The bridge to possible

Cisco SD-Access for Manufacturing Verticals

Mahesh Nagireddy
Technical Marketing Engineering, Technical Leader
CCIE R&S

BRKENS-2821

Cisco Webex App

https://ciscolive.ciscoevents.com/ciscolivebot/#BRKENS-2821

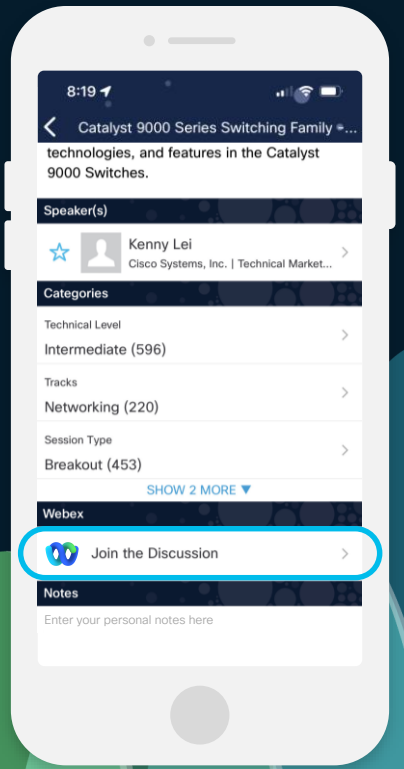
Questions?

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 June 7, 2024.



Cisco Live US SD-Access/ISE Learning Map

Sunday–2nd

- TECENS-2820 9AM
  Cisco Software-Defined Access LISP: Architecture Overview

Monday–3rd

- BRKENS-2810 8:30AM
  Cisco Software-Defined Access LISP Solution Fundamentals
- BRKENS-2800 9:30AM
  Cisco SD-Access Zero-Touch Provisioning Using LAN Automation
- BRKENS-2811 1PM
  Connecting Cisco SD-Access LISP to the World: Use Cases and Segmentation
- LTRENS-2419 1PM
  SD-Access LISP Pub/Sub Wired Lab
- BRKENS-2816 3PM
  Cisco SD-Access Transit: Advanced Design Principles
- BRKSEC-2100 10:30AM
  ISE Your Meraki Network with Group Based Adaptive Policy
- BRKENS-1802 2:30PM
  SD-Access Success Stories: Concept to Reality by Petrobras and Ford Motor
- BRKSEC-2091 3PM
  Cisco ISE Performance, Scalability and Best Practices
- BRKENS-1852 4PM
  TrustSec Refresh Reinforced with Latest Segmentation Innovations

Tuesday–4th

- BRKENS-2502 10:30AM
  Cisco SD-Access LISP VXLAN Fabric Best Practices: Design and Deployment
- BRKENS-1801 4PM
  SD-Access Success Stories: Concept to Reality by Stanford Health and Yale University

Wednesday–5th

- BRKENS-2833 10:30AM
  LISP: Optimized Control Plane for Software-Defined Access
- BRKENS-2819 2:30PM
  Cisco SD-Access and Multi-Domain Segmentation
- CIUG-1003 2:30PM
  Zero Trust with Software-Defined Access Roadmap Update
- BRKENS-2821 4:00PM
  Cisco SD-Access LISP VXLAN Fabric for Manufacturing Verticals

Thursday–6th

- BRKENS-2827 11:00AM
  Cisco SD-Access Migration Tools and Strategies

Catalyst Center — Cisco SD-Access LISP

ISE — Cisco ISE

BU-led sessions

Agenda

- Introduction
- Operational Technology and its Challenges
- SD-Access
- OT Design Options
- Conclusion

Cisco Catalyst Center (formerly Cisco DNA Center)

Cisco SD-Access LISP Fabric

Industry Leading Campus Architecture

Deployments

4050+

Momentum

40%

YoY growth in customers

Key use case

70%

Wireless

+ 66%

API (YoY)

