Cisco Industrial Security Solution

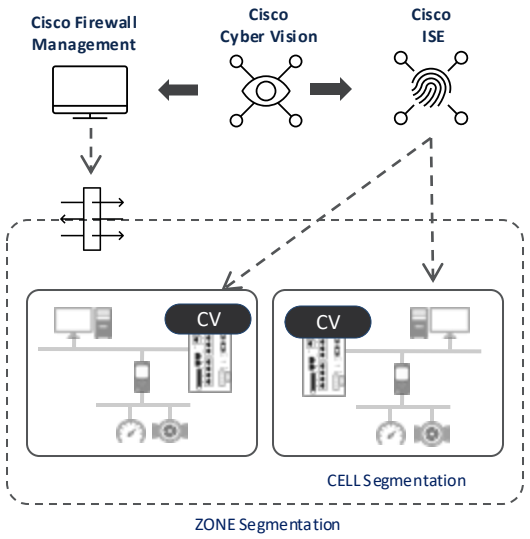
1 Build a Security Foundation



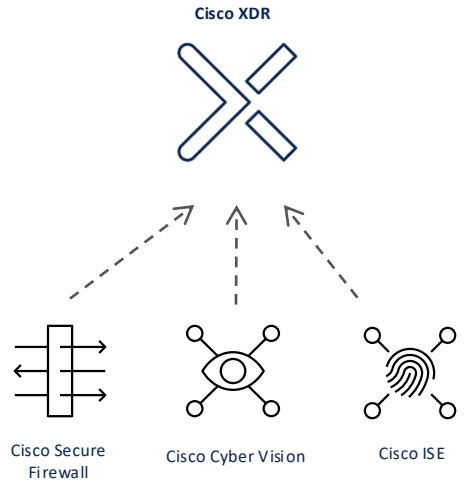
2 Security Posture & ZTNA of OT Assets



3 Segment Network into Smaller Trust Zones



4 Develop Incident Investigation & Response



Talos Threat Intelligence + Talos Incident Response

Cisco Validated Designs

Cisco Validated Design

Reference architectures validated for the specific needs of your industry

Faster deployments

Less risk

Predictability

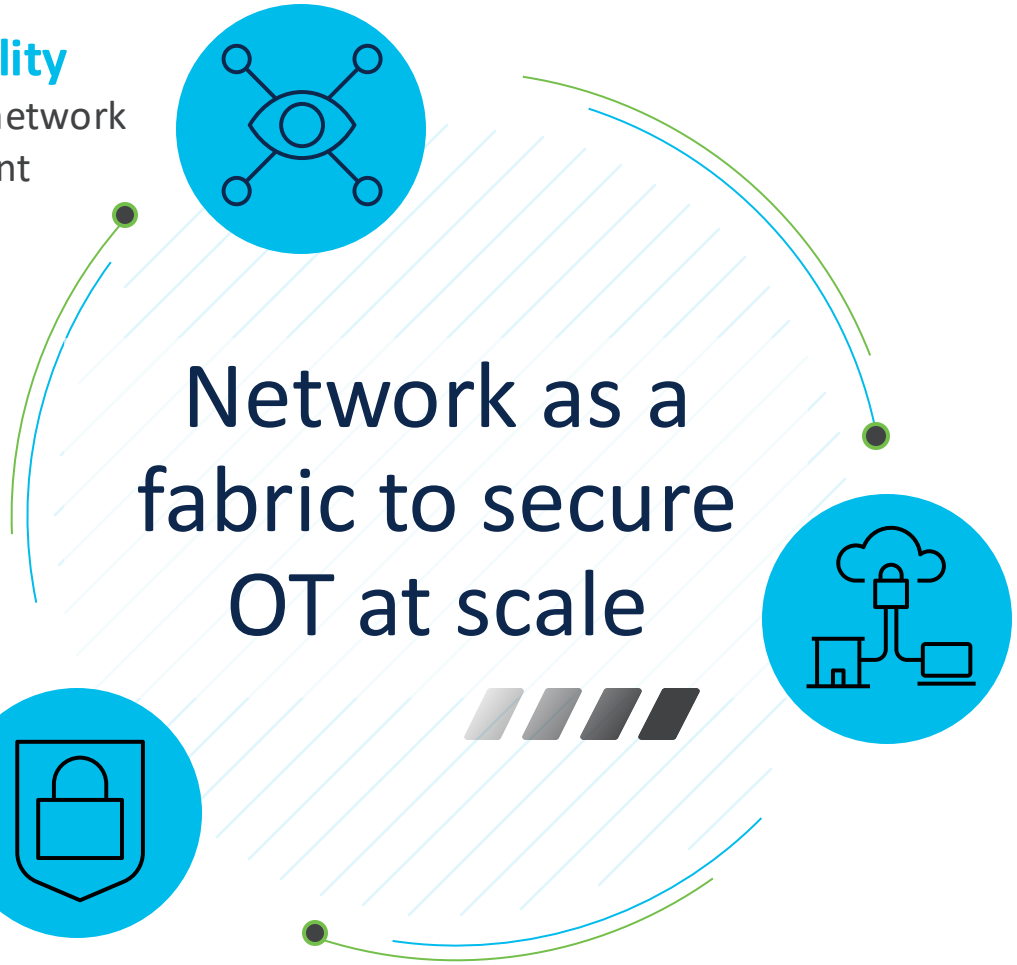
End to end designs

Design, deploy, and extend networking and cybersecurity technologies successfully

Helping industries with generic and specific designs, as well as addressing regulatory requirements.

The Cisco Industrial Security Differentiation

OT Visibility
embedded in network equipment



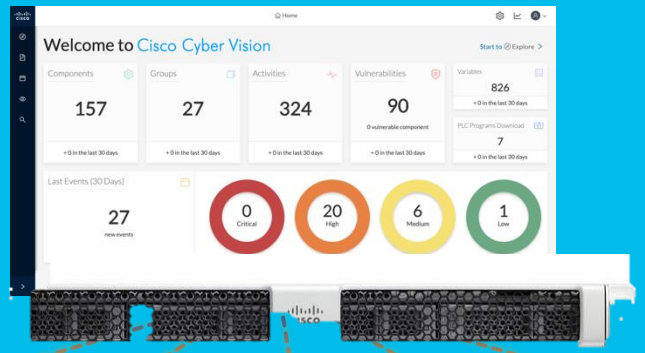
ZTNA Remote Access
gateway embedded in network equipment

Segmentation & Remediation Policies
enforced by network equipment

Unique **edge monitoring** architecture

Industrial cybersecurity that can be deployed at scale

Cisco Cyber Vision Center:
Centralized analytics & data visualization



Cisco integrations

SecureX, FMC, ISE,
Stealthwatch, DNA-C

Partner integrations

SIEM, CMDB,
ICS vendor software

Application flow

Sensor — Industrial Switching

Sensor — IoT Gateways / Compute

Sensor — Industrial Routing

Sensor — Industrial Wi-Fi

Sensor — Sensor Networking (RF Mesh)

Cyber Vision Sensors: Deep Packet Inspection & Active Discovery built into network elements

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 visualization. This only adds 3 to 5% extra traffic to the network

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

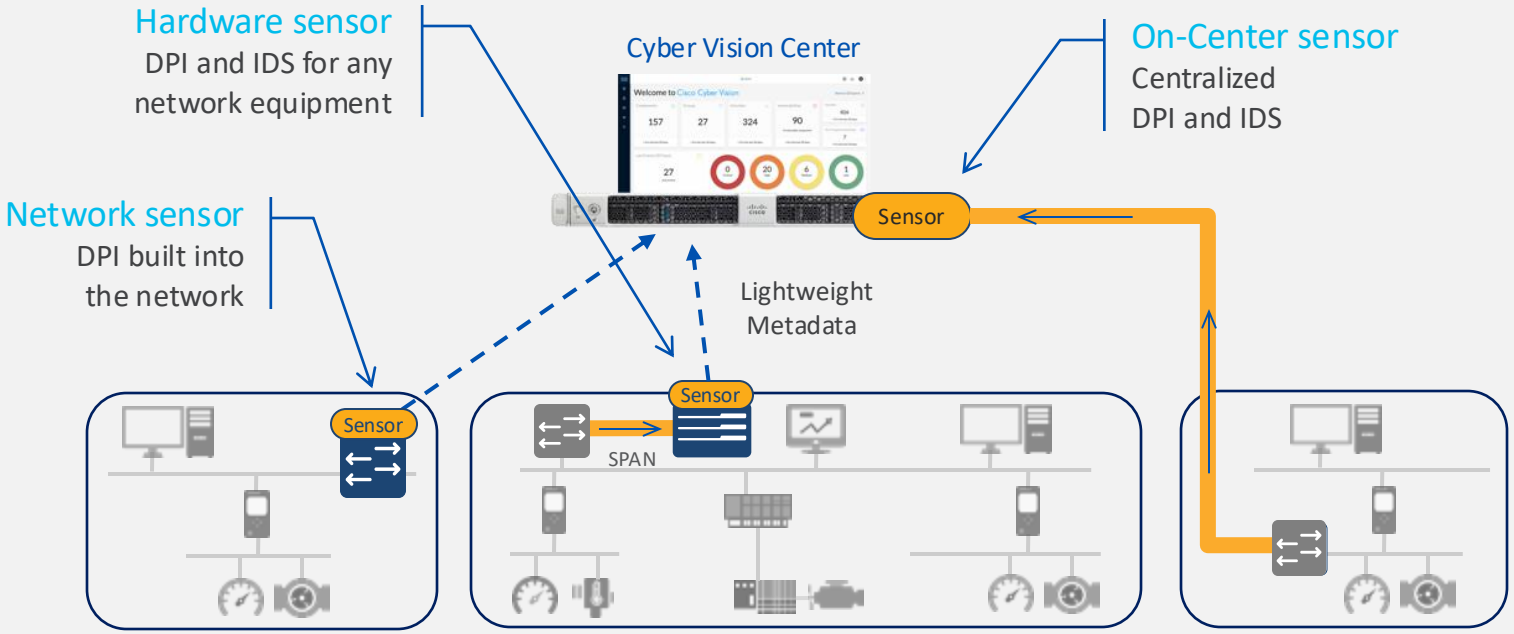
Network-Sensors
Deep Packet Inspection built into network-elements eliminating the need for SPAN

