
cisco Live!
Let's go

The bridge to possible

Let Cisco Catalyst Center be your guide to a Zero-Trust Workplace

Rojda Cicek, Solutions Engineer, Enterprise Networks
Felix Meixner, Solutions Engineer, Enterprise Networks

We guide your journey to a zero-trust workplace

Felix Meixner

Rojda Cicek

The path to zero-trust is full of distractions

Zero Trust means different things to different people

It’s segmentation

It’s ZTNA

It’s endpoint security

It’s firewall

It’s identity

Security adds complexity to the network

Modern business demands make security ON the network challenging

More interconnected than ever

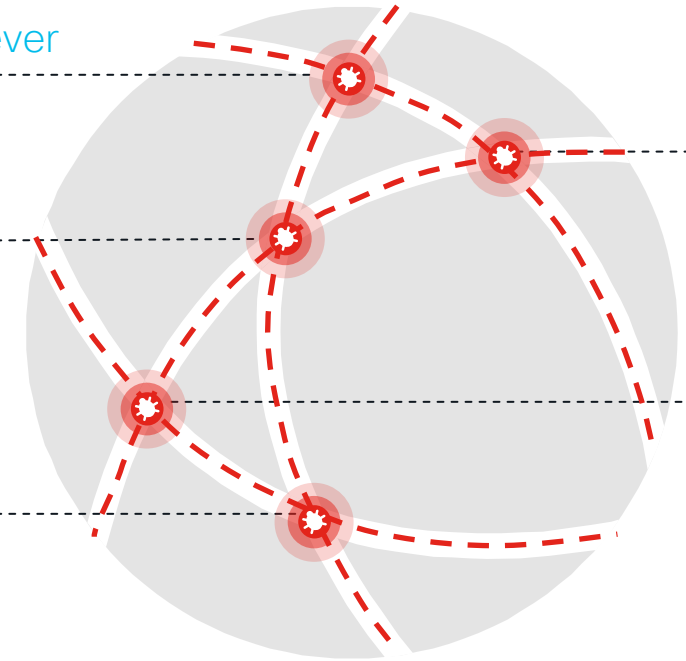
Expanded attack surface

Continuous operations

Persistent threats

Workers connecting everywhere

Loss of access control



Multi-cloud reality

Gaps in visibility

Rapid innovation

Sophisticated threats and attacks

Security needs integration IN, not ON the network

Converging Network and Security to meet modern business demands

Continuous Visibility

Utilize continuous real-time insights to identify and resolve events faster

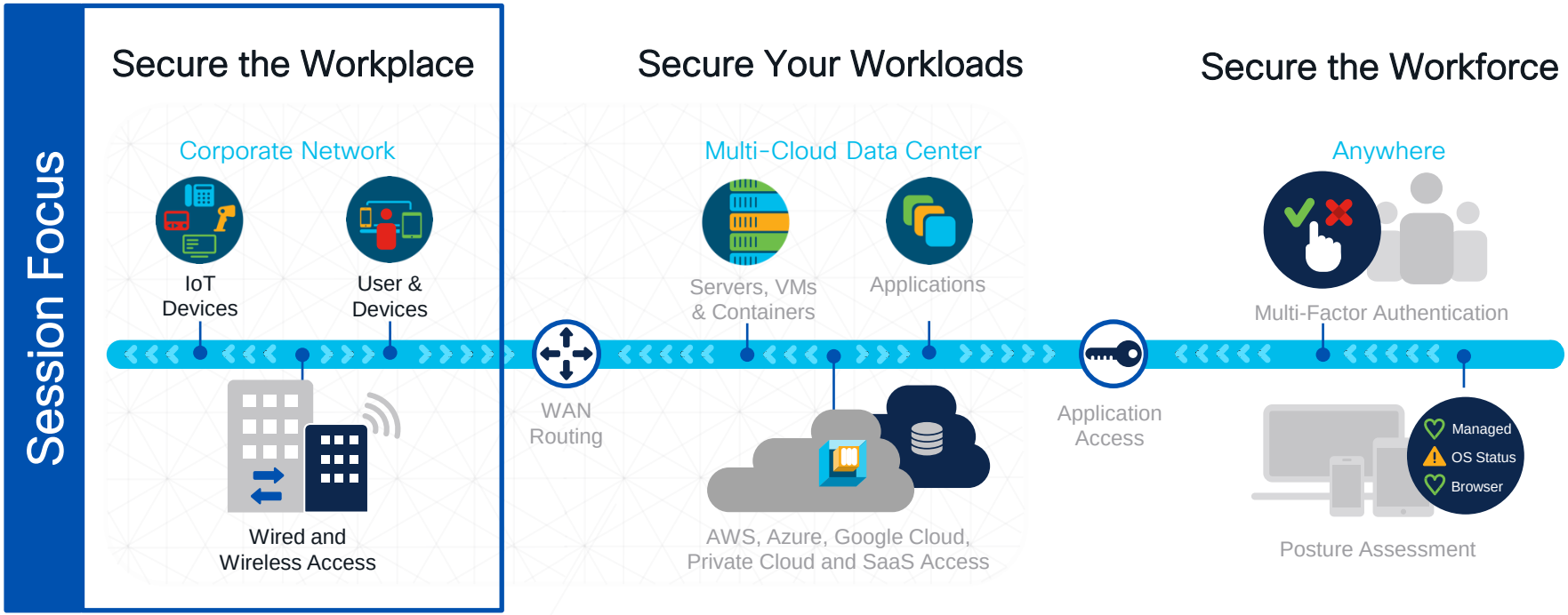
Identify who and what is on the network