Usage

24K+

Sites

1.8M+

Devices

Miercom PERFORMANCE VERIFIED

Top verticals: Government, Finance, Professional services, and Manufacturing

Adopted by 31% of U.S. **Fortune 100** Companies

EMEA: 52%

Americas 29%

APJC 20%

Modern, Open and Scalable Fabrics

IETF Standard based Protocols

Cisco Catalyst Center

Cisco SD-Access

LISP VXLAN Fabric*

Cisco Catalyst 9000

BGP EVPN VXLAN Fabric

IETF

IETF

Enterprise

Healthcare

Education

Financial

Public Sector

Manufacturing

Hospitality

Media

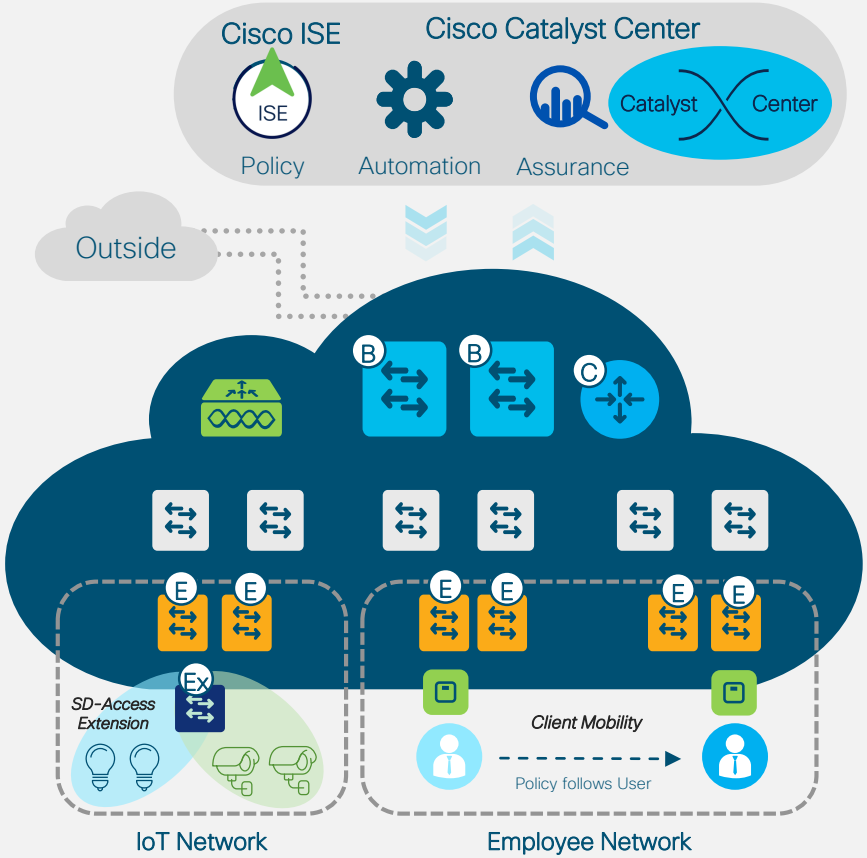
Transportation

Retail

*Cisco's Lead Motion

Cisco Software Defined Access

The Foundation for Cisco's Intent-Based Network



One Automated Network Fabric

Single fabric for Wired and Wireless with full automation

Identity-Based Policy and Segmentation

Policy definition decoupled from VLAN and IP address

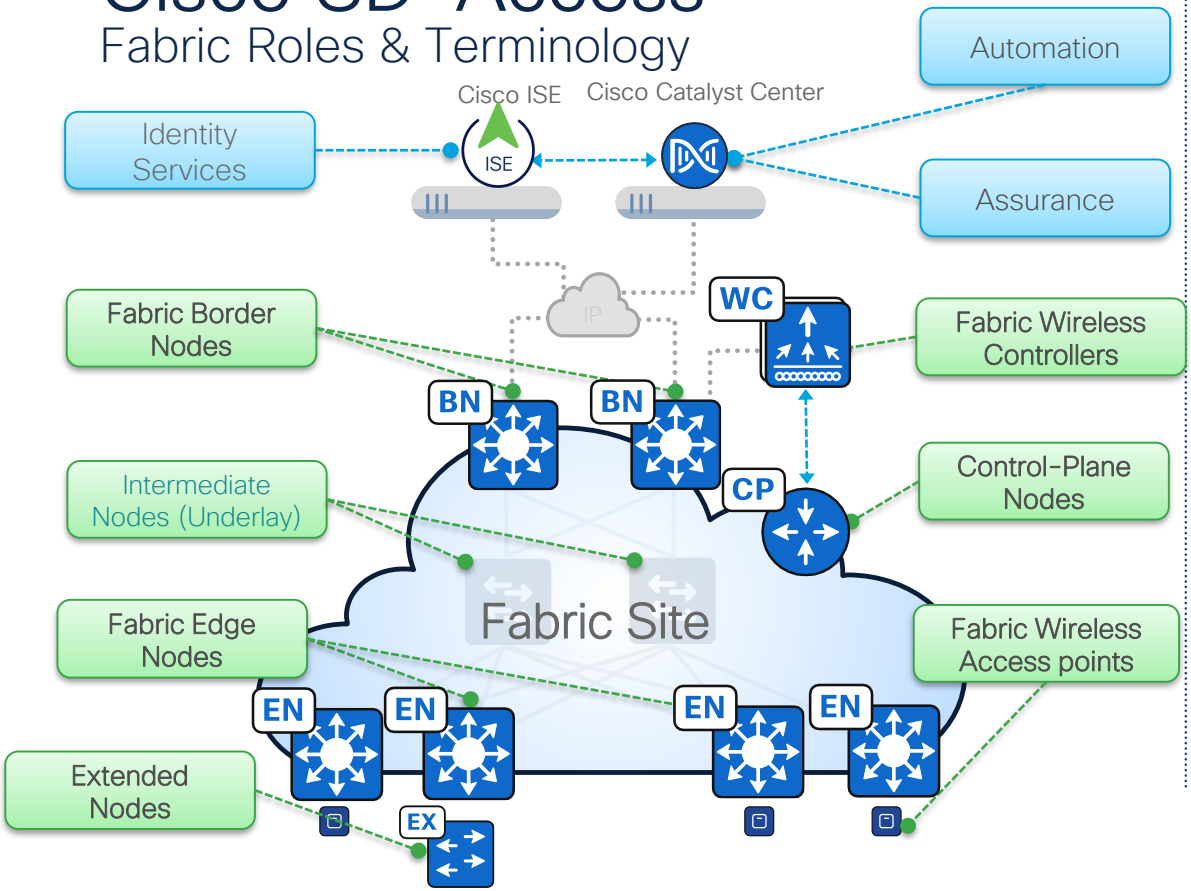
AI-Driven Insights and Telemetry

Analytics and visibility into User and Application experience

For your reference

Cisco SD-Access

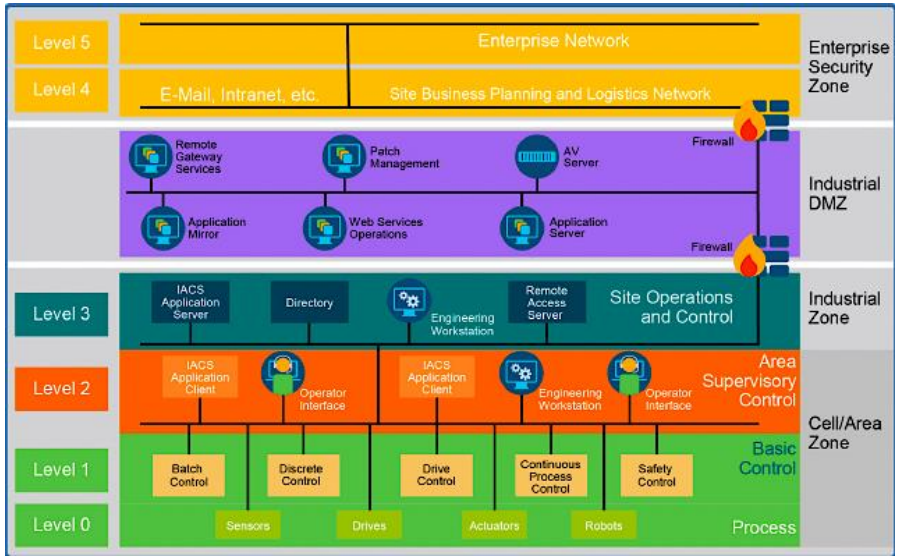
Fabric Roles & Terminology



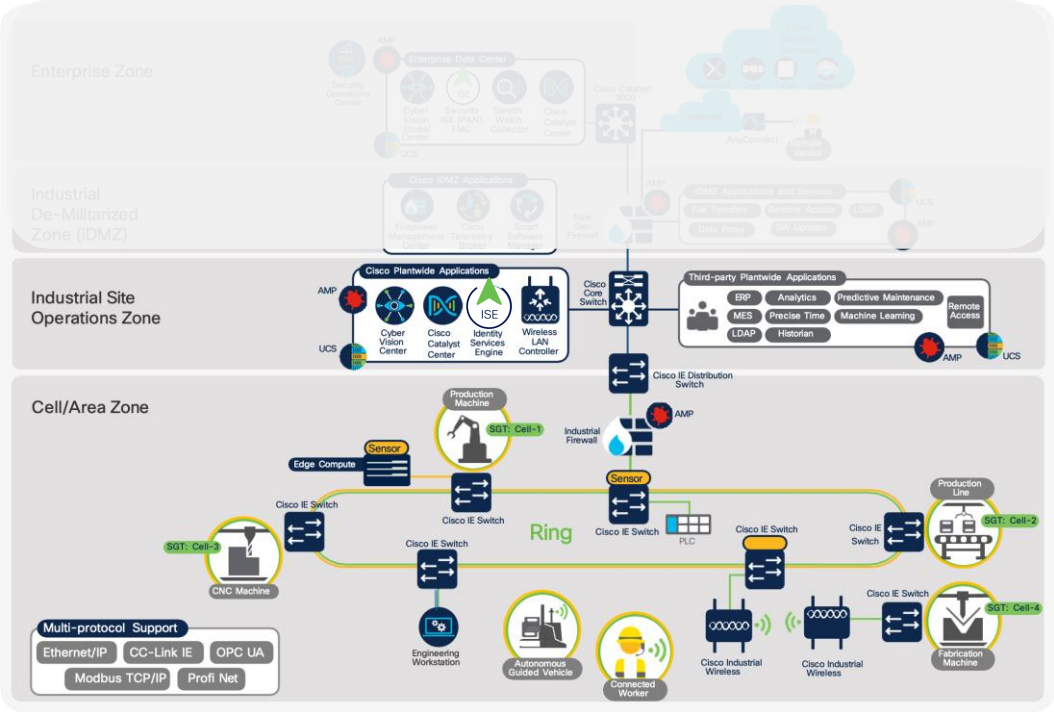
- **Network Automation** – Simple GUI and APIs for intent-based Automation of wired and wireless fabric devices
- **Network Assurance** – Data Collectors analyze Endpoint to Application flows and monitor fabric device status
- **Identity Services** – NAC & ID Services (e.g. ISE) for dynamic Endpoint to Group mapping and Policy definition
- **Control-Plane Nodes** – Map System that manages Endpoint to Device relationships
- **Fabric Border Nodes** – A fabric device (e.g. Core) that connects External L3 network(s) to the SD-Access fabric
- **Fabric Edge Nodes** – A fabric device (e.g. Access or Distribution) that connects Wired Endpoints to the SD-Access fabric
- **Extended Nodes** – An Extended nodes are switches that run in pure layer 2 mode and do not natively support fabric technology.
- **Fabric Wireless Controller** – A fabric device (WLC) that connects Fabric APs and Wireless Endpoints to the SD-Access fabric

Operational Technology(OT)

Industrial Plant Reference Architecture(Purdue Model)

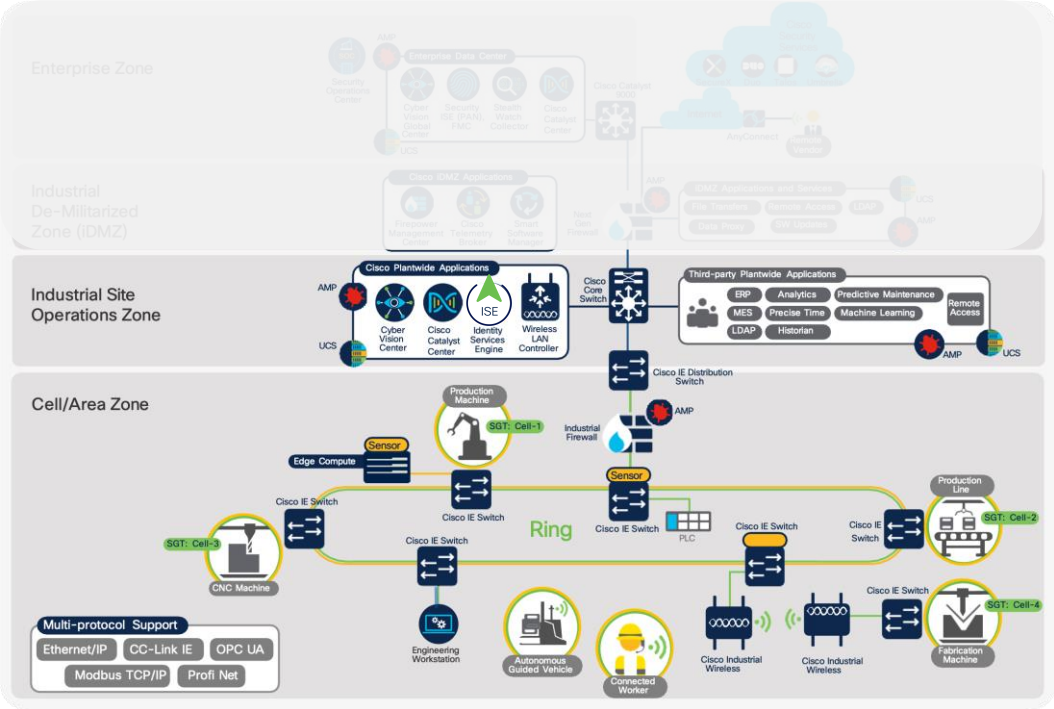


Challenges with Operational Technology



- Industrial Automation and Control Requirements
  - Core of Modern production facilities
  - Device Types
  - Location
  - Latency Sensitive
  - Protocols
  - Need Tighter Synchronization

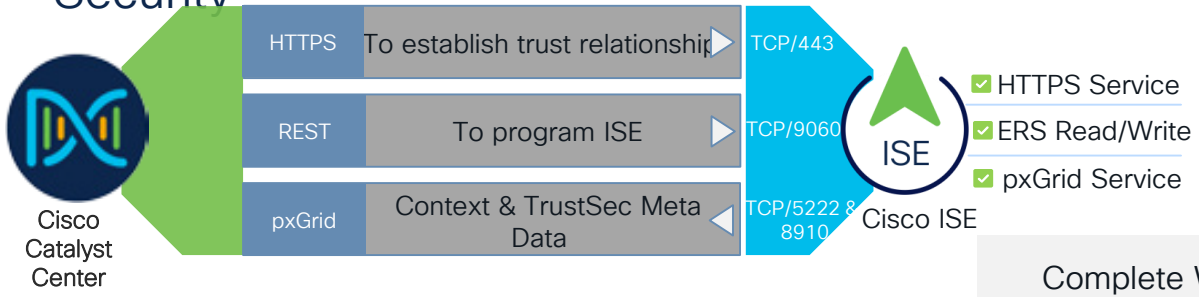
Challenges with Operational Technology



- Industrial Automation and Control Requirements
- Security
  - Implicit Trust
  - Separated or Air Gapped
  - Use Firewall
  - Application moving towards Cloud

Solutions to OT Challenges

Security



Complete Workplace Zero-Trust w/ SDA

AI/ML based multi-factor endpoint classification for IoT Visibility

Traffic analysis for granular policy discovery

Automated threat isolation and remediation

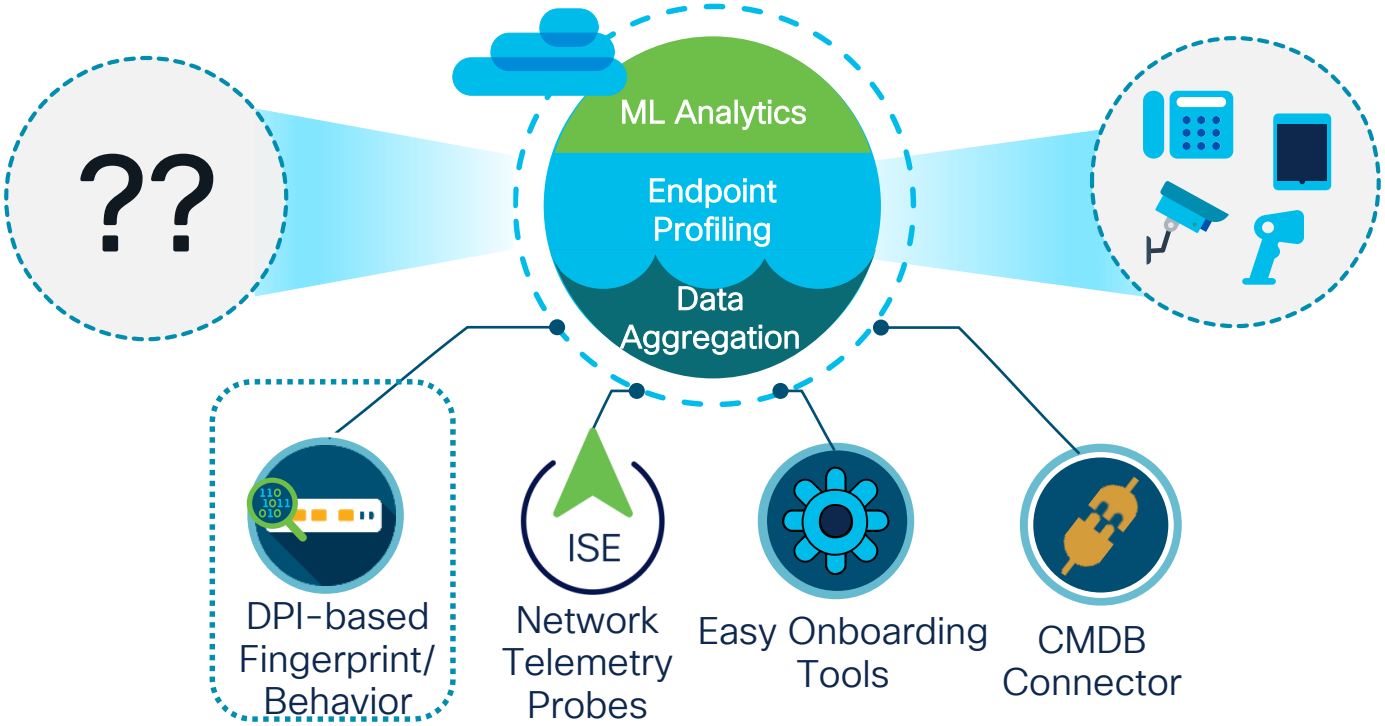
Flexible Macro/Micro segmentation with SD-Access