IC3000 Industrial Compute

Hardware-Sensor
DPI via SPAN to support brownfield

Container Sensor
DPI via SPAN to support brownfield

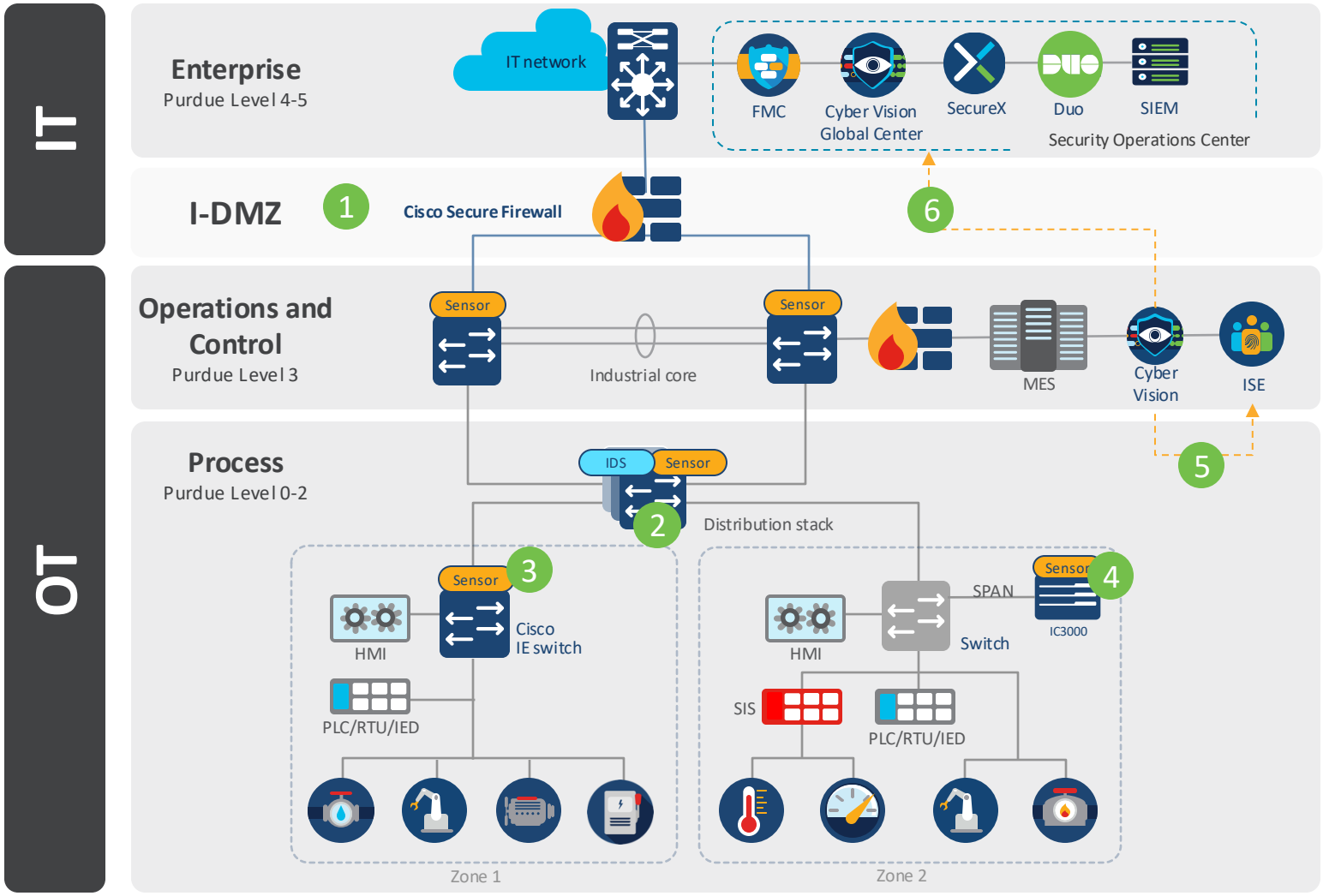
Cyber Vision offers **flexible deployment** options



- **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

Cyber Vision can mix architectures to best fit your constraints

Cisco Cyber Vision in Manufacturing

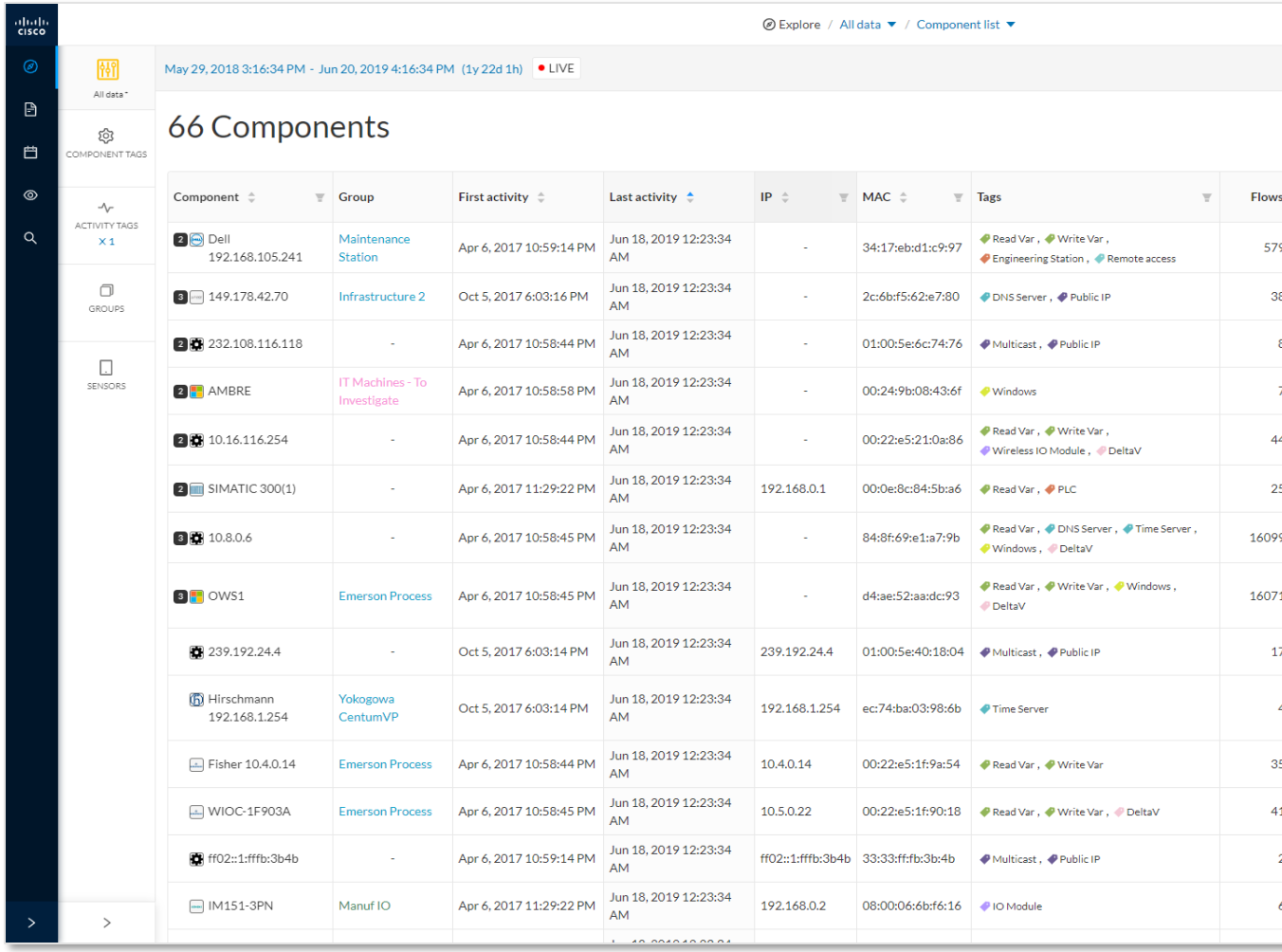


1. Isolate IT and OT by installing an industrial DMZ with Cisco Secure FW
2. Create macro-segmentation zones in the Catalyst 9300 switches and deploy Cyber Vision sensors with Snort IDS.
3. Cyber Vision sensors deployed within segments across IE3400 switches
4. Cyber Vision hardware-sensors deployed via one-hop SPAN to gain visibility on non-Cisco switches
5. Build zones and conduits in Cyber Vision and share with ISE for micro segmentation
6. Cyber Vision shares details on OT devices and events with SOC to build informed security policies and investigate threats across domains

Comprehensive asset inventory

- Automatically maintain a detailed list of all OT and IT equipment
- Immediate access to software and hardware characteristics
- Track rack-slot components
- Tags make it easy to understand asset functions and properties