Understand how they're communicating

Determine risk profile and compliance

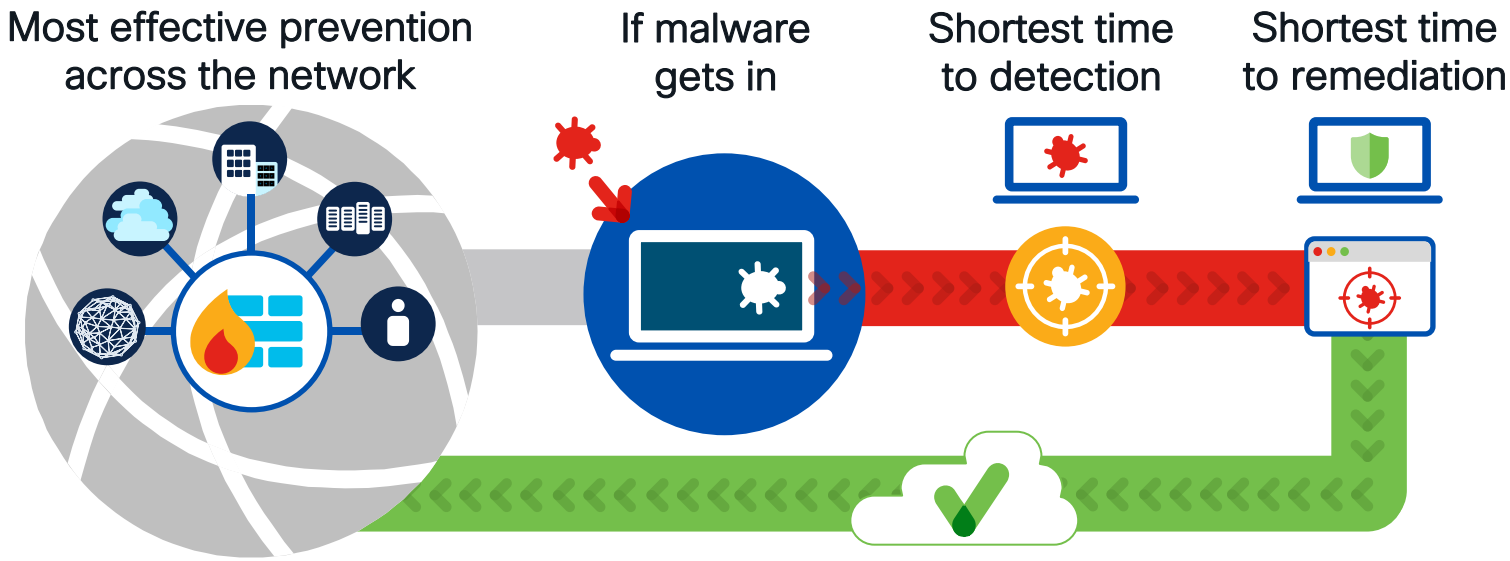
Zero-Trust Network Access

Use segmentation and verification to proactively stop breaches



Constant Protection

Stop chasing threats – identify risks and vulnerabilities through automation



Session Overview and Objectives

This session covers

- ✓ Zero-trust for workplace security with Catalyst Center
- ✓ Journey to endpoint visibility, network segmentation & trust monitoring

This session does not cover

- ✘ Zero-trust for workloads or workforce
- ✘ Details of related security products, services and integrations
- ✘ Catalyst Center use-cases not related to security

Dive deeper into other topics with this curated collection of Learning Maps

https://www.ciscolive.com/emea/learn/technical-education/learning-maps.html

Webex App

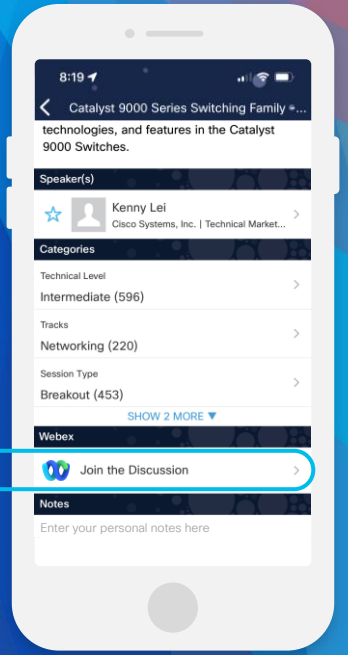
Questions?

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

How

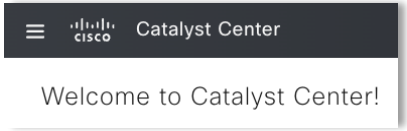
1. Find this session in the Cisco Events Mobile App
2. Click “Join the Discussion”
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until February 23, 2024.