AI/ML-led network behavior anomaly detection

Solutions to OT Challenges

Security – Cisco Endpoint Analytics

Rapidly reducing the unknowns by aggregating data from different sources

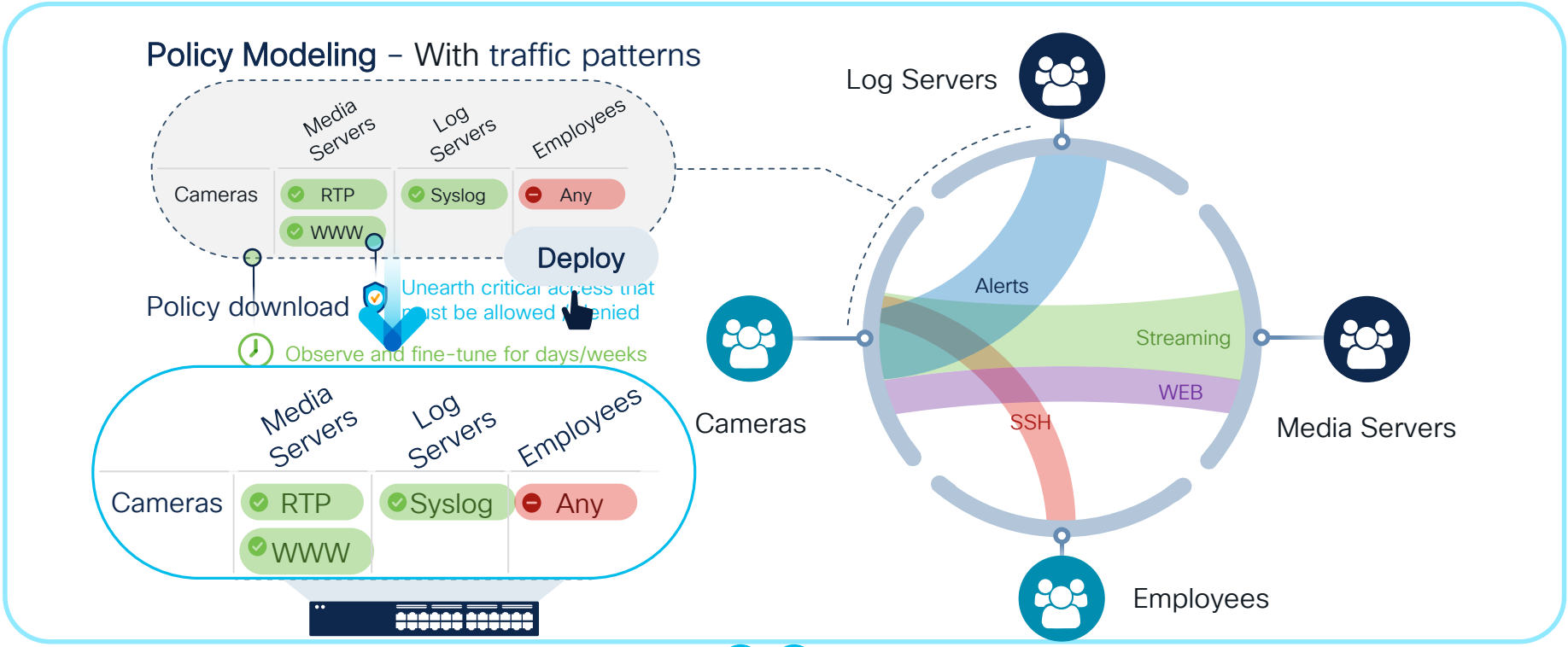


Classifying endpoints

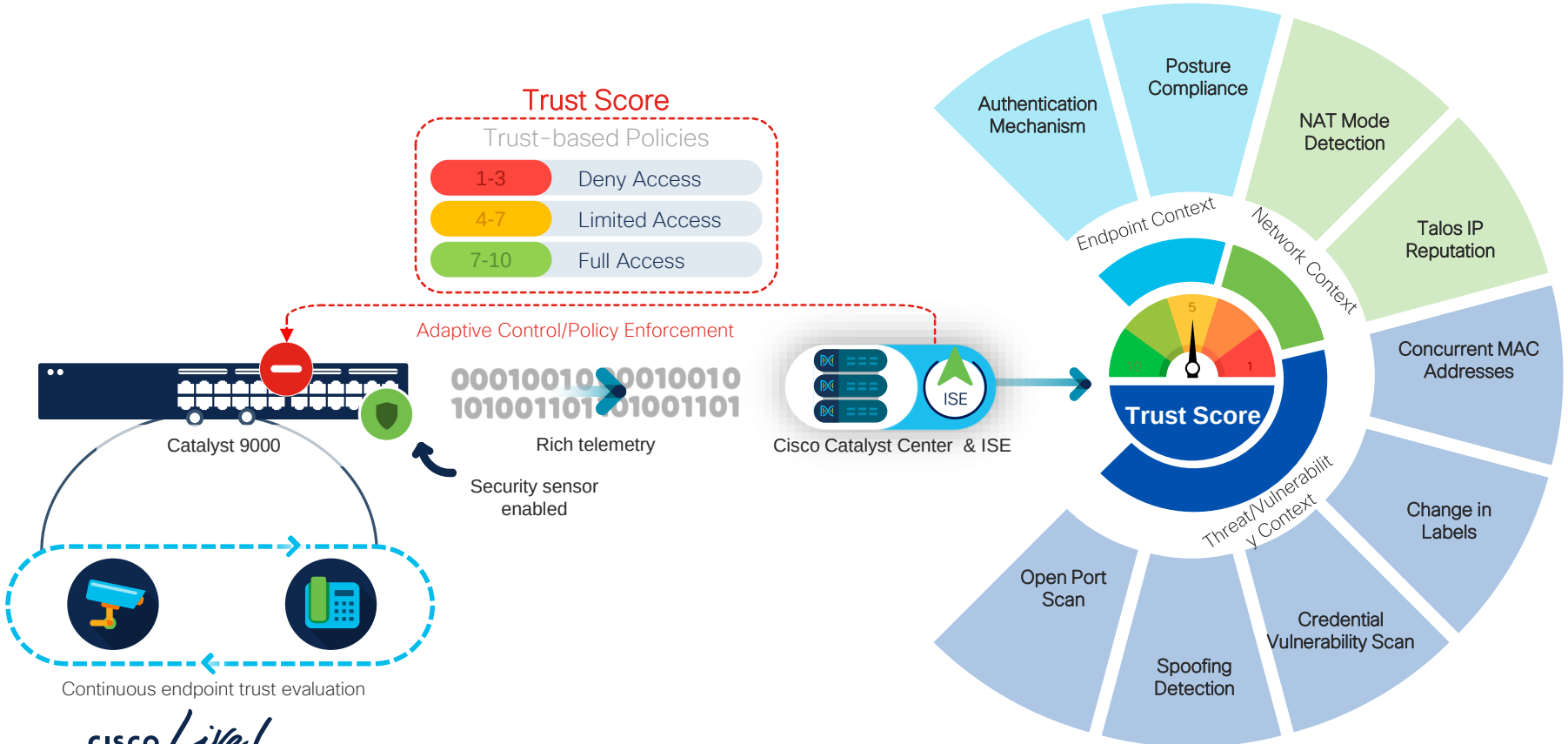
- Device type
- Hardware model
- Hardware MFR
- Operating system

CMDB: Configuration Management Database

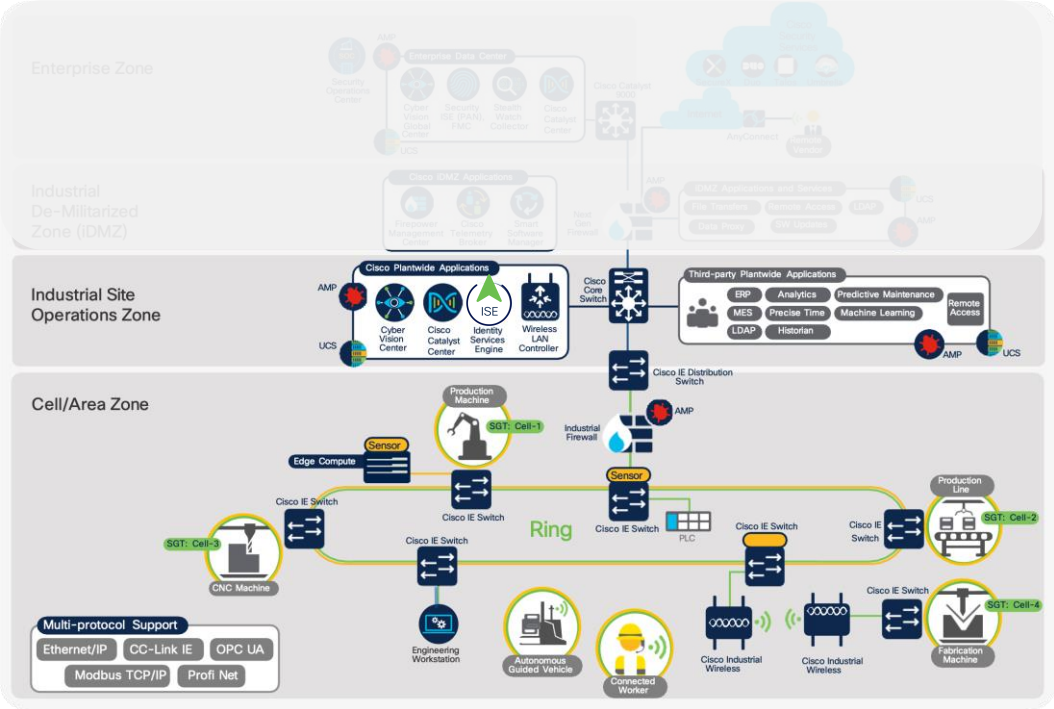
Solutions to OT Challenges
Security – Policy Analytics



Solutions to OT Challenges
Security – Trust Score for Endpoints

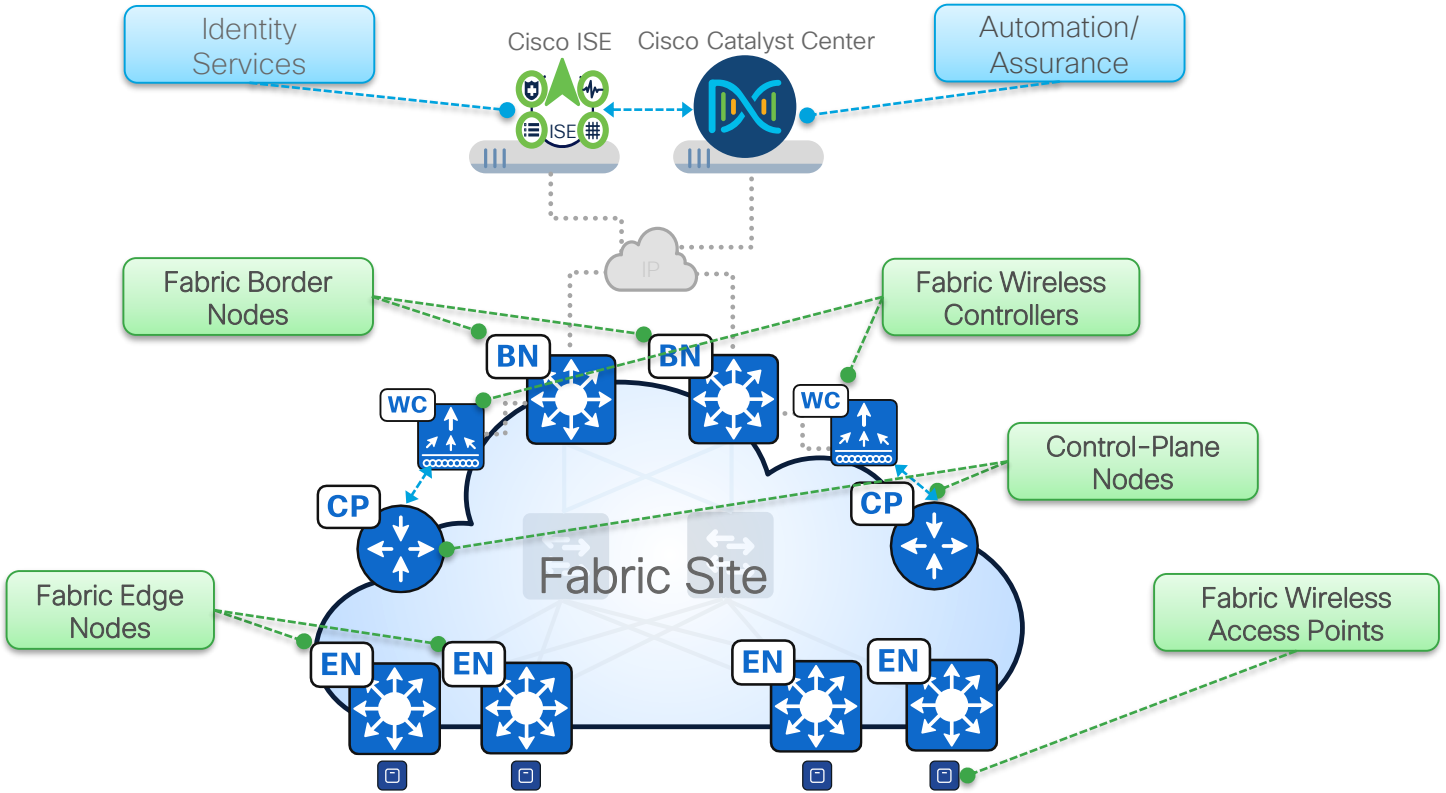


Challenges with Operational Technology

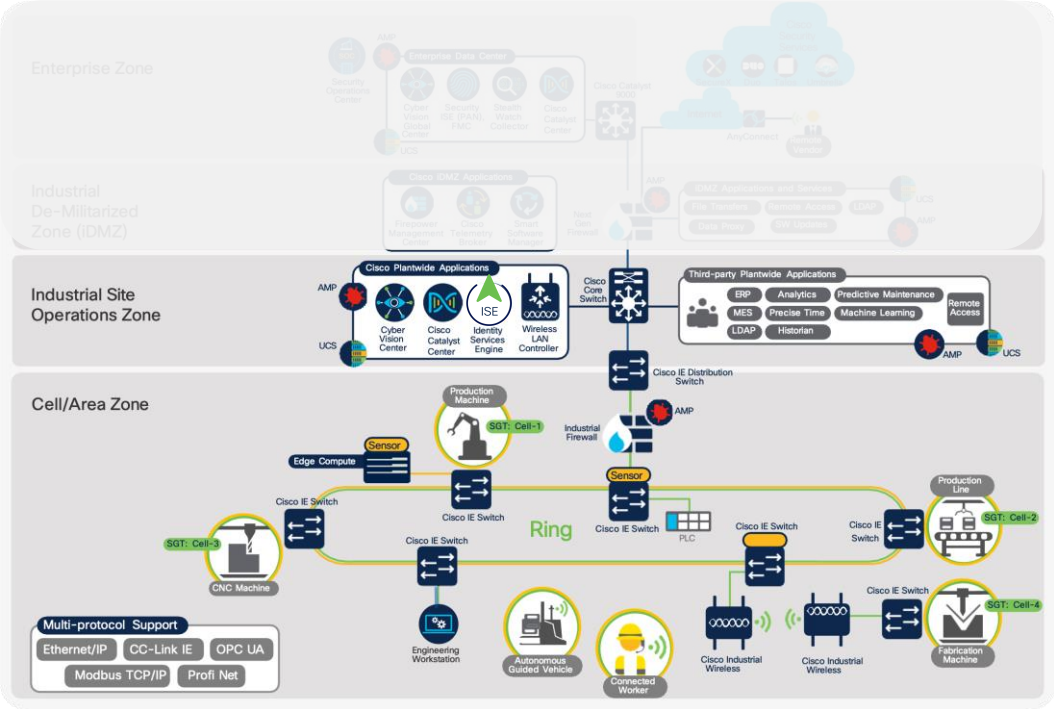


- Industrial Automation and Control Requirements
- Security
- Network Resiliency and Uptime
  - Highly Critical
  - Network Impact