Track the industrial assets to protect throughout their life cycles



Component	Group	First activity	Last activity	IP	MAC	Tags	Flows
Dell 192.168.105.241	Maintenance Station	Apr 6, 2017 10:59:14 PM	Jun 18, 2019 12:23:34 AM	-	34:17:eb:d1:c9:97	Read Var, Write Var, Engineering Station, Remote access	579
149.178.42.70	Infrastructure 2	Oct 5, 2017 6:03:16 PM	Jun 18, 2019 12:23:34 AM	-	2c:6b:f5:62:e7:80	DNS Server, Public IP	38
232.108.116.118	-	Apr 6, 2017 10:58:44 PM	Jun 18, 2019 12:23:34 AM	-	01:00:5e:6c:74:76	Multicast, Public IP	8
AMBRE	IT Machines - To Investigate	Apr 6, 2017 10:58:58 PM	Jun 18, 2019 12:23:34 AM	-	00:24:9b:08:43:6f	Windows	7
10.16.116.254	-	Apr 6, 2017 10:58:44 PM	Jun 18, 2019 12:23:34 AM	-	00:22:e5:21:0a:86	Read Var, Write Var, Wireless IO Module, DeltaV	44
SIMATIC 300(1)	-	Apr 6, 2017 11:29:22 PM	Jun 18, 2019 12:23:34 AM	192.168.0.1	00:0e:8c:84:5b:a6	Read Var, PLC	25
10.8.0.6	-	Apr 6, 2017 10:58:45 PM	Jun 18, 2019 12:23:34 AM	-	84:8f:69:e1:a7:9b	Read Var, DNS Server, Time Server, Windows, DeltaV	16099
OWS1	Emerson Process	Apr 6, 2017 10:58:45 PM	Jun 18, 2019 12:23:34 AM	-	d4:ae:52:aa:dc:93	Read Var, Write Var, Windows, DeltaV	16071
239.192.24.4	-	Oct 5, 2017 6:03:14 PM	Jun 18, 2019 12:23:34 AM	239.192.24.4	01:00:5e:40:18:04	Multicast, Public IP	17
Hirschmann 192.168.1.254	Yokogowa CentumVP	Oct 5, 2017 6:03:14 PM	Jun 18, 2019 12:23:34 AM	192.168.1.254	ec:74:ba:03:98:6b	Time Server	4
Fisher 10.4.0.14	Emerson Process	Apr 6, 2017 10:58:44 PM	Jun 18, 2019 12:23:34 AM	10.4.0.14	00:22:e5:1f:9a:54	Read Var, Write Var	35
WIOC-1F903A	Emerson Process	Apr 6, 2017 10:58:45 PM	Jun 18, 2019 12:23:34 AM	10.5.0.22	00:22:e5:1f:90:18	Read Var, Write Var, DeltaV	43
ff02::1:fffb:3b4b	-	Apr 6, 2017 10:59:14 PM	Jun 18, 2019 12:23:34 AM	ff02::1:fffb:3b4b	33:33:ff:fb:3b:4b	Multicast, Public IP	2
IM151-3PN	Manuf IO	Apr 6, 2017 11:29:22 PM	Jun 18, 2019 12:23:34 AM	192.168.0.2	08:00:06:6b:f6:16	IO Module	6

Detailed information on assets

Insights on risks, vulnerabilities, communications, variables, etc.

Tags to easily understand characteristics, activities, and threats

Asset characteristics, version and network configuration

Control logic properties

Rack slot component details

Explore / All data / Device list

Device

PLC
Munich None
IP: 192.168.249.50
MAC: f4:54:33:91:cb:ee

First activity
Sep 10, 2020 3:36:37 PM

Last activity
Jan 19, 2022 2:00:01 AM

Tags
Controller, Rockwell Automation

Activity tags
Start CPU, Stop CPU, Diagnostics, Read Var, Write Var, Low Volume, CIP-IO, EtherNetIP, Umas (hide)

4 Activities | 42 Events | 10 Vulnerabilities | - Credential | - Variable

Basics | Risk score | Security | Activity | Automation

Properties | Components | Tags

Properties

Normalized Properties

fw-version: 31.11, 31.011

ip: 192.168.249.50

mac: f4:54:33:91:cb:ee

model-ref: 0x99, 0x474, 1769-L16ER/B LOGIX5316ER

name: 1769-L16ER/B LOGIX5316ER, SecDemo_LinePLC, 24VDC 16PT INPUT & 16PT OUTPUT (Port1-Link01)

public-ip: no

serial-number: 60771949, 00000000

vendor-name: Rockwell Automation

Other Properties

enip-cpuname: SecDemo_LinePLC

enip-devicetype: ProgrammableLogicController, GeneralPurposeDiscreteIO

enip-location: Endpoint, Port1-Link00, Port1-Link01

enip-name: 1769-L16ER/B LOGIX5316ER, 24VDC 16PT INPUT & 16PT OUTPUT

enip-productcode: 0x99, 0x474

enip-serial: 00000000, 60771949

enip-status: Owned,AtLeastOneIOConnectionInRunMode, NoIOConnectionsEstablished, AtLeastOneIOConnectionInRunMode,MinorRecoverableFault,ReservedBits12-15:0x3

enip-value: RA-ProgramName

enip-vendor: Rockwell Automation/Allen-Bradley

enip-version: 31.11, 31.011

name-enip: 1769-L16ER/B LOGIX5316ER, SecDemo_LinePLC, 24VDC 16PT INPUT & 16PT OUTPUT (Port1-Link01)

name-vendorip: Rockwell 192.168.249.50

vendor: Rockwell Automation

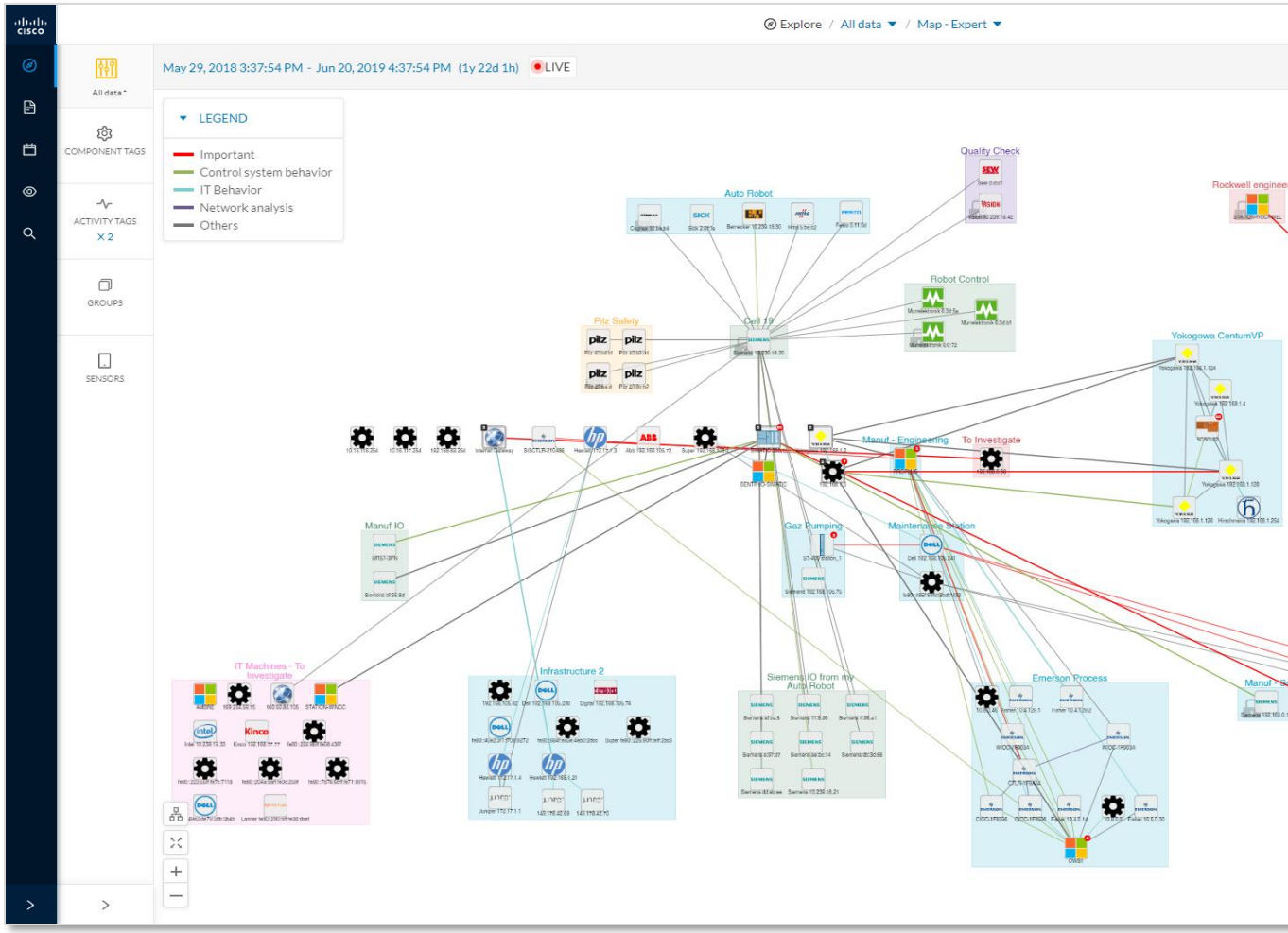
4 Components

Component	First activity	Last activity	IP	MAC	Tags	Vulnerabilities	Flows	VLAN ID	Sensor
1769-L16ER/B LOGIX5316ER	Sep 10, 2020 3:36:38 PM	Jan 19, 2022 2:00:01 AM	192.168.249.50	f4:54:33:91:cb:ee	Controller	10	~10	-	
SecDemo_LinePLC	Sep 10, 2020 3:36:41 PM	Jan 19, 2022 2:00:01 AM	192.168.249.50	f4:54:33:91:cb:ee	Controller	10	~10	-	
24VDC 16PT INPUT & 16PT OUTPUT (Port1-Link01)	Sep 10, 2020 3:36:41 PM	Jan 19, 2022 2:00:01 AM	192.168.249.50	f4:54:33:91:cb:ee	No tags	0	~10	-	
1769-L16ER/B LOGIX5316ER	Sep 10, 2020 3:36:37 PM	Jan 19, 2022 2:00:01 AM	192.168.249.50	f4:54:33:91:cb:ee	Controller, Rockwell Automation	10	~20	-	