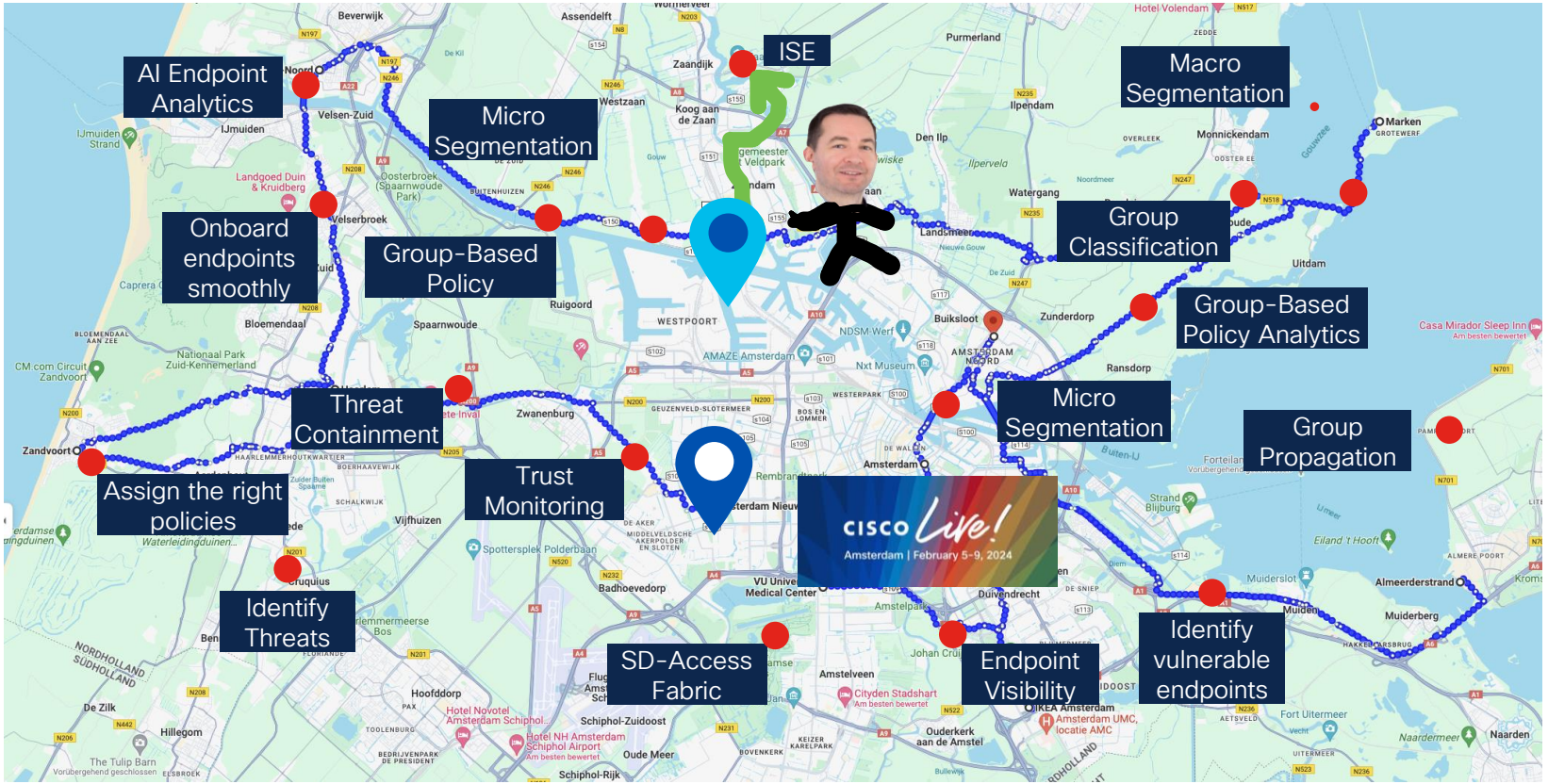
https://ciscolive.ciscoevents.com/ciscolivebot/#BRKOPS-2683

Let’s pack the bags for our journey



Catalyst Center	• Release 2.3.7 • Cat9000 switches in managed state	operational
Catalyst 9000	• Release 17.12 • DNA Advantage License	
ISE	• Release 3.2 • ISE Premier License	

Ready to enter the trail and start our journey?



Ready to enter the trail and start our journey?

Let's use our helpers!