Solutions to OT Challenges
Network Resiliency and Uptime

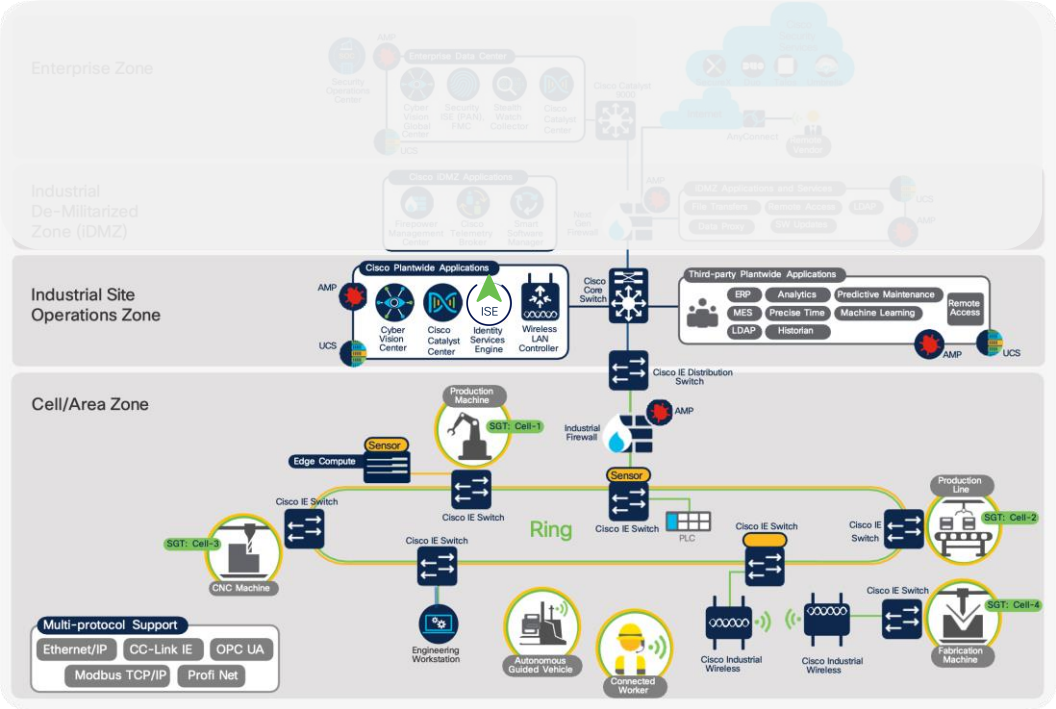


Challenges with Operational Technology



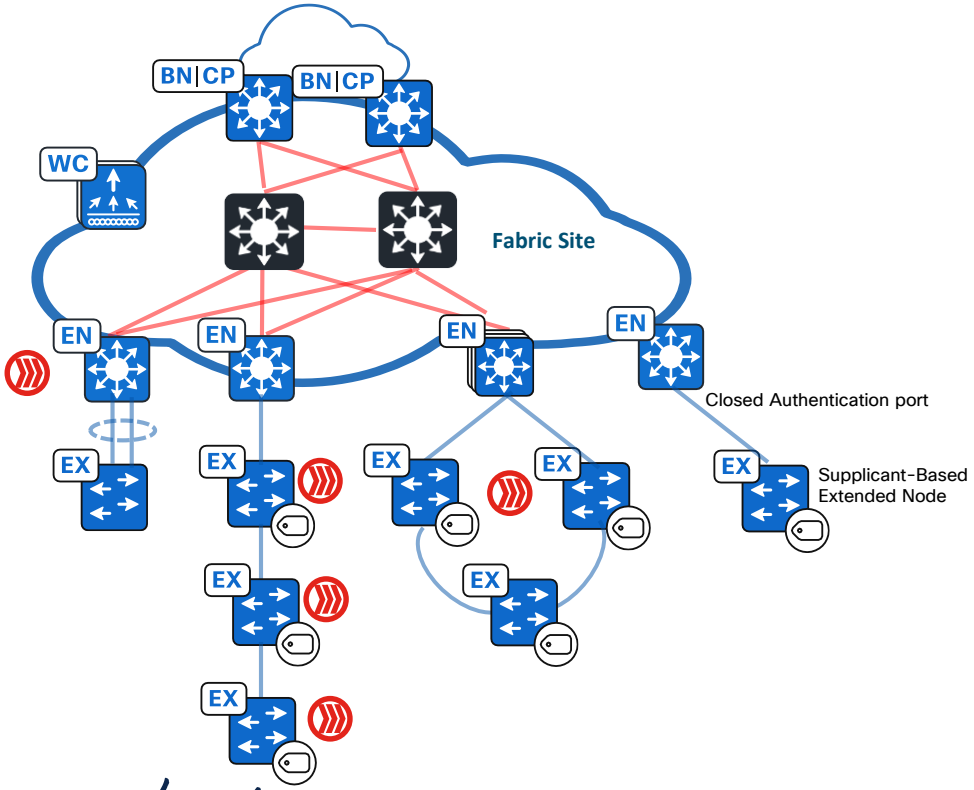
- Industrial Automation and Control Requirements
- Security
- Network Resiliency and Uptime
- Environmental
  - Withstand Harsh Conditions

Challenges with Operational Technology



- Industrial Automation and Control Requirements
- Security
- Network Resiliency and Uptime
- Environmental
- Connectivity
  - Far more geographically distributed
  - Too costly to home run connections

Solutions to OT Challenges
Environmental and Connectivity



Two Types
- Extended Node(EX)
- Policy Extended Node(PEN)
- Supplicant-based Extended Node(SBEN)

Supported devices

EX Node
- IE3200
- IE3300
- IE4000
- IE4010
- IE5000
- Cat9K*(Ess License)
- ESS-9300
- CDB Series

PEN Node
- IE3400
- IE3400H
- Cat9K*(Adv License)
- IE9300

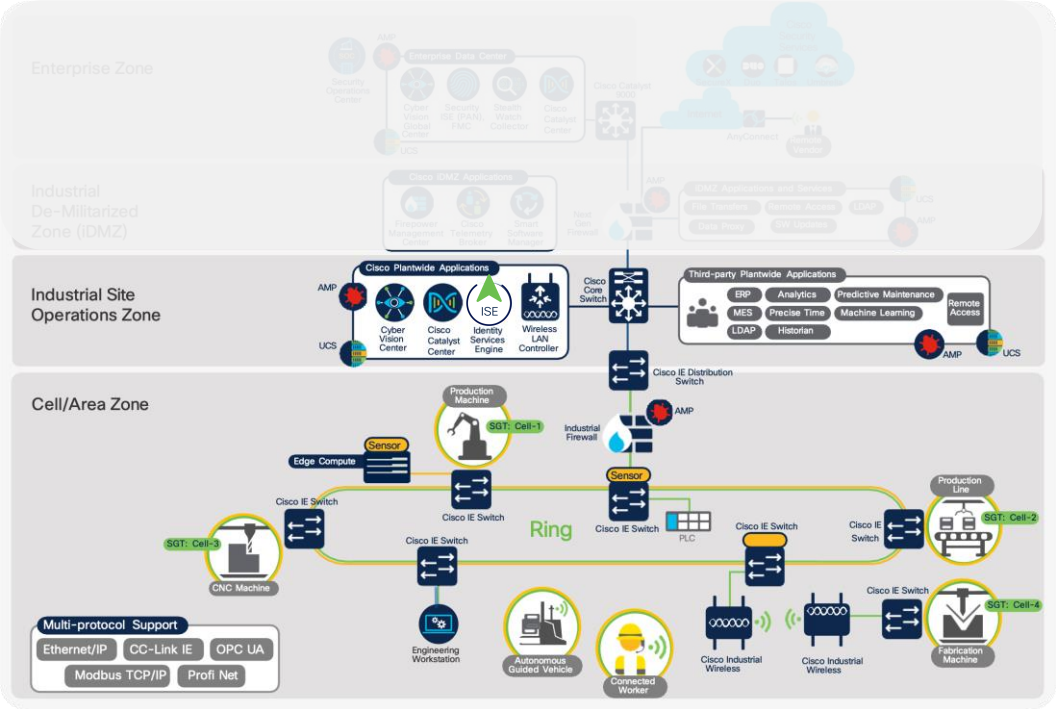
SBEN Node
- C9200
- C9300
- C9400
- C9500

Supported Topologies
- Daisy Chain(Like device type)**
  - Max of 18 IE switches
  - Max of 3 Cat9k switches
- Ring(Like device type)
  - Max of 18 IE switches

Enforcement

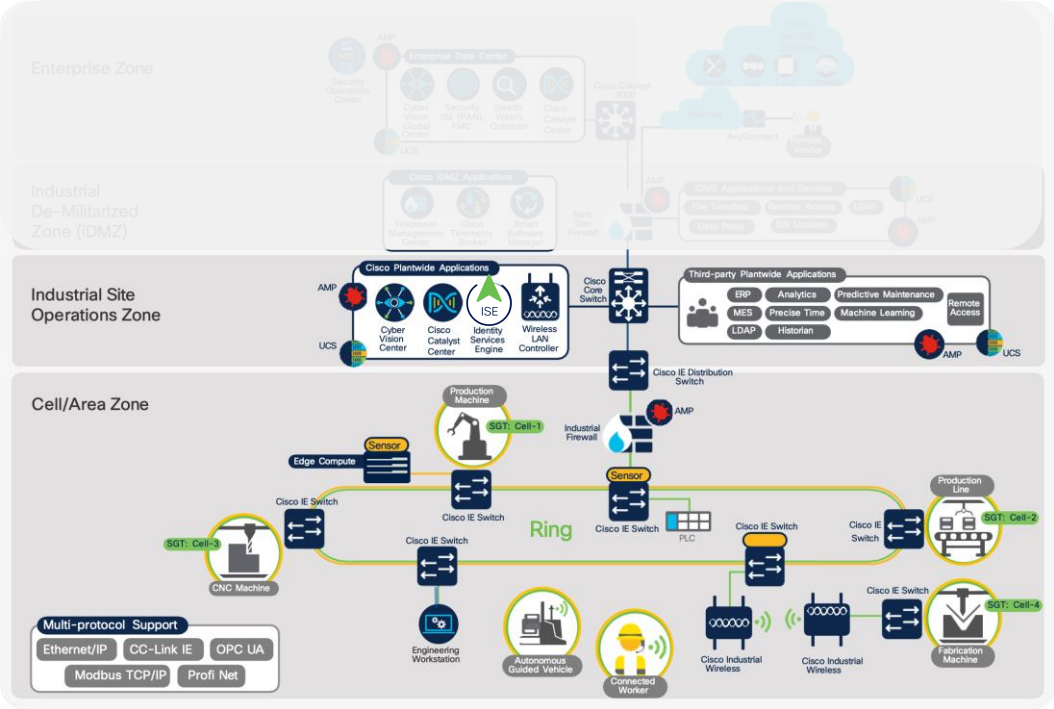
*- Excluding C9600
** EX and PEN Only

Challenges with Operational Technology



- Industrial Automation and Control Requirements
- Security
- Network Resiliency and Uptime
- Environmental
- Connectivity
- Upgradeability
  - Uptime is Critical

Challenges with Operational Technology



- Industrial Automation and Control Requirements
- Security
- Network Resiliency and Uptime
- Environmental
- Connectivity
- Upgradeability
- Resources and Access to Networking Skills
  - Team without networking skill sets
  - No access to Network management tools

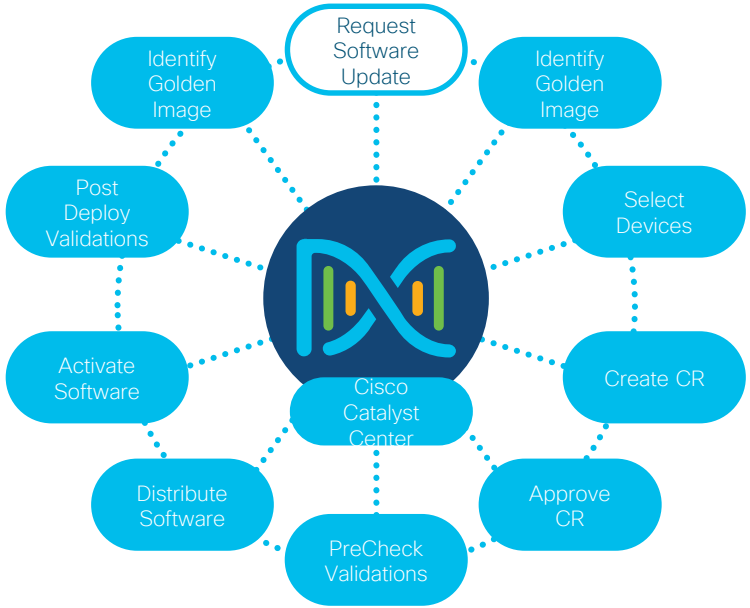
Solutions to OT Challenges
Upgradeability

Intent Based Network Upgrades
Captures your upgrade intent to automate process and drive consistency

Streamlined Upgrade Process
Upgrade base image, patches, and other add-ons in one single flow

Trustworthiness Integration
Assures that device images are not compromised in any way.