Detailed communication maps

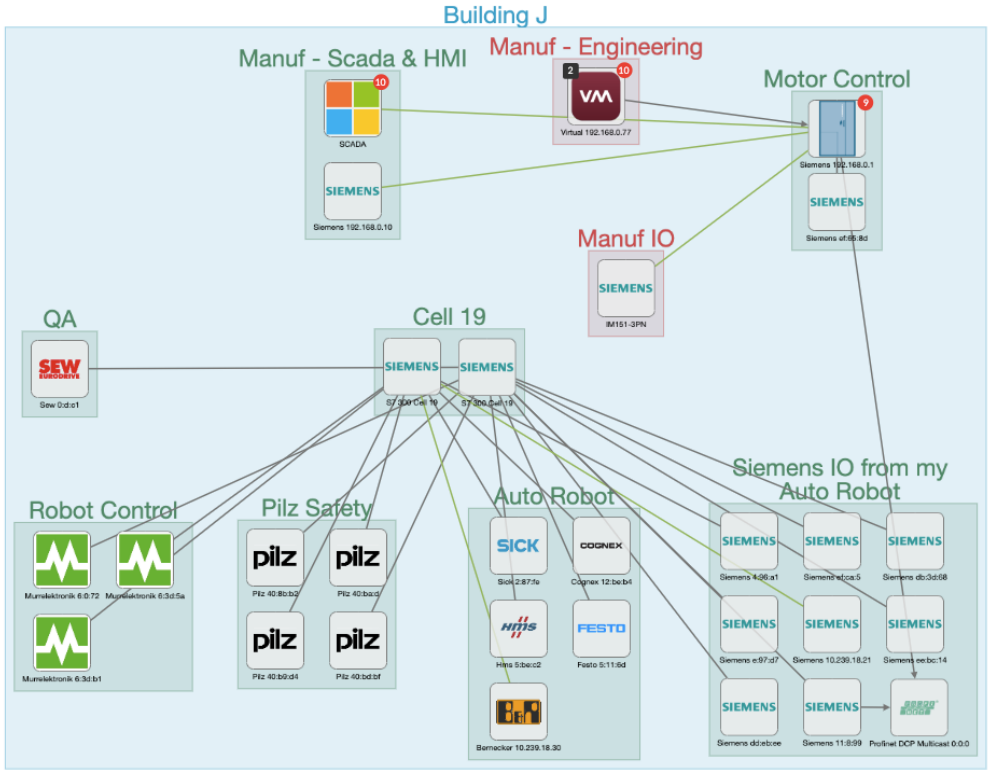
- Identify all relations between assets including application flows
- Spot unwanted communications & noisy assets
- Tags make it easily to understand the content of each communication flow
- View live information or go back in time

Drive network segmentation and fine-tune configurations



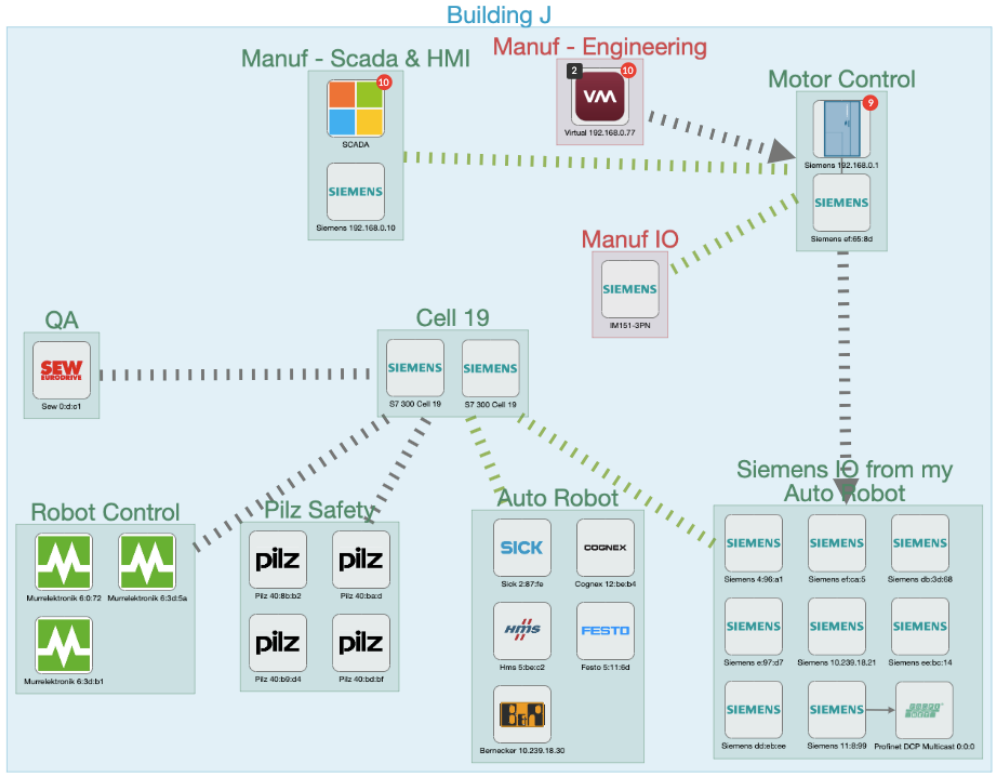
Aggregated activities match ISA/IEC 62443 conduits

Unaggregated



View all asset relationships

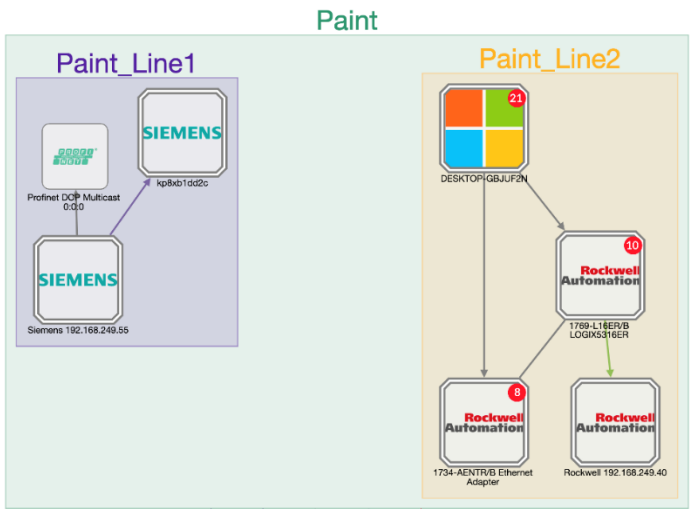
Aggregated



Easily browse through conduits

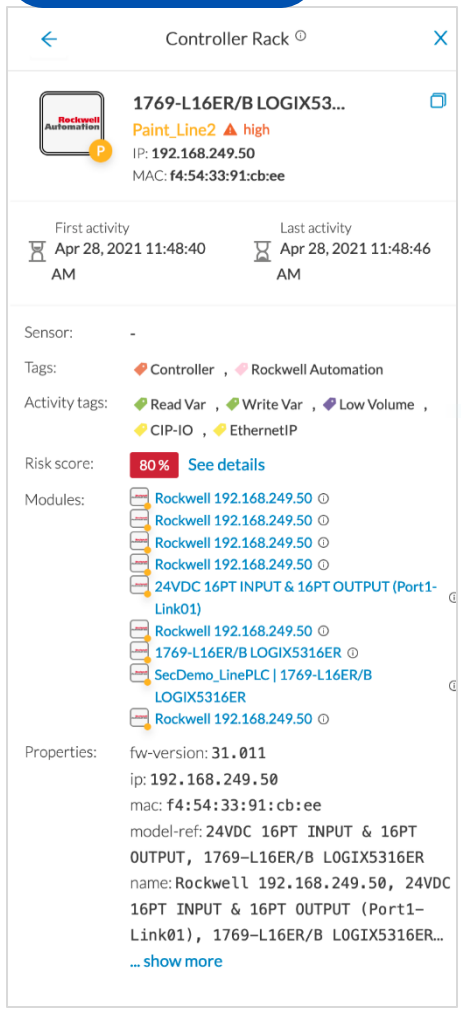
Aggregated components match the physical inventory