Catalyst Center guides your journey to zero-trust

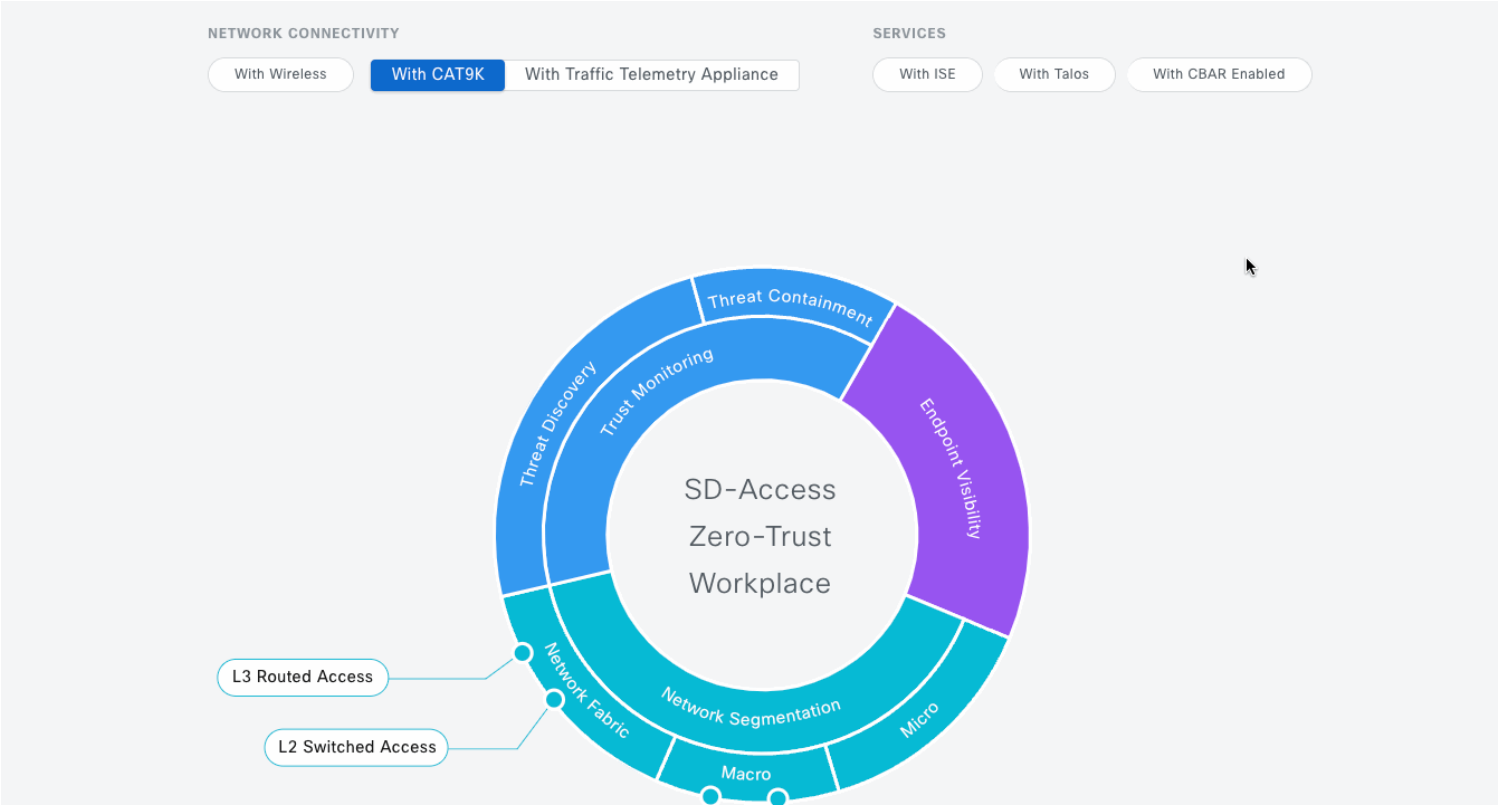
Zero-Trust Journey Map

Endpoint Visibility

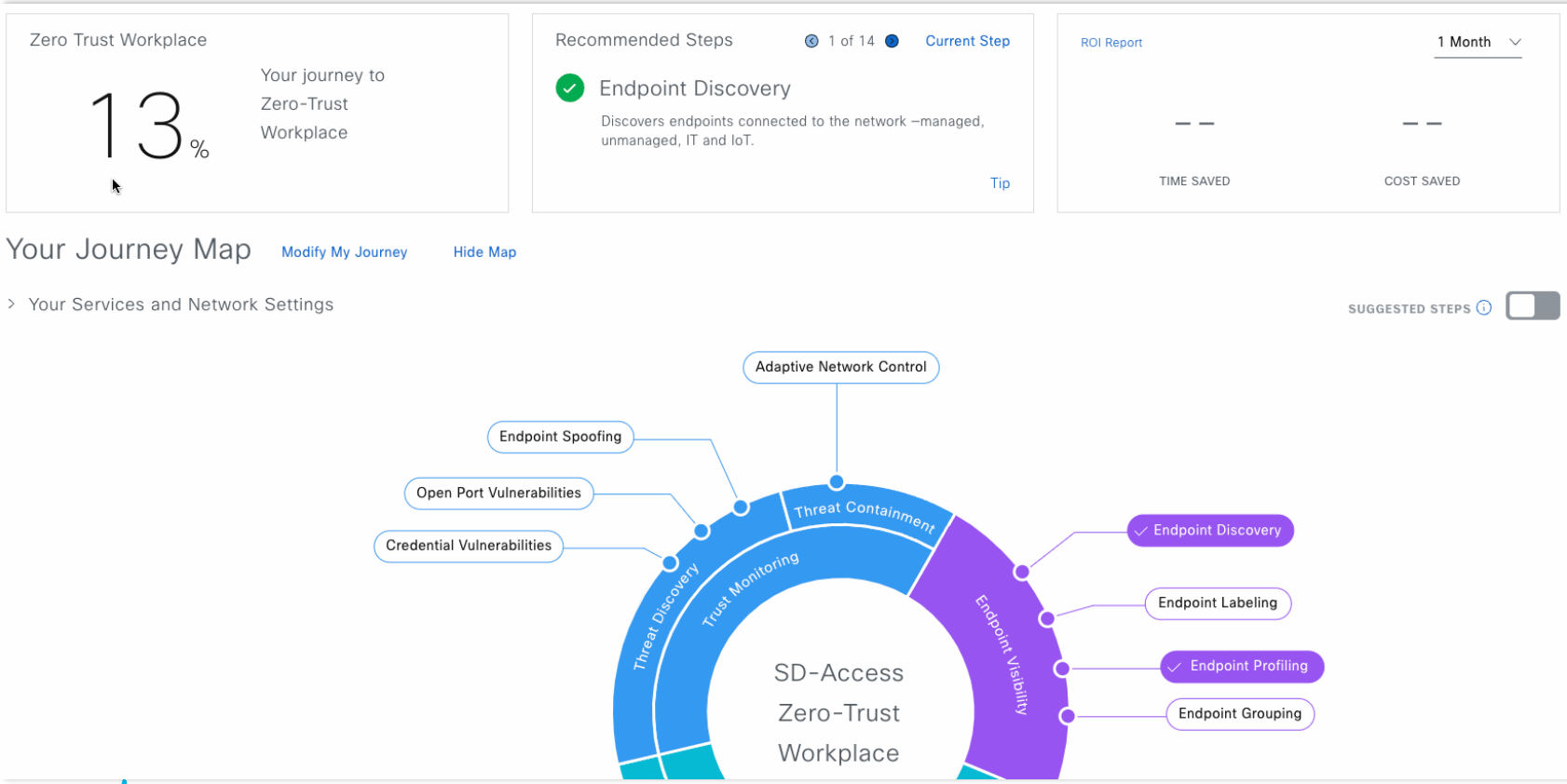
Network Segmentation

Trust Monitoring

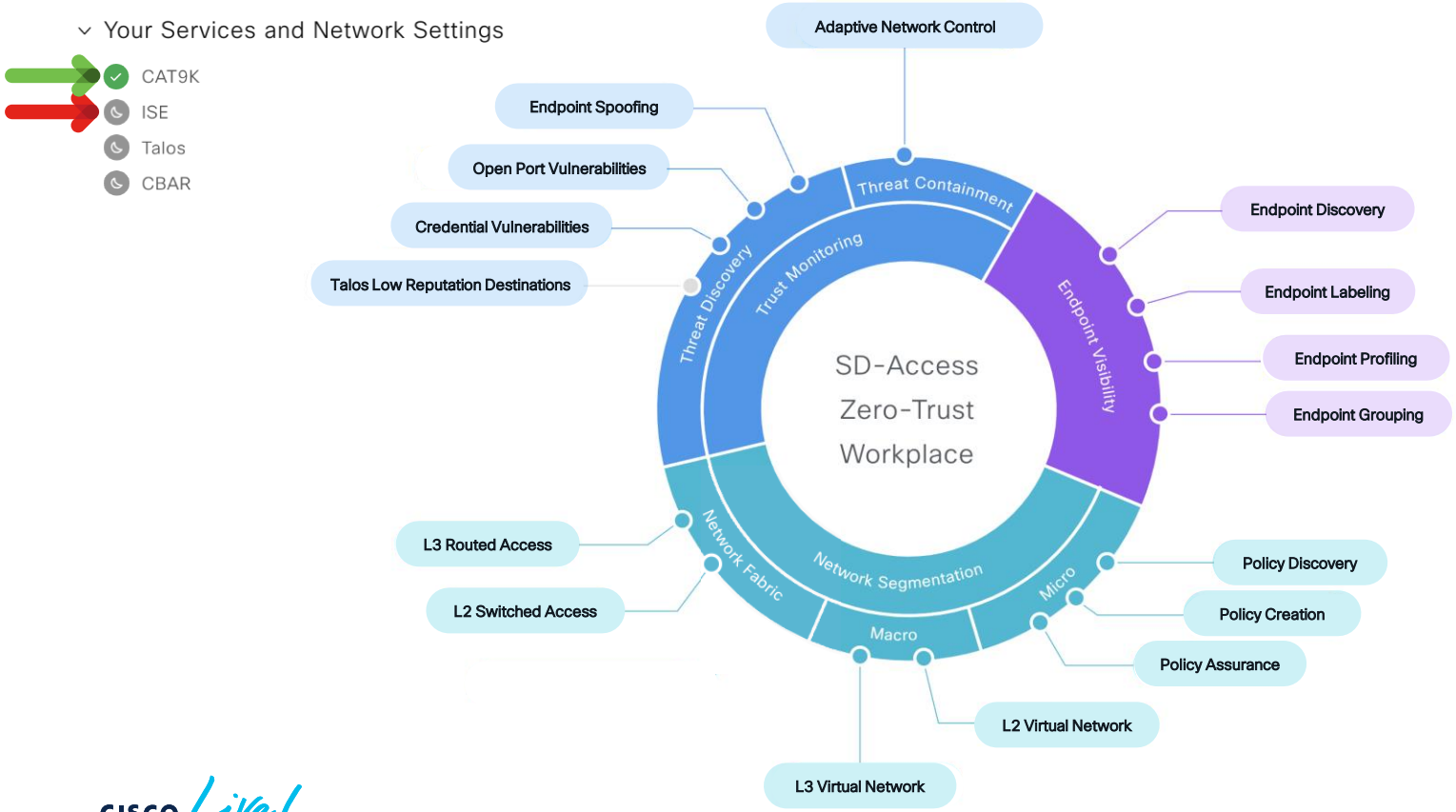
Select the components of your journey



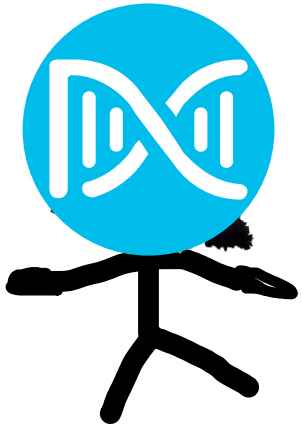
Explore the status of your journey



Start your journey to zero-trust workplace



Everyone needs a best friend to share things



CISCO

The bridge to possible

context

trust

network devices