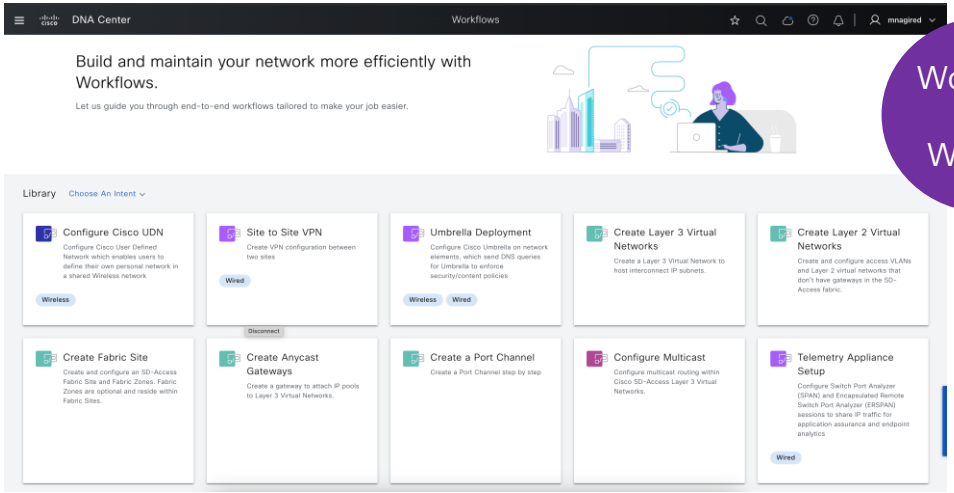
Patching Support
Pre/Post check ensures updates do not have adverse effects on network



Automate your software upgrade cycle

Solutions to OT Challenges

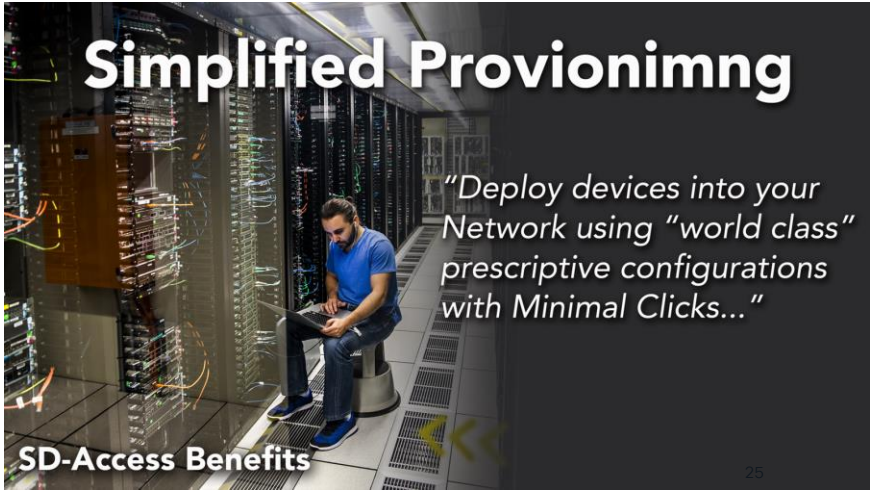
Resources and Access to Networking Skills – Workflows



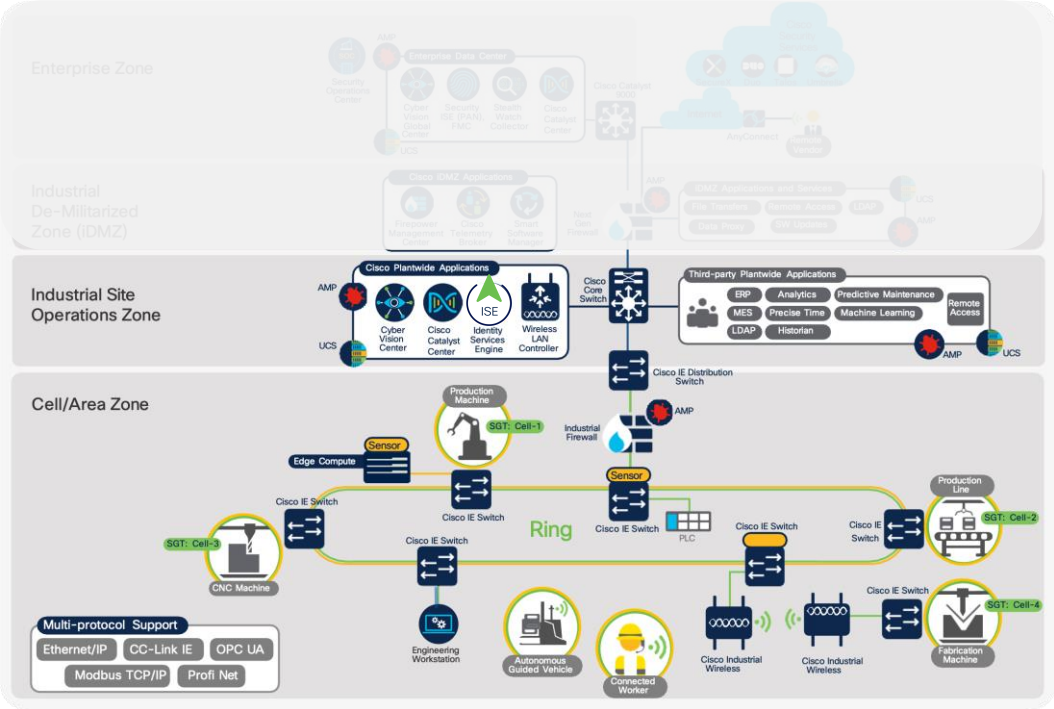
Workflow = Wizards

New Navigation Flow

The new Fabric Sites page contains an Overview, a map, and list view of fabric sites and links to Fabric Infrastructure and Host Onboarding pages.

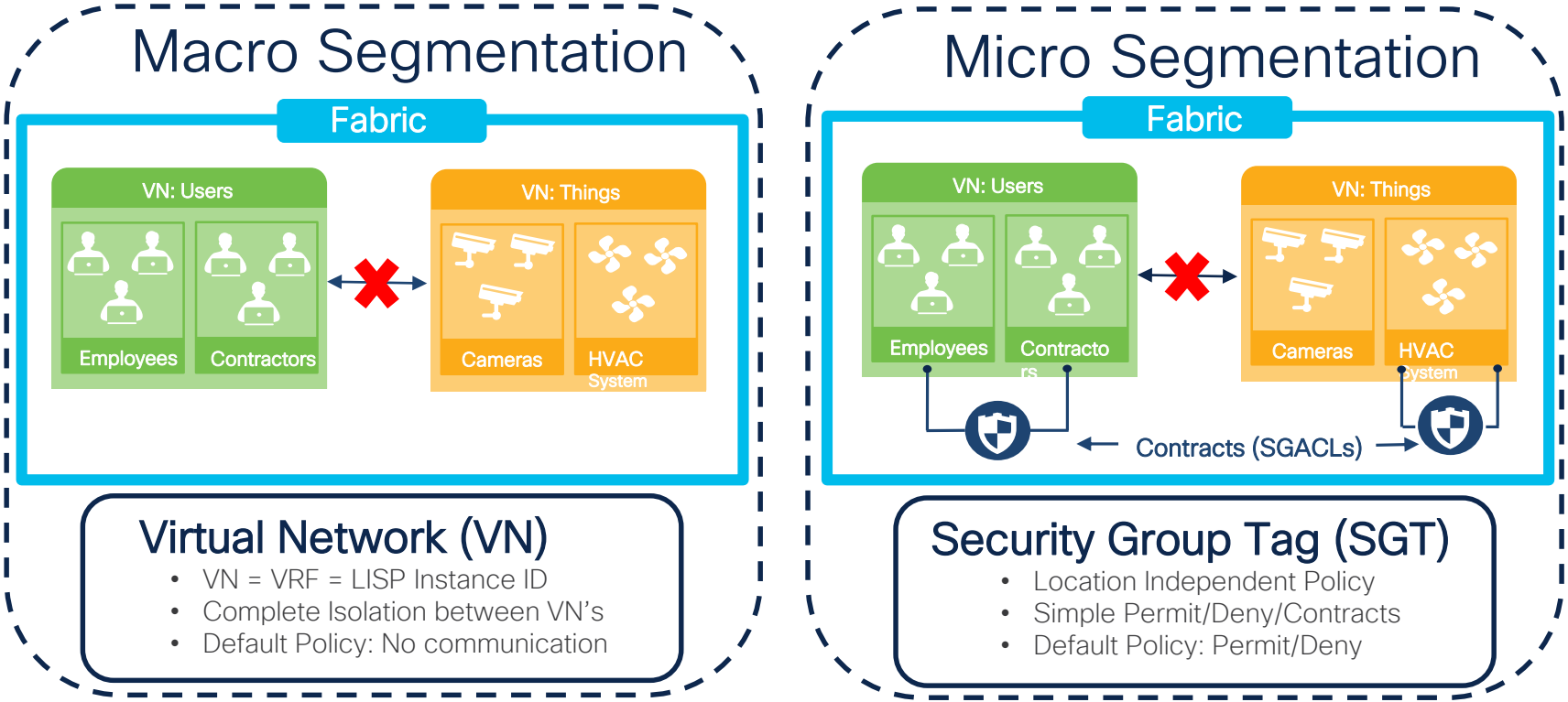


Challenges with Operational Technology



- Industrial Automation and Control Requirements
- Security
- Network Resiliency and Uptime
- Environmental
- Connectivity
- Upgradeability
- Resources and Access to Networking Skills
- Network Segmentation
  - Vlan based Segmentation
  - Physically separate OT Networks

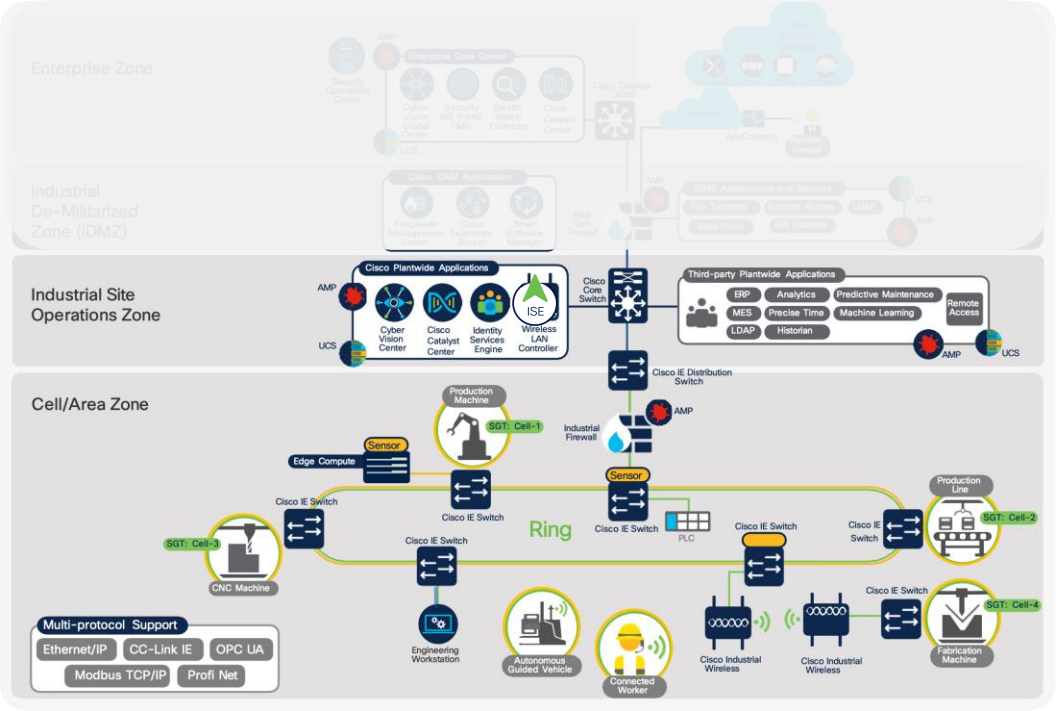
Solutions to OT Challenges
Network Segmentation



Virtual Network (VN)
- VN = VRF = LISP Instance ID
- Complete Isolation between VN's
- Default Policy: No communication