Map view

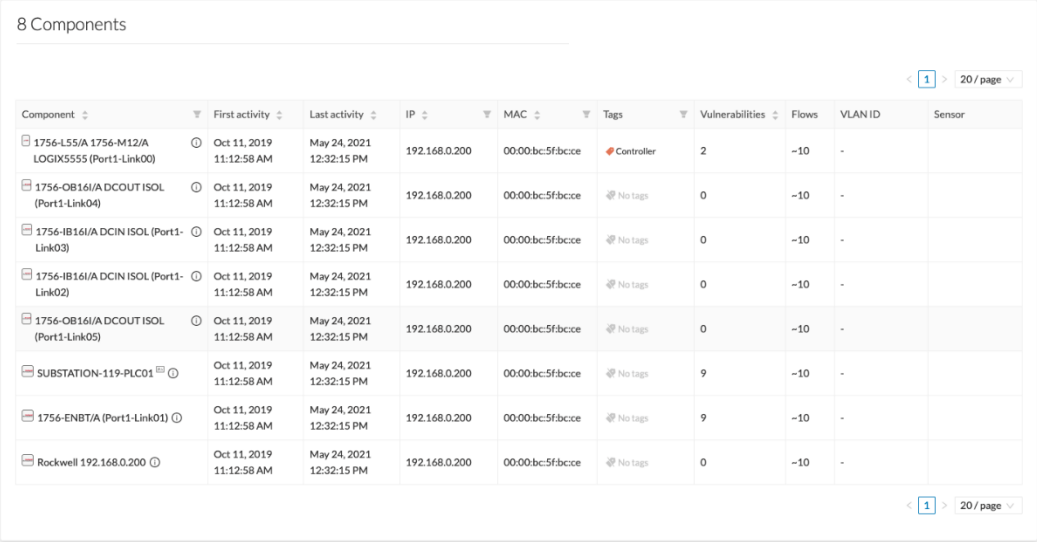


Double-border icons indicate a device with multiple components

ID Cards



Technical Sheets

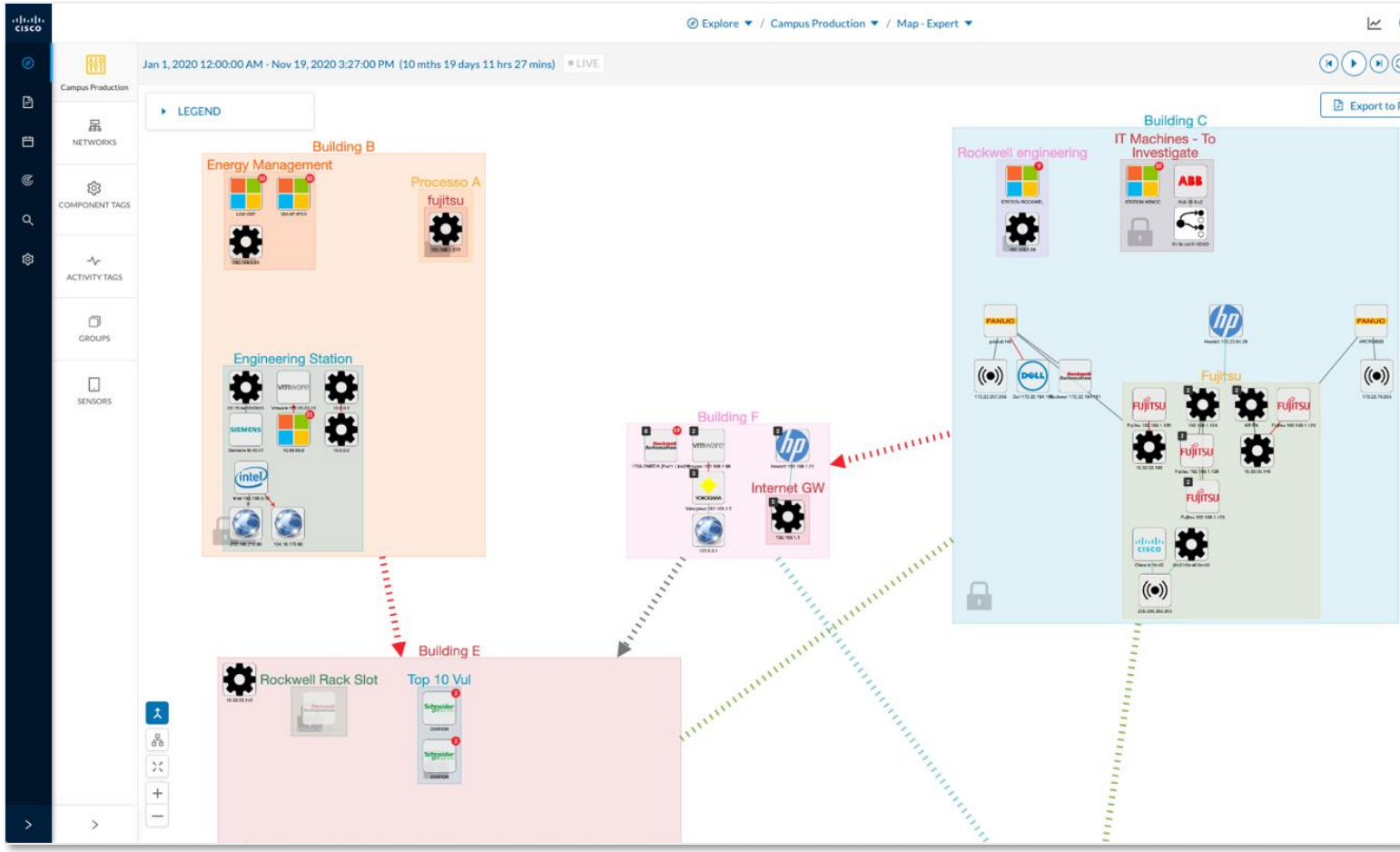


Component	First activity	Last activity	IP	MAC	Tags	Vulnerabilities	Flows	VLAN ID	Sensor
1756-L55/A 1756-M12/A LOGIX5555 (Port1-Link00)	Oct 11, 2019 11:12:58 AM	May 24, 2021 12:32:15 PM	192.168.0.200	00:00:bc:5f:bc:ce	Controller	2	~10	-	
1756-OB16I/A DCOUT ISOL (Port1-Link04)	Oct 11, 2019 11:12:58 AM	May 24, 2021 12:32:15 PM	192.168.0.200	00:00:bc:5f:bc:ce	No tags	0	~10	-	
1756-IB16I/A DCIN ISOL (Port1-Link03)	Oct 11, 2019 11:12:58 AM	May 24, 2021 12:32:15 PM	192.168.0.200	00:00:bc:5f:bc:ce	No tags	0	~10	-	
1756-IB16I/A DCIN ISOL (Port1-Link02)	Oct 11, 2019 11:12:58 AM	May 24, 2021 12:32:15 PM	192.168.0.200	00:00:bc:5f:bc:ce	No tags	0	~10	-	
1756-OB16I/A DCOUT ISOL (Port1-Link05)	Oct 11, 2019 11:12:58 AM	May 24, 2021 12:32:15 PM	192.168.0.200	00:00:bc:5f:bc:ce	No tags	0	~10	-	
SUBSTATION-119-PLC01	Oct 11, 2019 11:12:58 AM	May 24, 2021 12:32:15 PM	192.168.0.200	00:00:bc:5f:bc:ce	No tags	9	~10	-	
1756-ENBT/A (Port1-Link01)	Oct 11, 2019 11:12:58 AM	May 24, 2021 12:32:15 PM	192.168.0.200	00:00:bc:5f:bc:ce	No tags	9	~10	-	
Rockwell 192.168.0.200	Oct 11, 2019 11:12:58 AM	May 24, 2021 12:32:15 PM	192.168.0.200	00:00:bc:5f:bc:ce	No tags	0	~10	-	

Easily list the components of a device. Click on a component to view more details

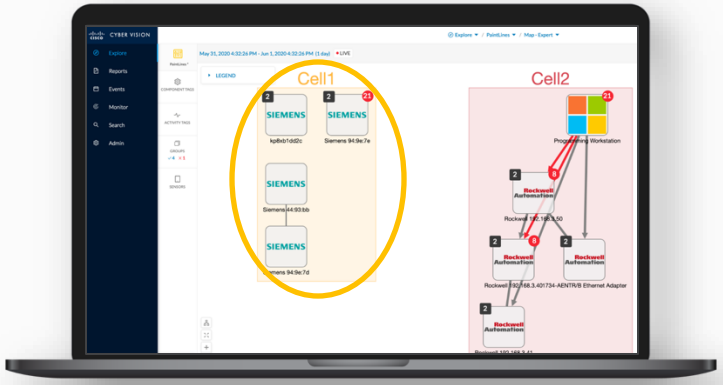
Group assets to define zones and conduits

- Organize your map to match the business and processes
  - Groups and Nested groups
  - Multi-faceted views
  - Quick drilldown
- Enables IT/OT collaboration to define security policies
- Group information shared with IT security tools such as Cisco ISE



Leveraging visibility to drive segmentation

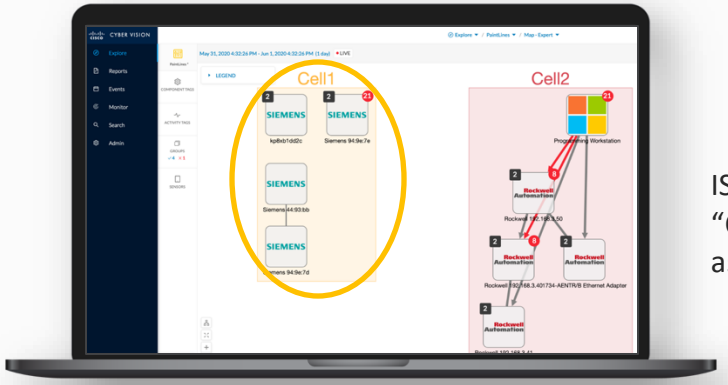
Cisco Cyber Vision



- Group OT assets into zones
- Visualize conduits
- Identify traffic violations
- Share context with other platforms to enforce segmentation

Leveraging visibility to drive segmentation

Cisco Cyber Vision



- Group OT assets into zones
- Visualize conduits
- Identify traffic violations
- Share context with other platforms to enforce segmentation

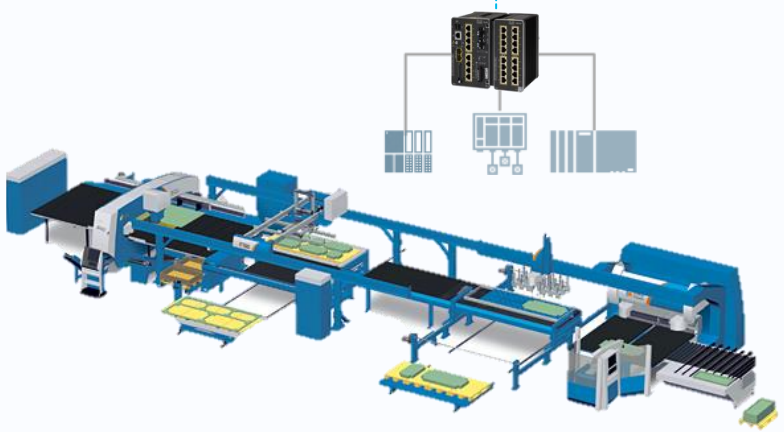
	Cell 1	Cell 2	PLC	MES
Cell 1	✓	✗	✓	✗
Cell 2	✗	✓	✓	✗
PLC	✓	✓	✓	✓
MES	✗	✗	✓	✓

pxGrid

ISE profiles endpoints based on "Cell1" custom attribute and assigns SGT in AuthZ policy