interests

policies

secrets

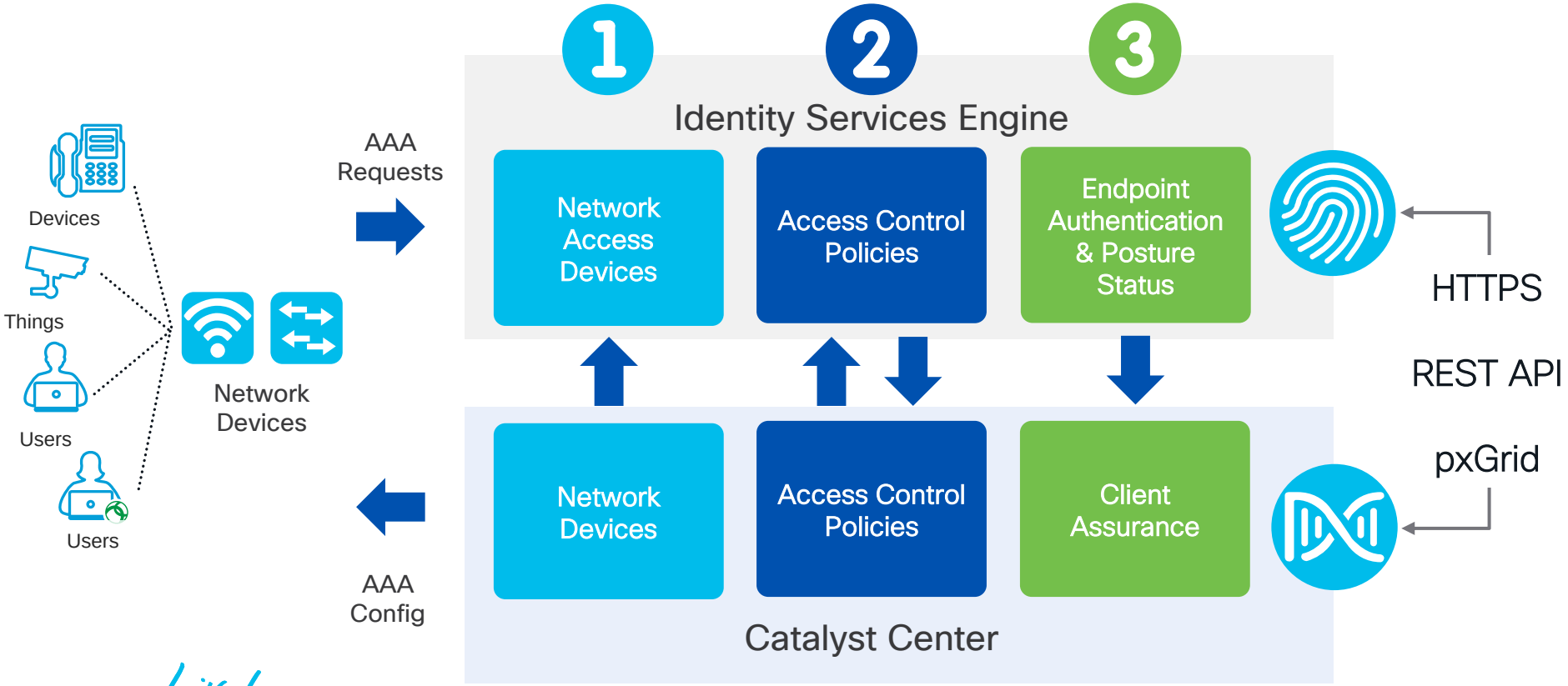
endpoint visibility

workload

status

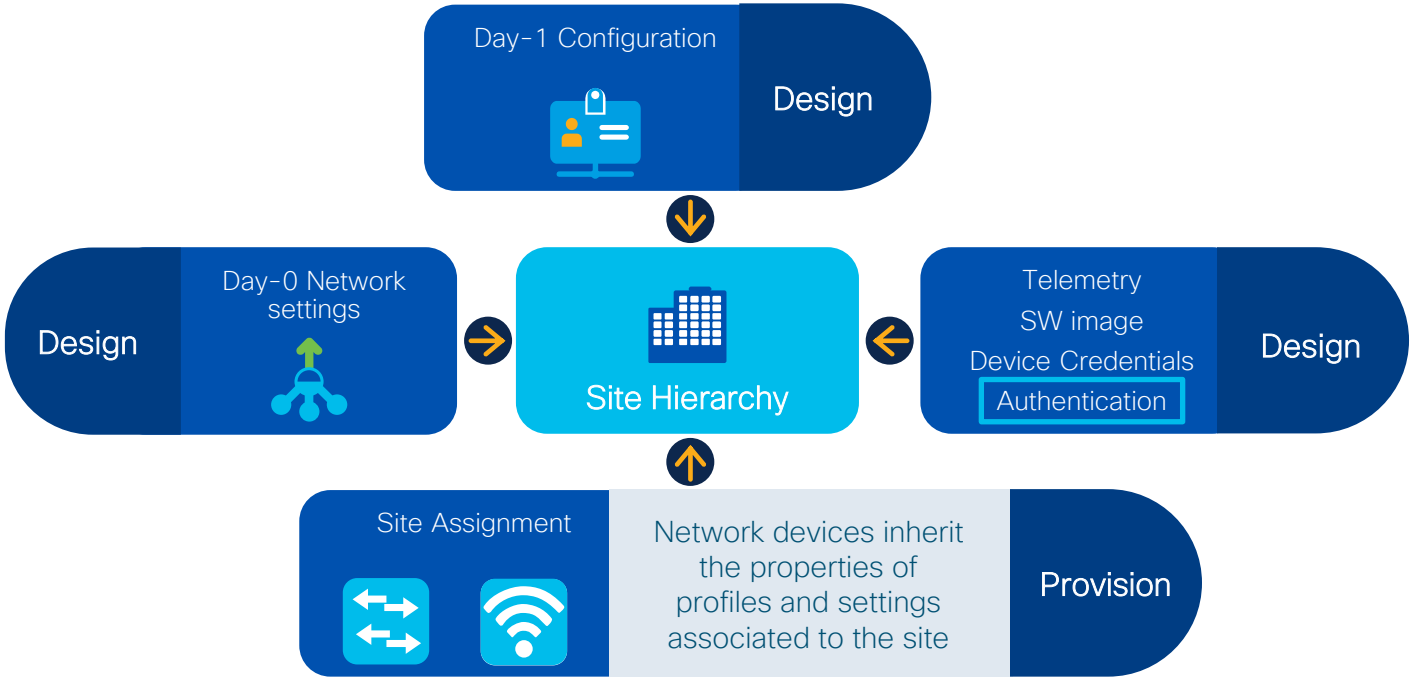
Best friends share workload

Cisco ISE has three main use cases with Catalyst Center



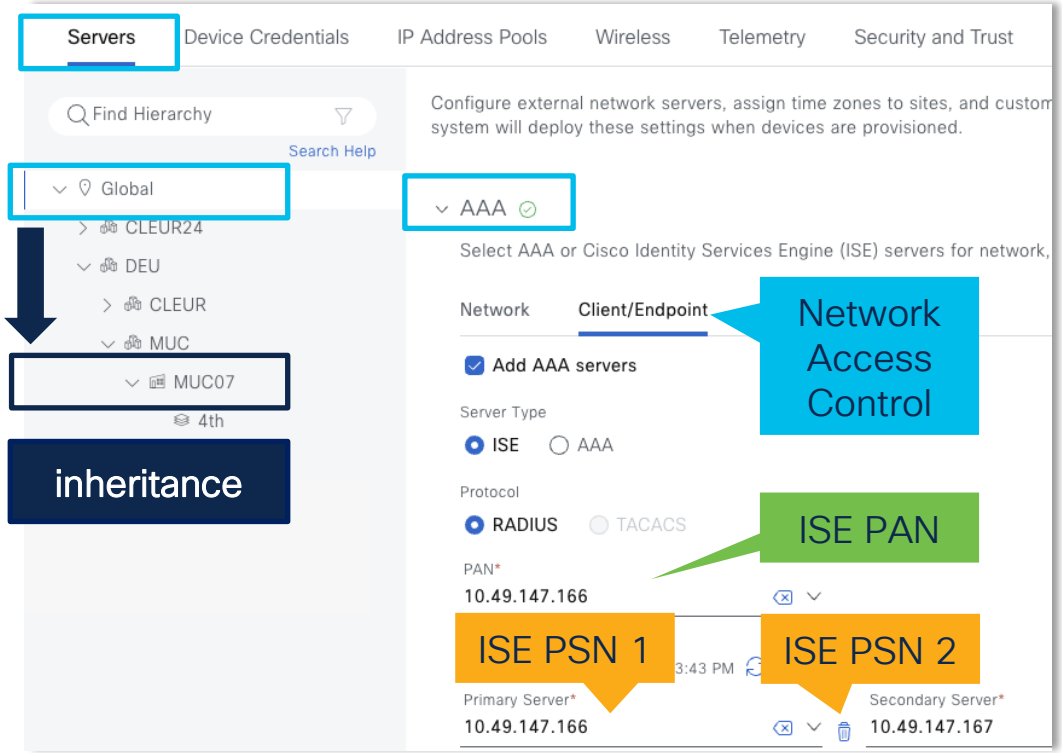
Simplified Configuration Management

Catalyst Center uses an Intent Based deployment model

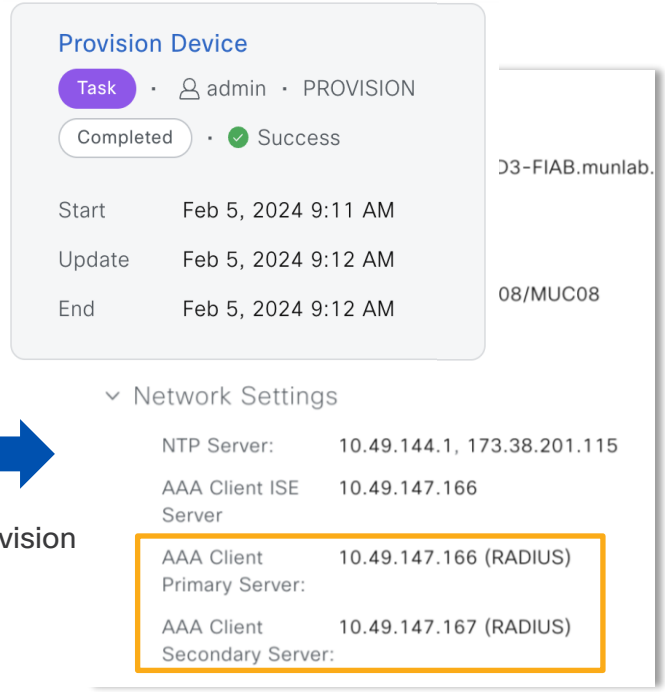


Catalyst Center automates your AAA Settings

Intent Based AAA Server Configuration

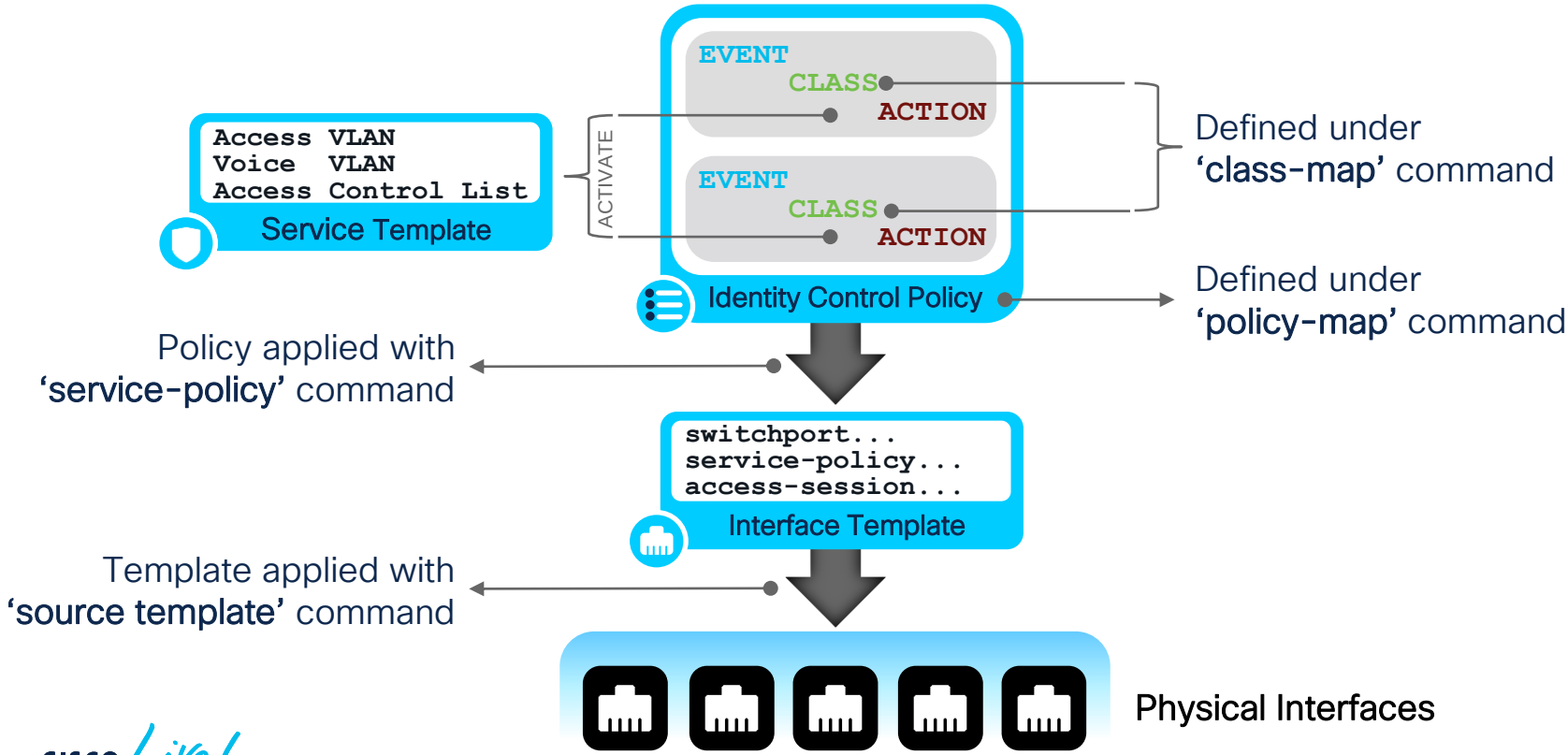