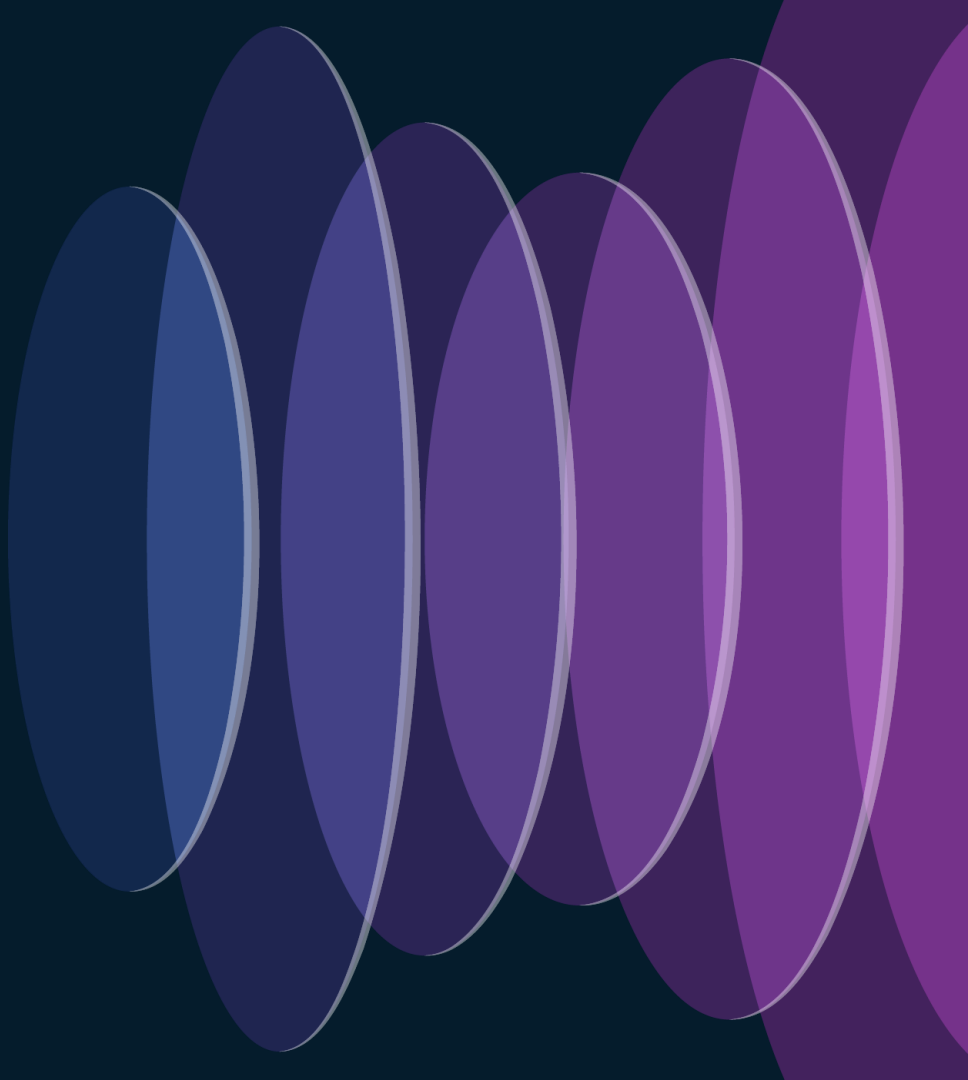
Security Group Tag (SGT)
- Location Independent Policy
- Simple Permit/Deny/Contracts
- Default Policy: Permit/Deny

Challenges with Operational Technology



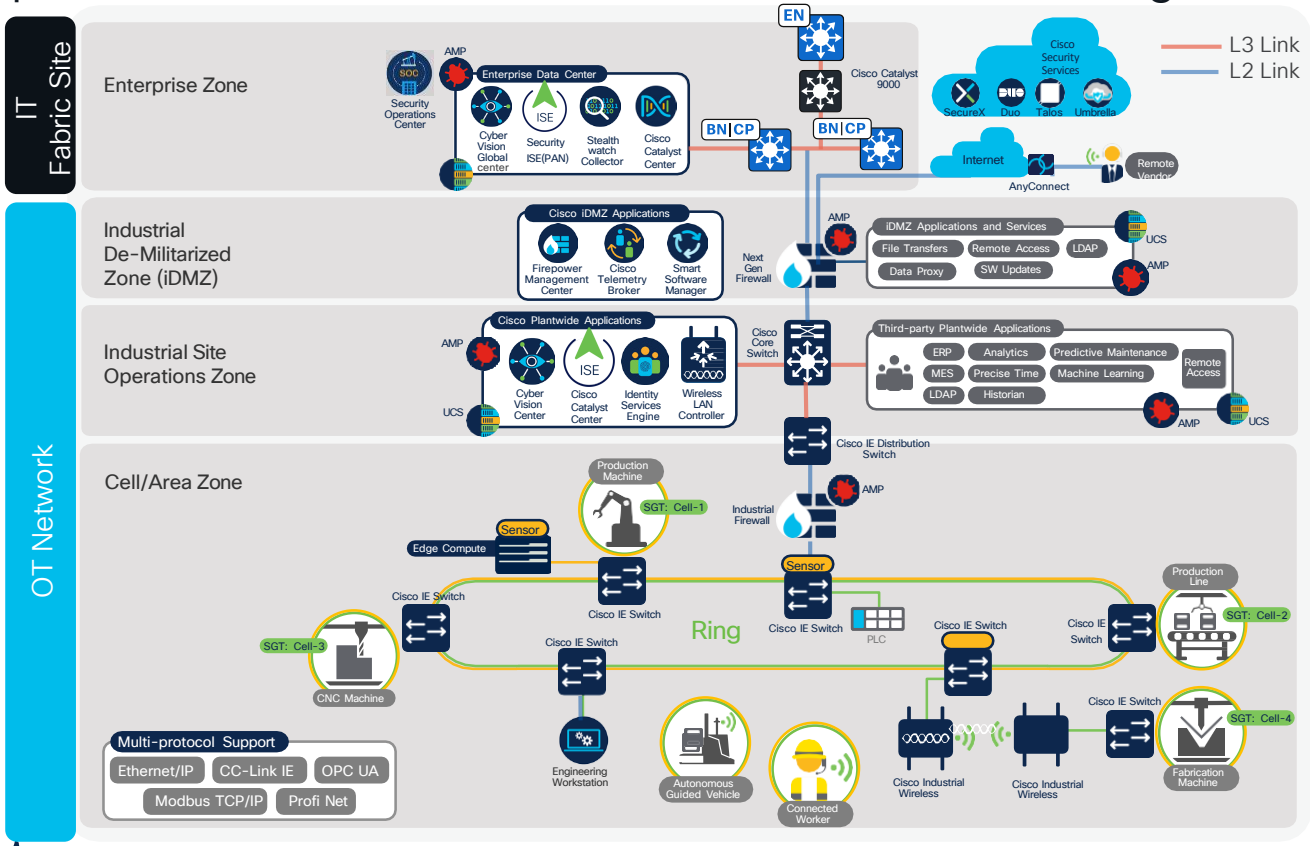
- Industrial Automation and Control Requirements
- Security
- Network Resiliency and Uptime
- Environmental
- Connectivity
- Upgradeability
- Resources and Access to Networking Skills
- Network Segmentation
- IP Addressing
  - Static IP address
  - Same IP Subnets repeated across Cell/Area's
  - NAT

Designs Options



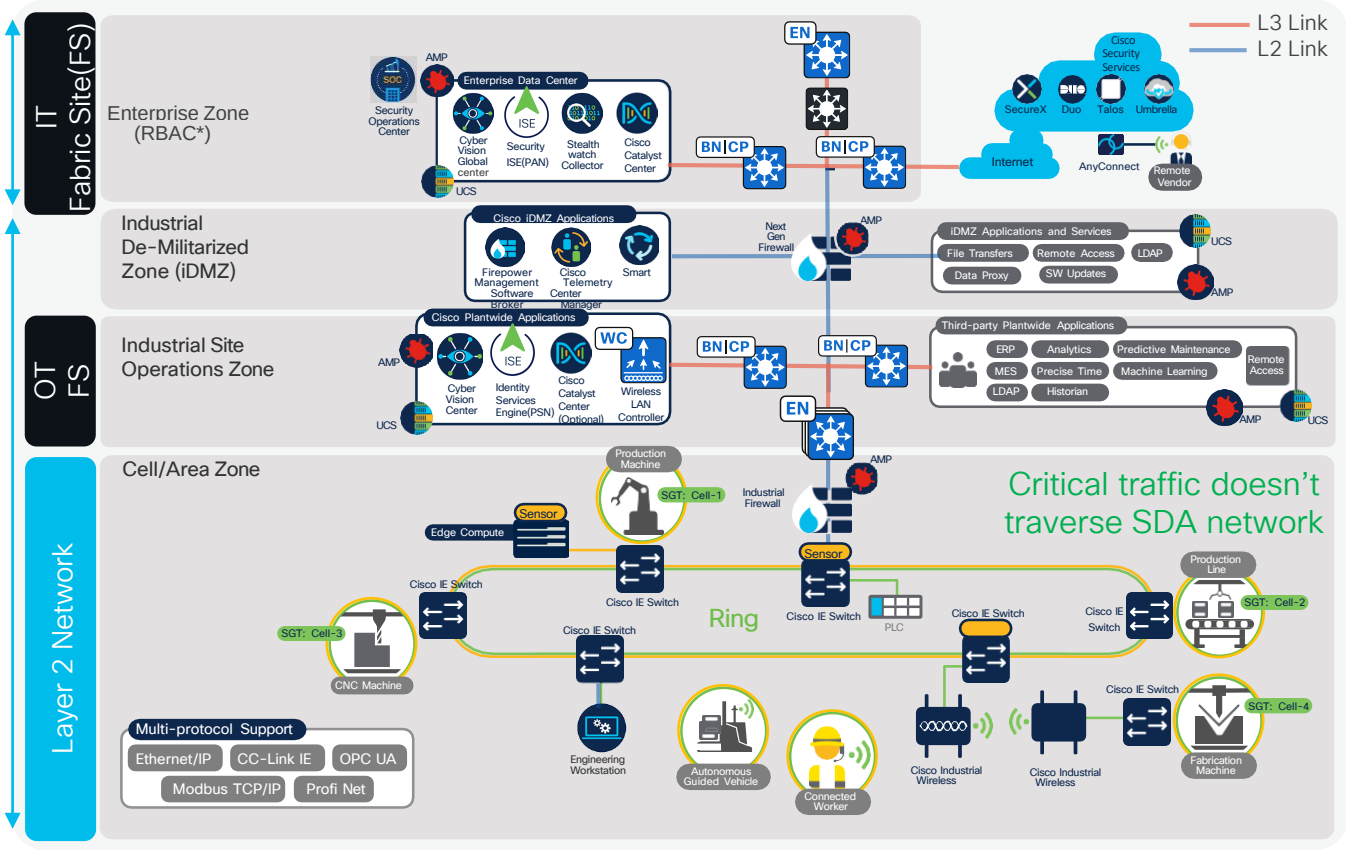
SD-Access Manufacturing Vertical

Enterprise IT SD-Access Fabric with Non-Fabric OT Design



SD-Access Manufacturing Vertical

Enterprise IT with Partial OT SD-Access Fabric Design



SD-Access Manufacturing Vertical
Enterprise IT with Partial OT SD-Access Fabric Design

PROS

- Provides OT/IT separation.
- IT assigns IP pools and downlinks to OT.
- Easy transition for OT persona as no change in tools is needed.
- Cisco standard architecture