Cisco ISE & Catalyst Center

RADIUS

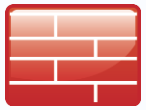


Leveraging visibility to drive segmentation

Cisco Firewall Management Center

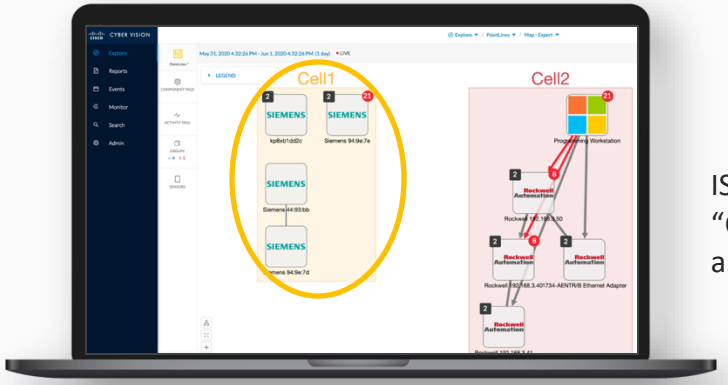
CSDAC

Creates dynamic objects in FMC



Cisco Secure Firewall

Cisco Cyber Vision



- Group OT assets into zones
- Visualize conduits
- Identify traffic violations
- Share context with other platforms to enforce segmentation

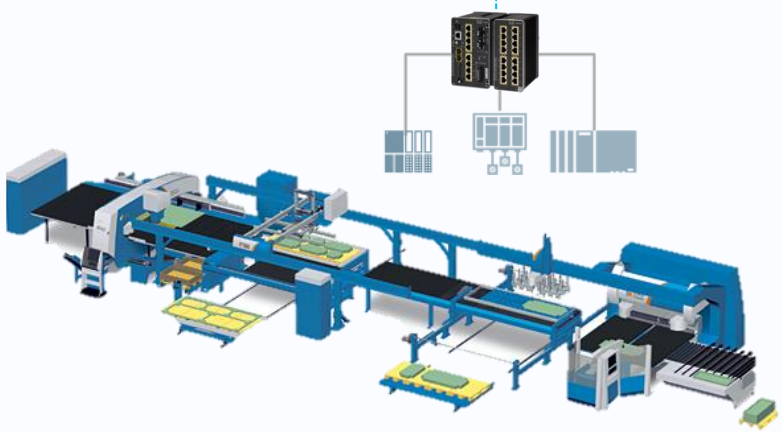
pxGrid

ISE profiles endpoints based on "Cell1" custom attribute and assigns SGT in AuthZ policy

	Cell 1	Cell 2	PLC	MES
Cell 1	✓	✗	✓	✗
Cell 2	✗	✓	✓	✗
PLC	✓	✓	✓	✓
MES	✗	✗	✓	✓

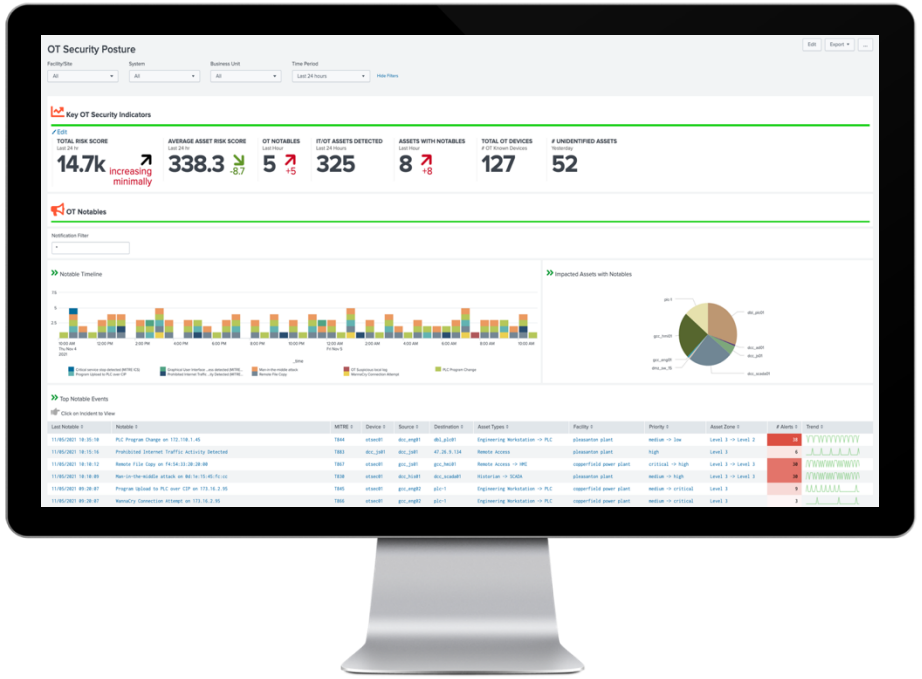
Cisco ISE & Catalyst Center

RADIUS



Splunk for OT Security

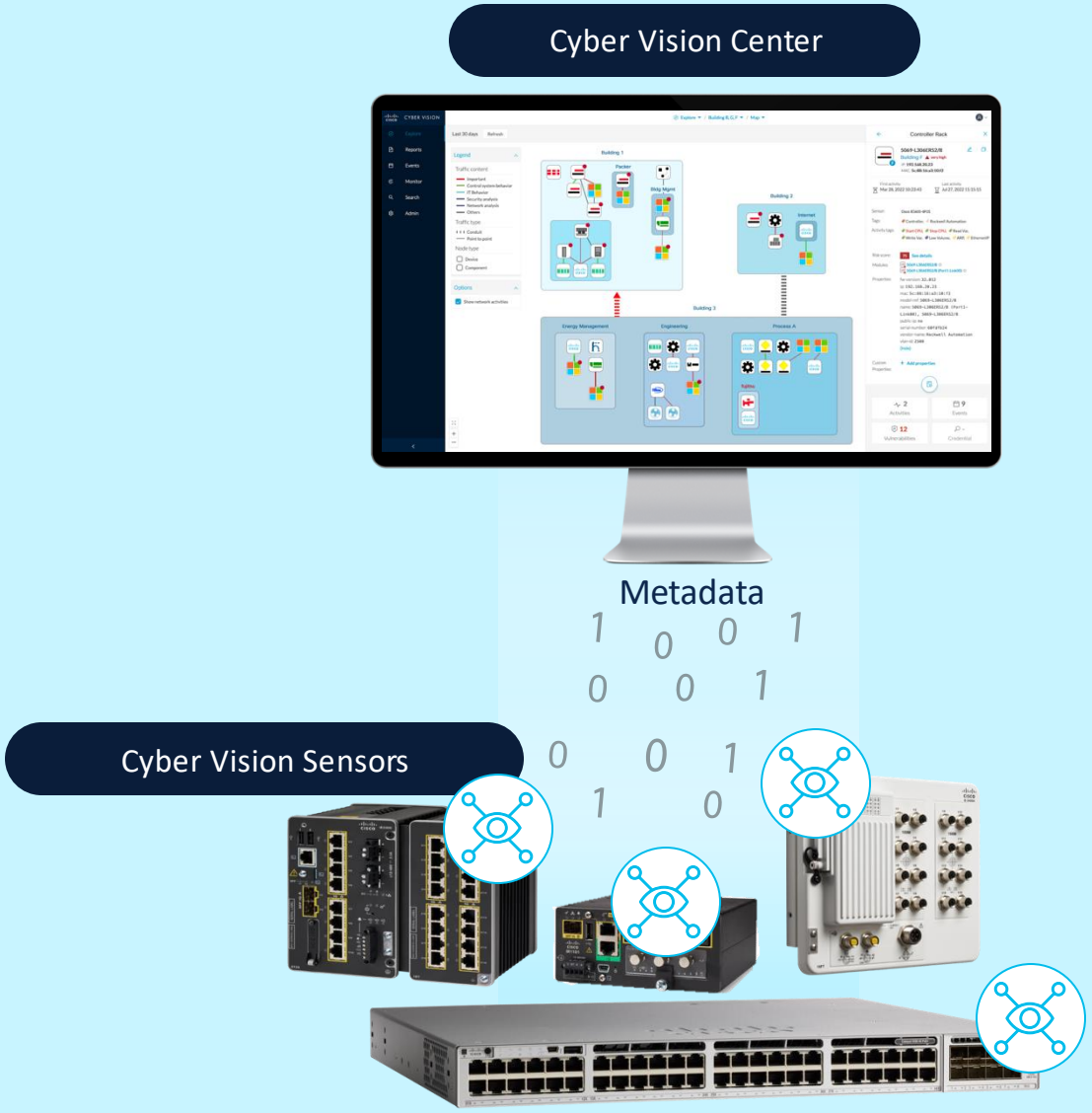
Break silos between OT & IT domains with cross-domain detection and remediation



Improve threat detection, incident investigation, and response **across OT & IT domains** with telemetry from Cisco and 3rd party security products

Cyber Vision 5.0

Introducing the NEW Cyber Vision UX



Deep Packet Inspection and Active Discovery
built into your network infrastructure