Provision



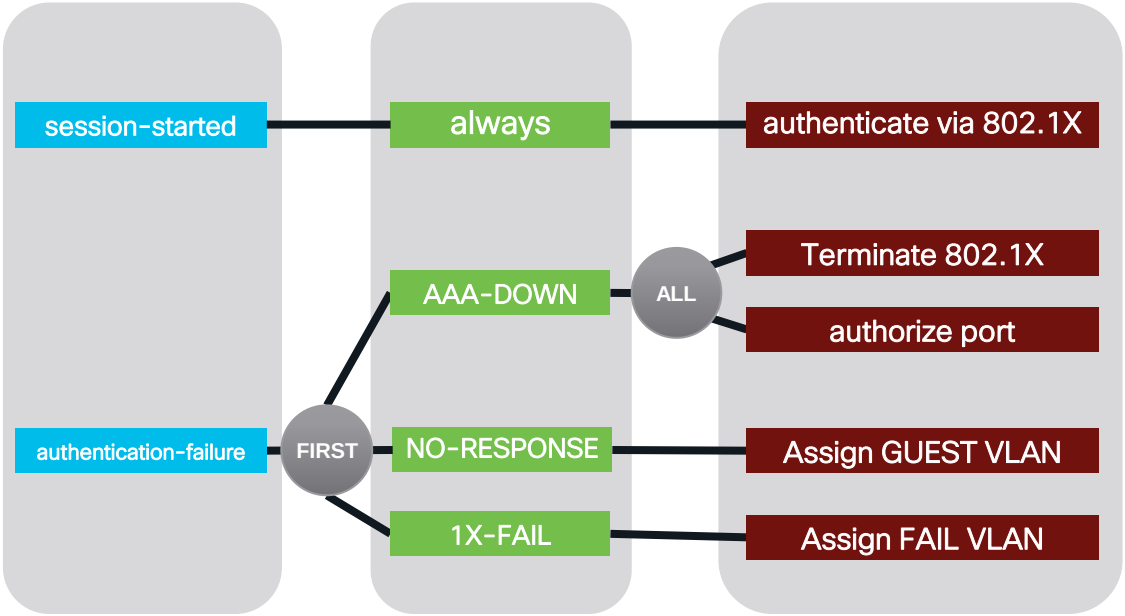
Identity Control Policy links the elements

Cisco Identity Based Networking Solution (IBNS) 2.0



Identity Control Policy links the elements

Cisco Identity Based Networking Solution (IBNS) 2.0



Identity Control Policy

```
policy-map type control subscriber POLICY-A

event session-started match-all
  10 class always do-until-failure
   10 authenticate using dot1x

event authentication-failure match-first
  10 class AAA-DOWN do-all
   10 terminate dot1x
   20 authorize