CONS

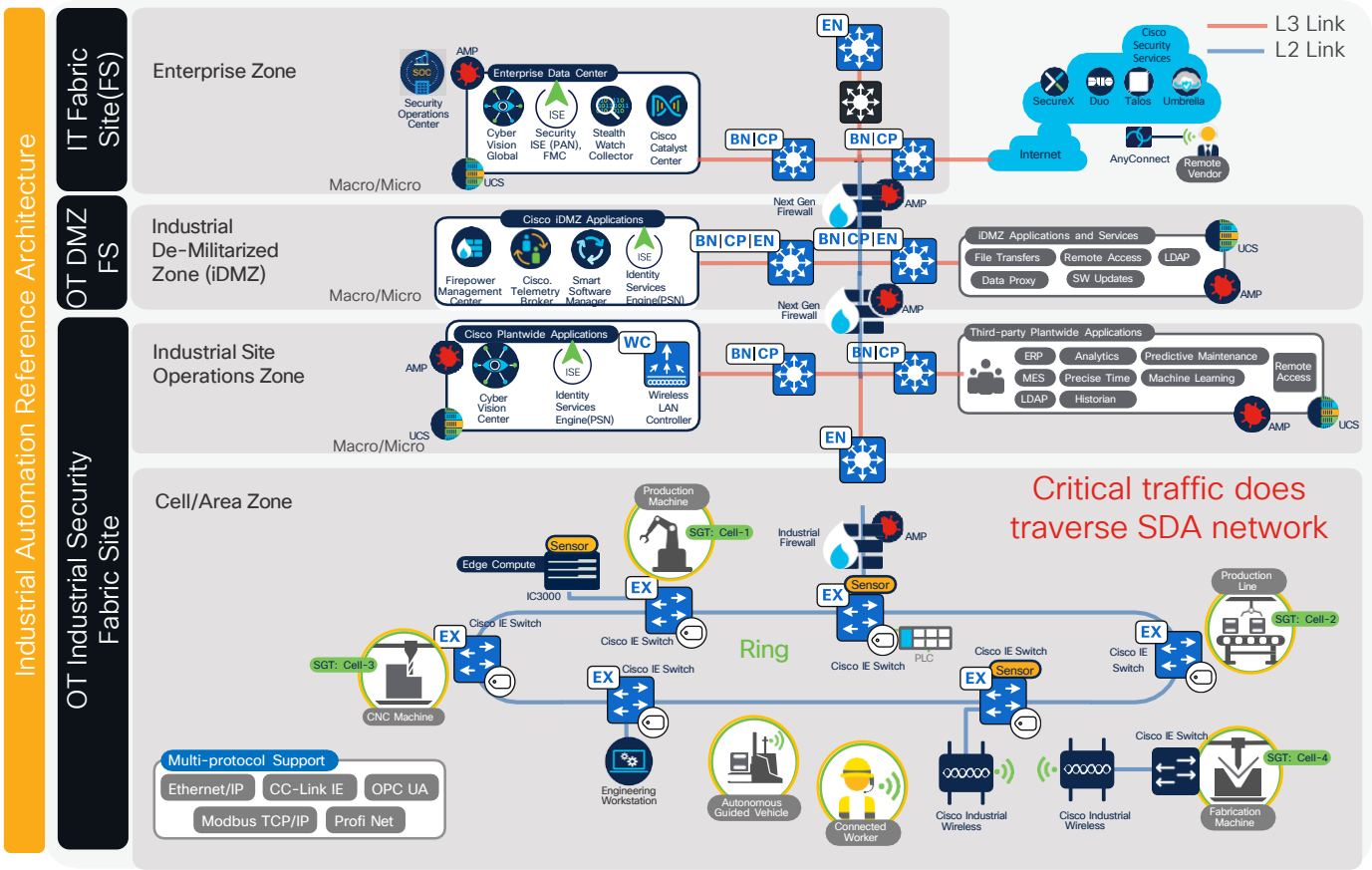
- Cisco Catalyst Center does not provide automation and assurance to the industrial switches.
- Dynamic segmentation policy not recommended in this architecture (More on this later)

Cell area zone network is operated independently by OT

* - Needs Cisco BU Design Review

SD-Access Manufacturing Vertical

Enterprise IT & OT SD-Access Fabric Design – Option 1



SD-Access Manufacturing Vertical
Enterprise IT & OT SD-Access Fabric Design – Option 1

PROS

- No templates required for Industrial switches.
- Rich API support for industrial switch operations.

CONS

- OT SD-Access network and cell area zone managed by same team using a single Catalyst Center cluster
- Only REP or daisy chain topologies are supported
- Cannot mix PEN and EN in same daisy chain because of security policy
- No support for Brownfield switches, must be greenfield
- If templates are required for OT features, they need to be reviewed for conflicts

All network devices on OT network benefit from Catalyst Center Automation

SD-Access Manufacturing Vertical]
EN/PEN vs Traditional L2 Switches

- Minimal modifications via templates are required
- Strong need of automation via APIs
- Same team is responsible for Core/Distribution and Cell area zone switches

- Templates required to support additional features (more on this later)
- Switch needs to be part of the overlay (i.e. visibility of switch in profinet topology)
- Different teams are responsible for Core/Distribution and Cell area zone switches
- Switch is configured by system integrator

SD-Access Manufacturing Vertical
EN/PEN vs L2 Switches

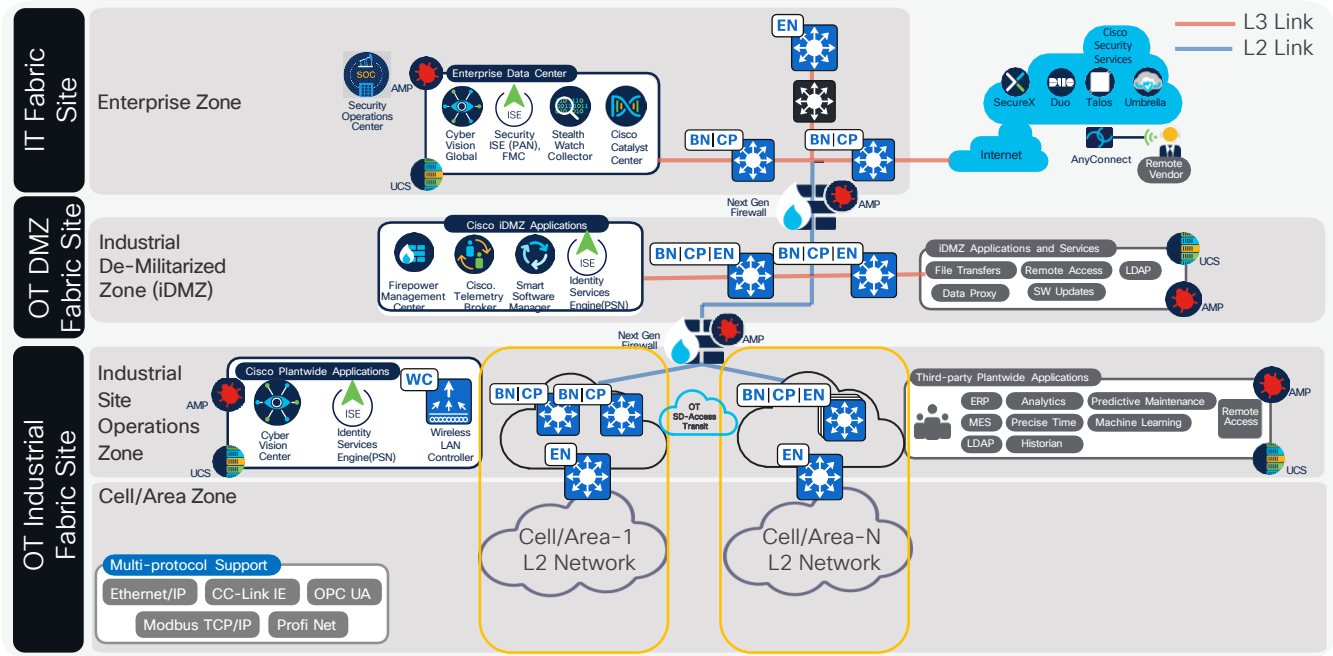
- Minimal modifications via templates are required
- Strong need of automation via APIs
- Same team is responsible for Core/Distribution and Cell area zone switches

- Templates required to support additional features (more on this later)
- Switch needs to be part of the overlay (i.e. visibility of switch in profinet topology)
- Different teams are responsible for Core/Distribution and Cell area zone switches
- Switch is configured by system integrator

* - Needs Cisco BU Design Review

SD-Access Manufacturing Vertical

Enterprise IT & OT SD-Access Fabric Design – Option 2



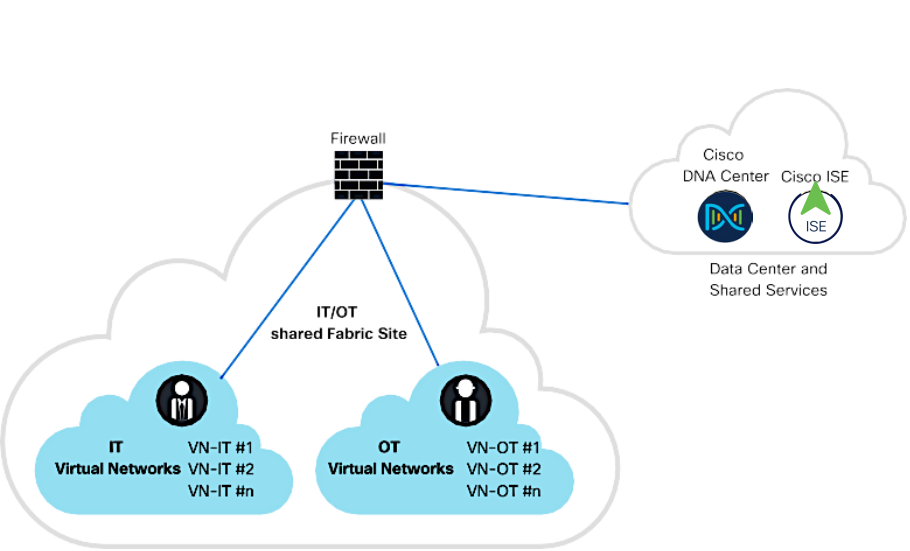
IT Managed

OT Managed

* - Needs Cisco BU Design Review

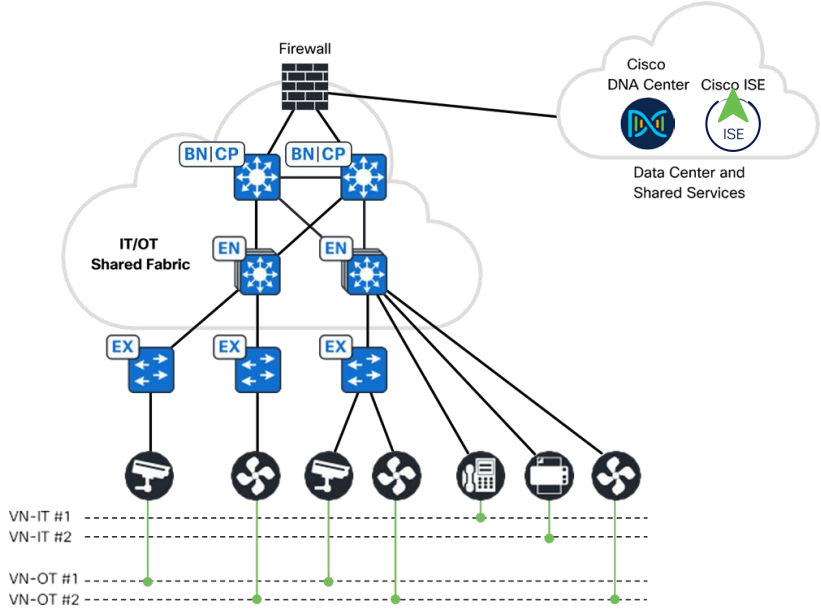
SD-Access Manufacturing Vertical

Shared IT and OT SD-Access Fabric Design



Logical Topology

Shared IT and OT Fabric Site



Physical Topology

IT Managed

OT Managed

SD-Access Manufacturing Vertical
Dedicated OT vs Shared IT/OT

Dedicated OT

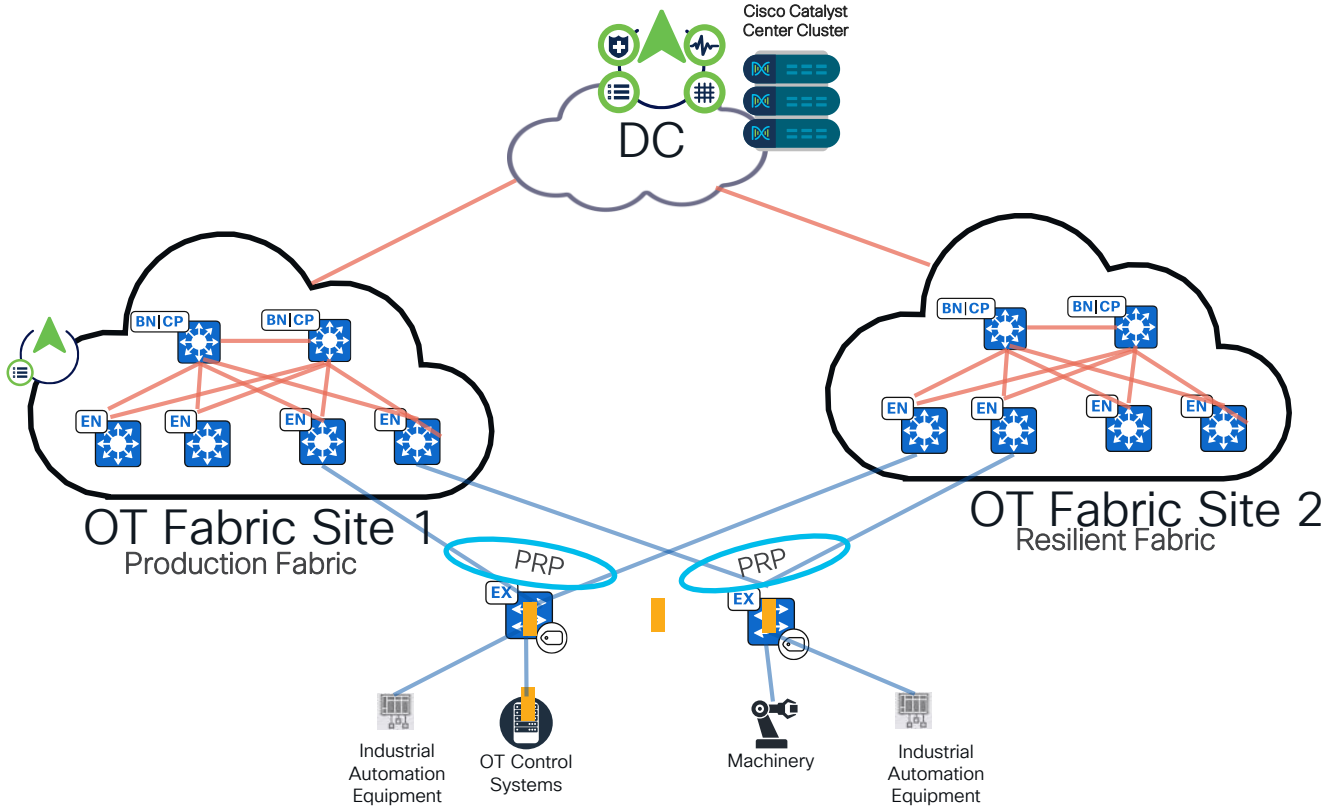
- Isolation from IT Configuration Changes
- Custom Macro and Micro Segmentation policies
- Tailored Quality of Services
- Scalability for Large Industrial Deployments