Cyber Vision 5.0

Enhanced Feature Set

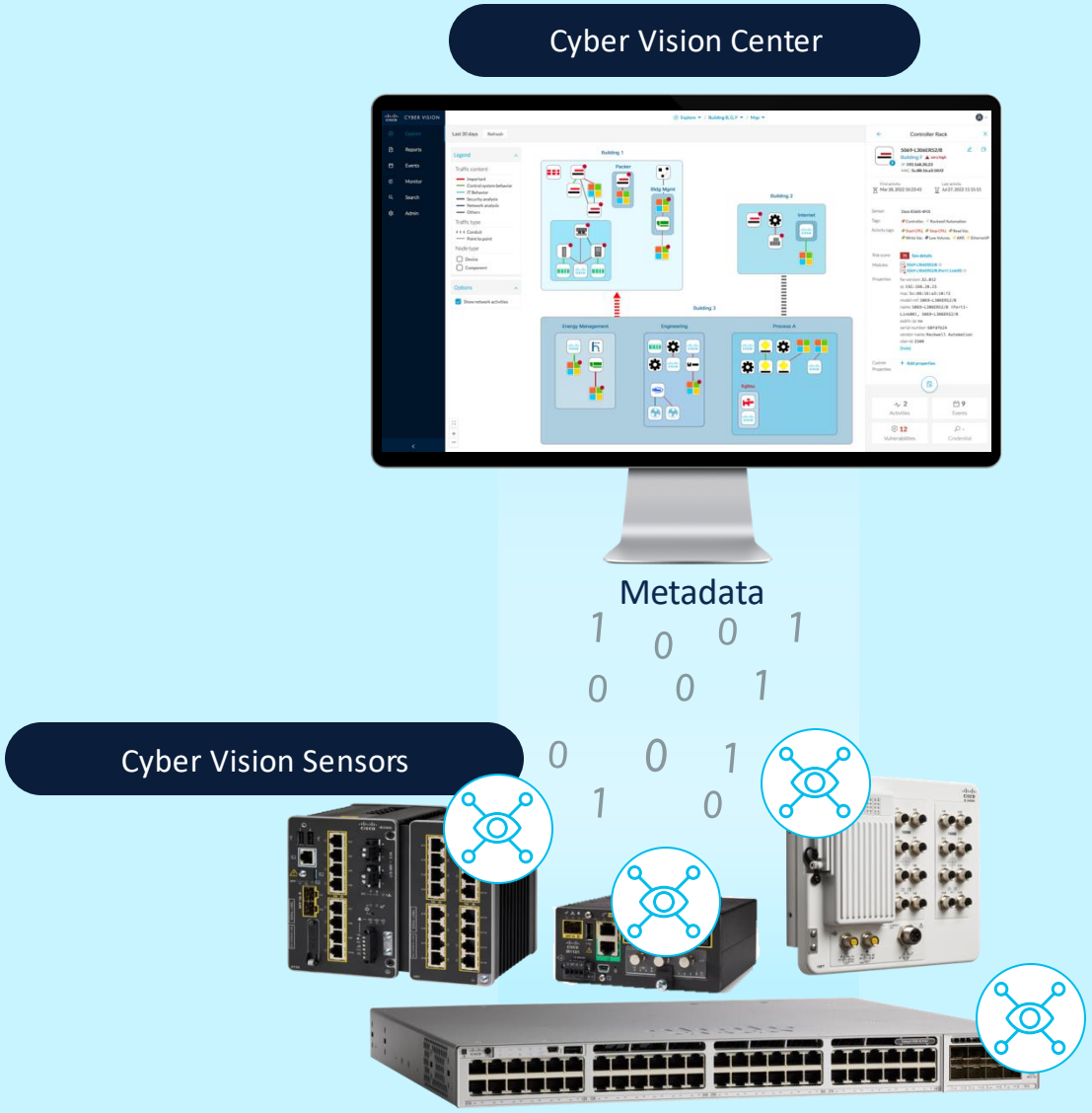
- Custom preset category
- Zone and Conduit visualization
- Active discovery UI
- Inventory report
- DPI enhancements

Enhanced Deployment Capabilities

- Catalyst IR1800 support
- Docker sensor
- Zero-touch provisioning (ZTP)
- Certificate auto renewal

Integrations enhancement

- Splunk Add on App
- API improvements



Deep Packet Inspection and Active Discovery
built into your network infrastructure

Secure Equipment Access + Updates

Existing options are either security backdoors or come with many trade-offs

Ad-Hoc Software

Often installed on operator workstations

Backdoor to IT security policies

Cellular Gateways

Dedicated hardware installed by machine builders

Backdoor to IT security policies

VPN

Always-On, All-or-Nothing access

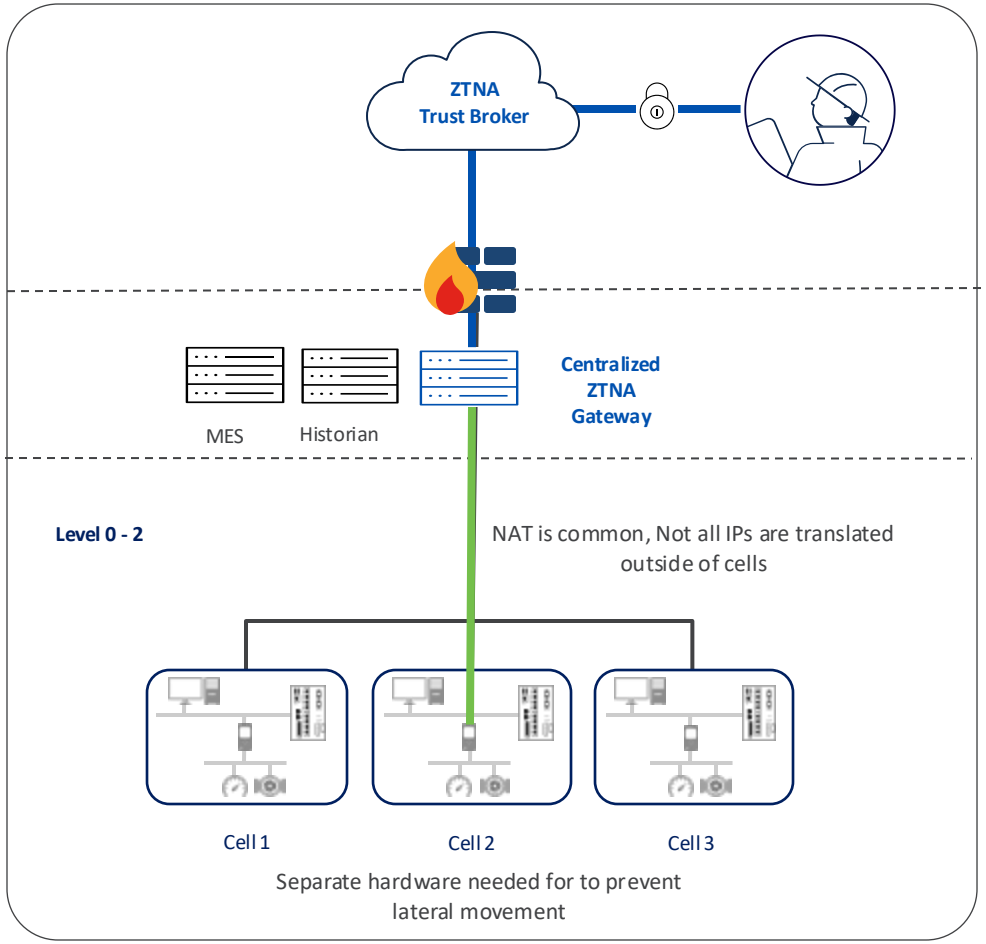
Need additional controls to deny full network access

ZTNA deployed in iDMZ

Provides controlled identity and context-aware access

Challenging to deploy in industrial settings

But existing ZTNA solutions do not translate well to OT



Centralized ZTNA gateway located far from OT Assets

Distributing ruggedized ZTNA gateways among cells in Level 0-2 is expensive, and cumbersome to maintain

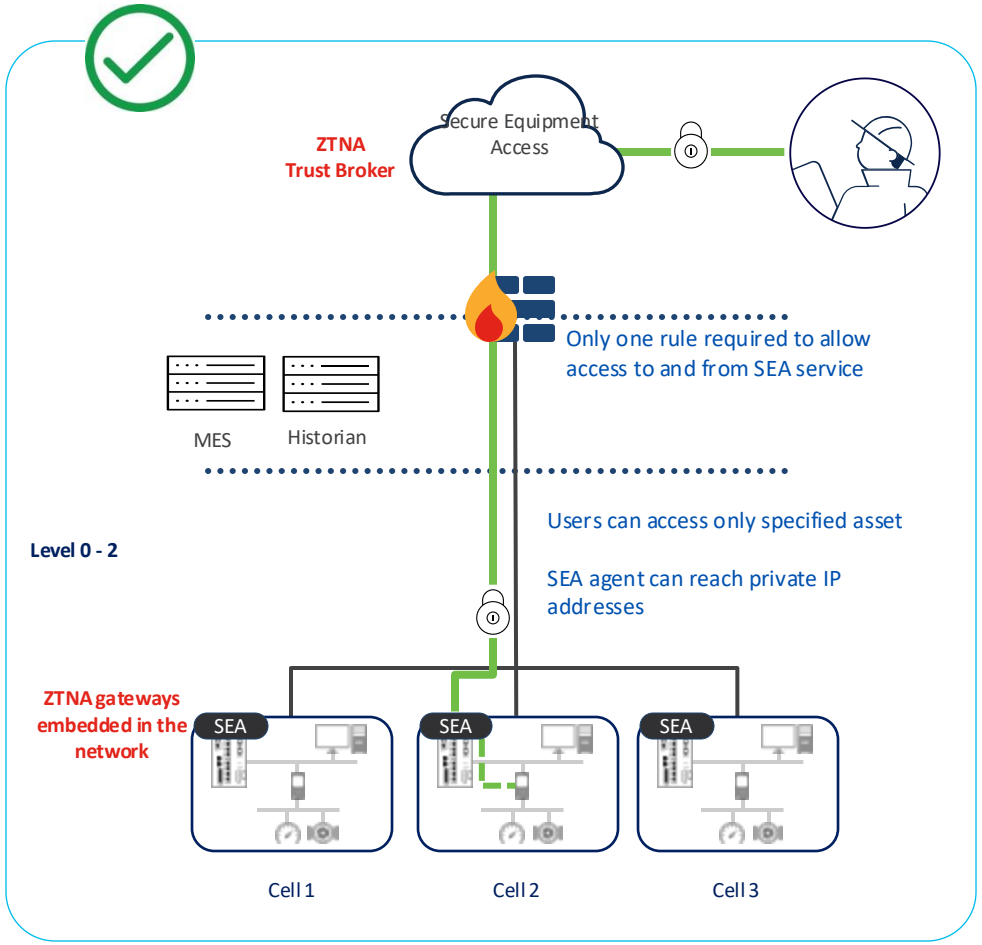
Forces exposing private IPs outside Level-2

Burden end users to unnecessarily NAT private IPs, negating resource isolation and increasing attack surface

Lack control on lateral movement

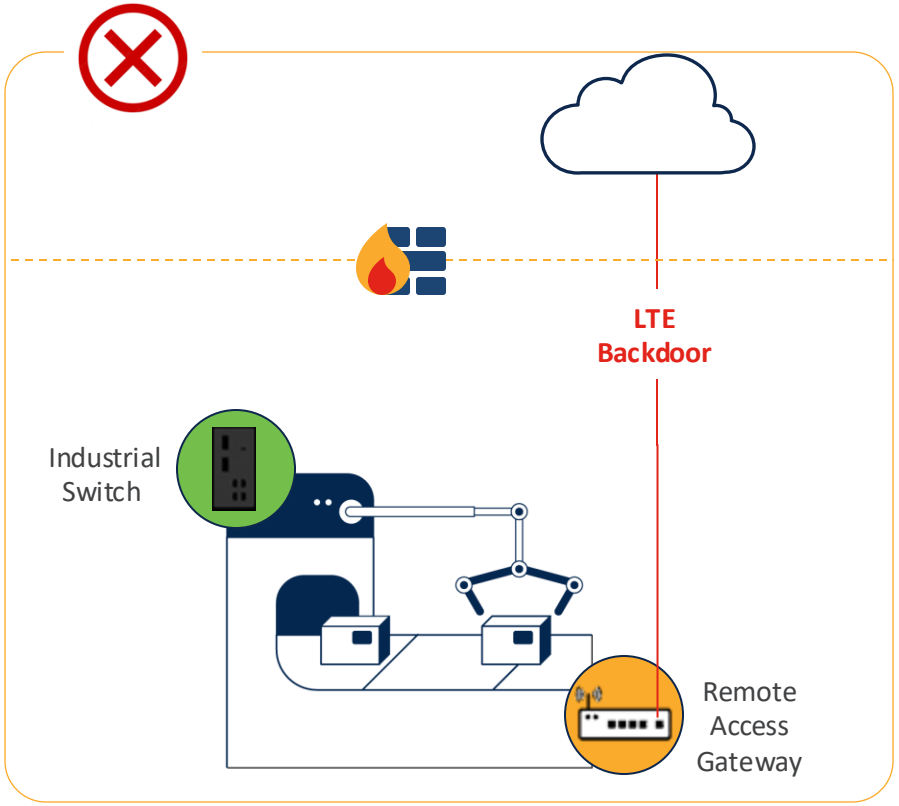
Since gateway is far from the OT assets, a separate solution is needed for east-west segmentation among cells

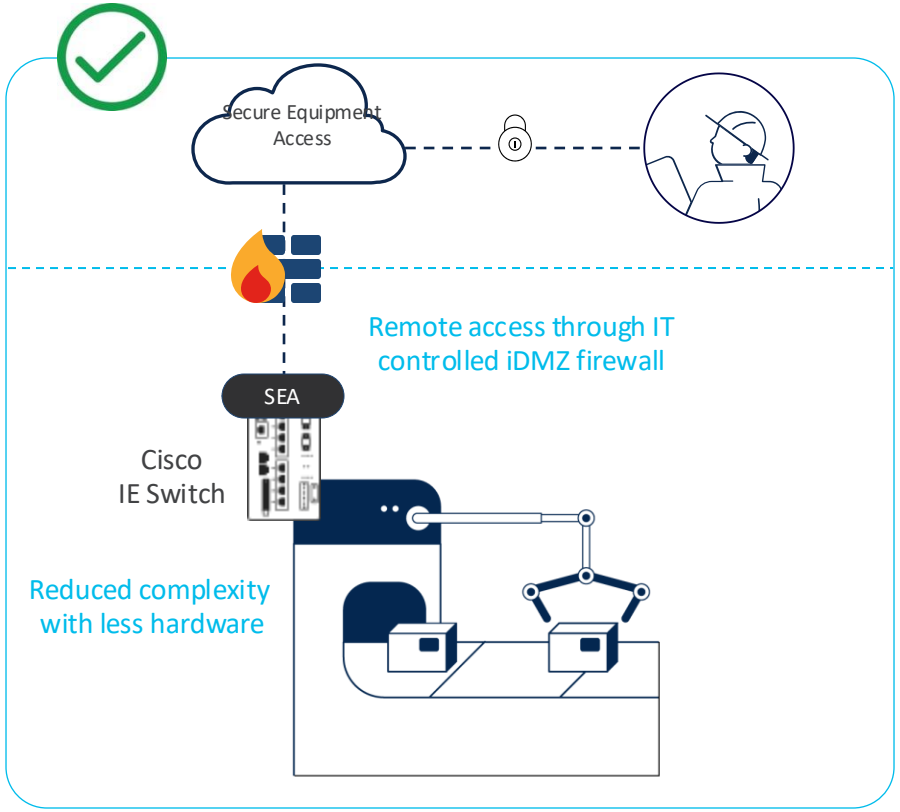
Simple, Scalable, Distributed ZTNA



- Get remote access to assets using the same switch that provides secure connectivity
- Eliminate complexity of creating and managing multiple firewall rules across all your sites
- Maintain resource isolation by traversing NAT boundaries without exposing private IP addresses
- Prevent lateral movement by enforcing segmentation on the switch that runs the ZTNA gateway

Address the shadow IT problem

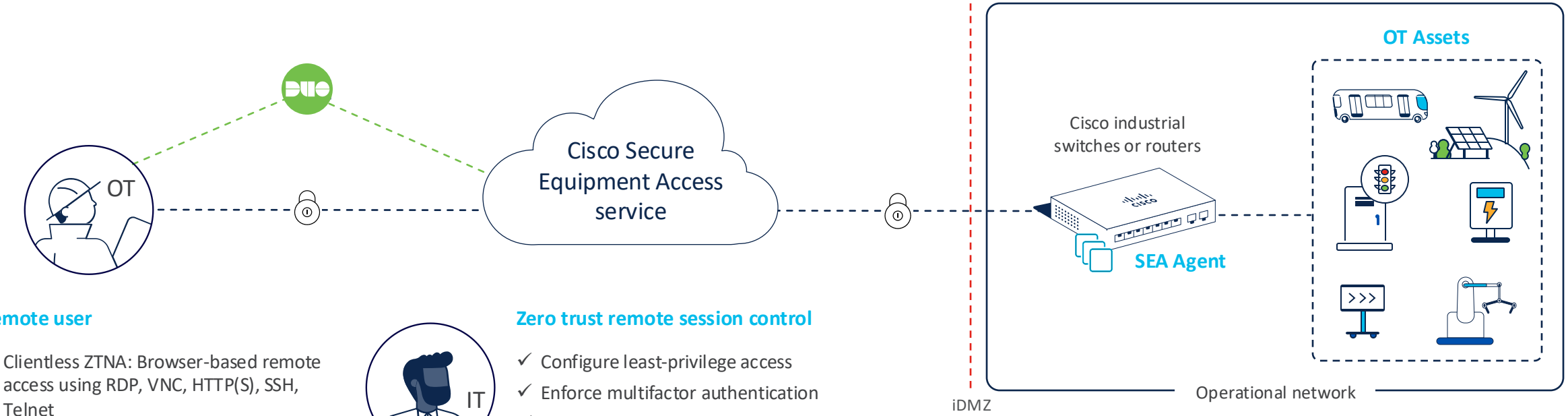




- Eliminate complexity of maintaining point hardware for remote access
- Stop security backdoors from cellular gateways
- Get remote access to assets using the same switch that provides secure connectivity
- Move beyond conventional remote access to ZTNA for OT assets

Cisco Secure Equipment Access

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



Remote user

- ✓ Clientless ZTNA: Browser-based remote access using RDP, VNC, HTTP(S), SSH, Telnet
- ✓ Agent-based ZTNA: remote access that supports native desktop applications

Zero trust remote session control

- ✓ Configure least-privilege access
- ✓ Enforce multifactor authentication
- ✓ Check remote users' security posture
- ✓ Record, monitor, terminate sessions

Cloud simple
Accelerate time to value

Cisco secure
Built to keep operations safe

Designed for OT
Drive business outcomes

Highly scalable
Cloud + network working together

Platforms that support SEA Agent

SEA Agent is the ZTNA gateway function embedded in network platforms

Industrial Switches

IE3300, IE3400

Roadmap

IE3400H

Roadmap
(Q4 CY23)

IE3100

Roadmap
(H2 CY24)

IE9300

Industrial Routers

IR1101

IR1800

Roadmap
(H2 CY24)

IR8300

cisco Engage

GO BEYOND