Shared IT/OT

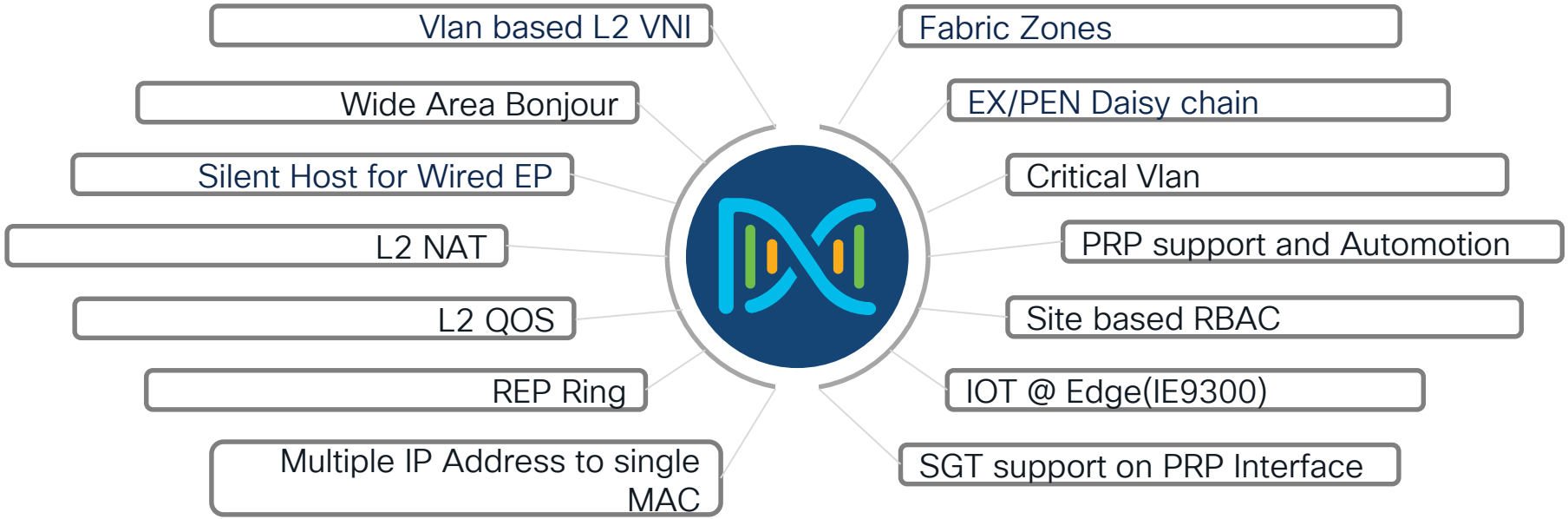
- Cost-Efficient Infrastructure
- Simplified Administration

SD-Access Manufacturing Vertical

Zero-Loss Redundancy: Dual Fabric High Level Design with PRP



Operation Technology
Specific Features



New Feature
Enhanced

Catalyst Leadership in Enterprise Networks

A Platform based Approach

Catalyst Center and Meraki Dashboard

28M Network Devices Managed

50% Y/Y

19M APs | 6M Switches | 2.5M Routers | 830M Clients

13M
Devices on Catalyst Center

15.3M
Devices on Meraki Dashboard

Catalyst 9000 Family

100,000+ Customers, Millions of Switches

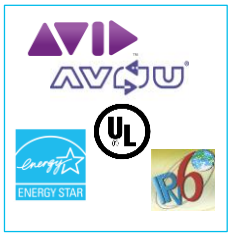
"Catalyst 9K continues to be the fastest ramping product in the company's history"

- Chuck Robbins, CEO Cisco Systems

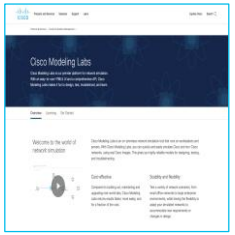
Secure Networking	Digital Experience	Operational Simplicity
Common Policy	Campus Automation	Cloud Managed Catalyst
Secure Equipment Access	AI Endpoint Analytics	Infrastructure as a Code
SD-Access (LISP & EVPN)	Digital Experience ThousandEyes	S3 & CloudWatch Integration
High-speed Encryption	AI Ops & Assurance	Visibility, Control & Rollback

Cisco Validated Profiles (CVP)

Industry Validated Reports



Industry Certifications



Cisco Modeling Labs

cisco Live!

Global Partner Solution Advisors

- *NEW* - Fully Virtualized, SD-Access Secure Campus Lab

Virtualized SD-Access Lab

- Fully Customizable Topology with virtualized 9kv's and 8kv's
- Access on dCloud or build on your existing Data Center
- Fraction of the cost
- GPSA mentored lab buildout support available!

CTF Mission

- Experience the SD-Access Virtual Lab at Capture the Flag in The World of Solutions
- Use Cases – Fabric Sites and Virtual Network Provisioning, Fusion Automation, Extranet, Micro Segmentation, and more!

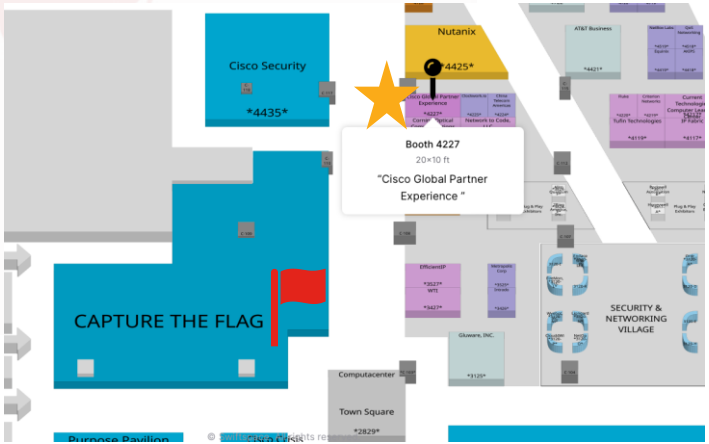
Contact

- GPSA is your source for no-cost, partner enabment and practice building!
- Visit the Global Partner Experience booth (4227) across from Capture the Flag, for more information.

Virtual SD-Access Lab on dCloud

GPSA Sales Connect Page

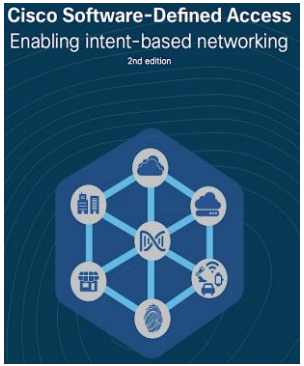
CTF at Cisco Live
Check out Secure Campus Section



Cisco SD-Access LISP Fabric Collaterals

Cisco Software-Defined Access for Industry Verticals

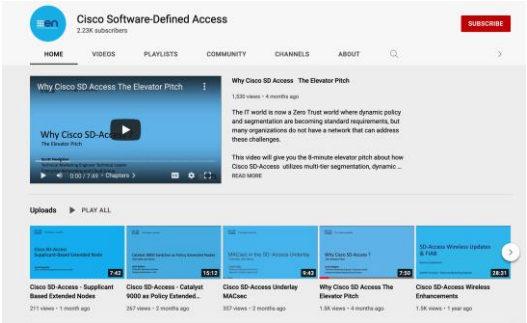
Cisco Software-Defined Access
Enabling intent-based networking



Cisco Solution Validated Profiles (CVPs)

- Cisco Large Enterprise and Government Profile
- Healthcare Vertical
- Financial Vertical
- Healthcare Vertical
- Manufacturing Vertical
- Retail Vertical
- University Vertical

Cisco SD-Access YouTube Link



Multiple Cisco DNA Center to ISE

Cisco SD-Access Design Tool

EN&C Validated Designs

The Latest SD-Access Guides

Complete Your Session Evaluations

Complete a minimum of 4 session surveys and the Overall Event Survey to be entered in a drawing to **win 1 of 5 full conference passes** to Cisco Live 2025.

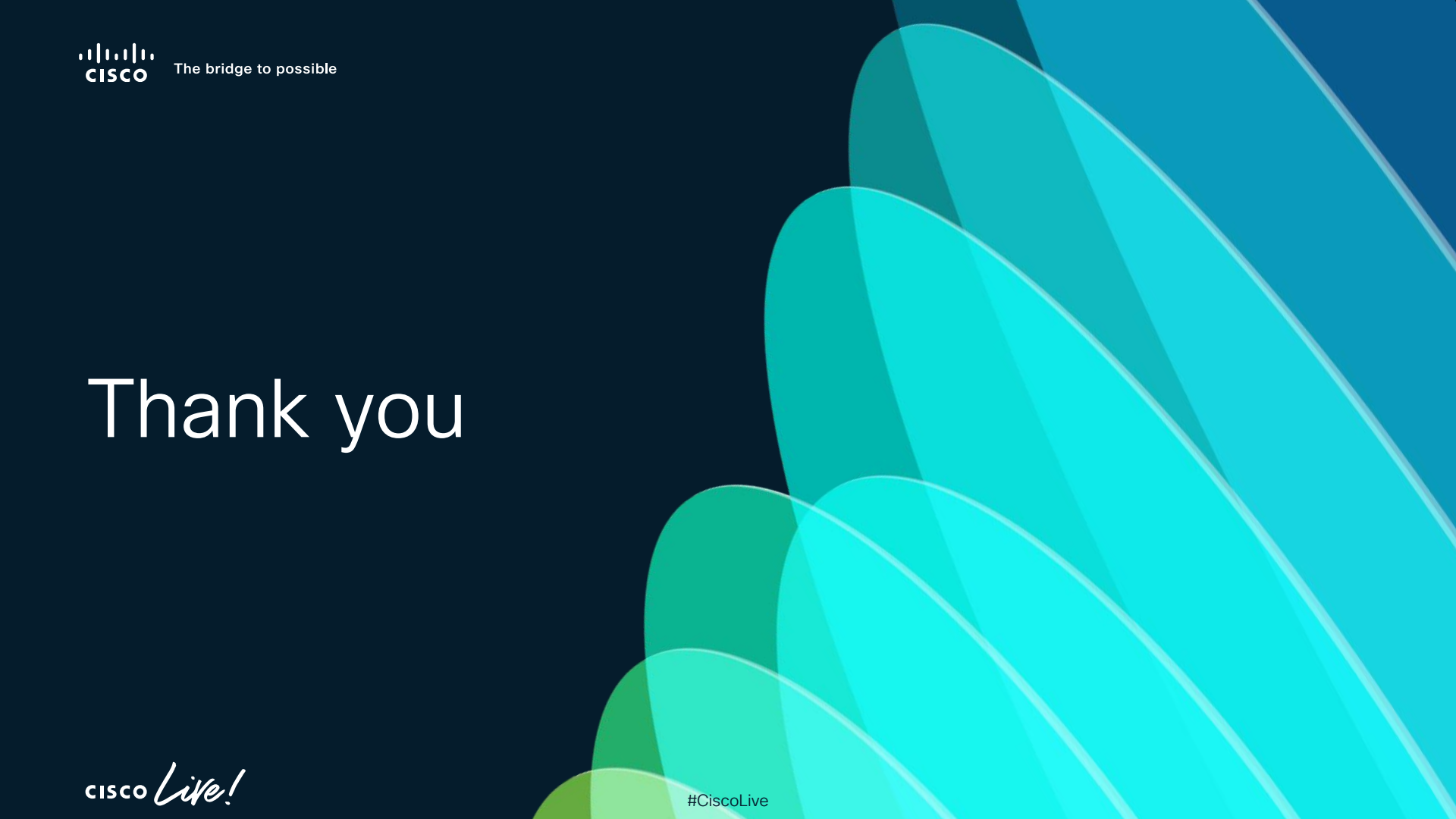
Earn 100 points per survey completed and compete on the Cisco Live Challenge leaderboard.

Level up and earn **exclusive prizes!**

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

Continue your education

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


The bridge to possible
Thank you
cisco Live!
#CiscoLive