  20 class DOT1X_NO_RESP do-until-failure
   10 activate service-template GUEST_VLAN
  30 class 1X-FAIL do-all
   10 activate service-template FAIL_VLAN
```

Is this really the easiest way to do it?

more complex than before?

lots of command line!

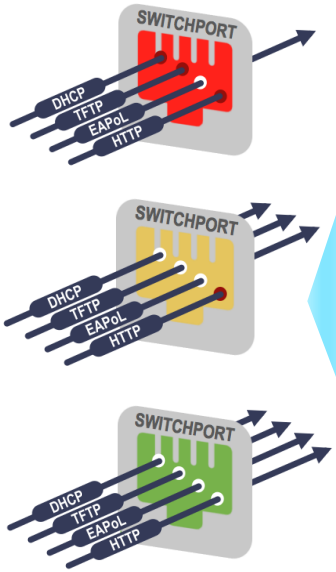
do I need scripting knowledge?

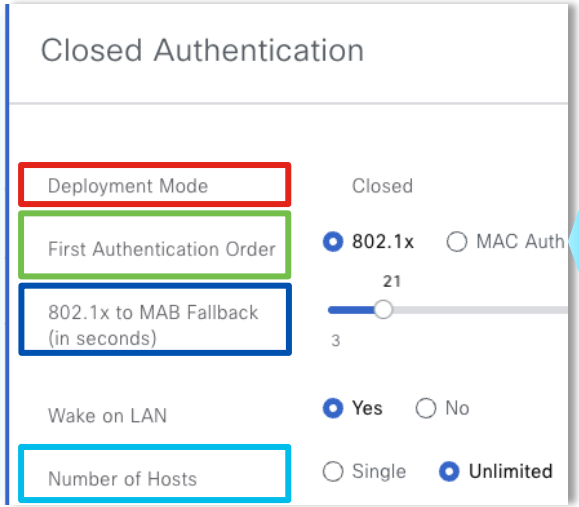
potential for typos

platform and code dependencies

The easy way: SDA Authentication Templates

Templates for each phase of policy rollout






```
template DefaultWiredDot1xClosedAuth
 dot1x pae authenticator
 dot1x timeout supp-timeout 7
 dot1x max-req 3
 switchport mode access
 switchport voice vlan 2046
 mab
 access-session closed
 access-session port-control auto
 access-session host-mode multi-auth
 authentication periodic
 authentication timer reauthenticate server
 service-policy type control subscriber
PMAP_DefaultWiredDot1xClosedAuth_1X_MAB
```

Closed	no access before authentication
Low-Impact	limited access before authentication
Open	network access always authorized

Visibility and Control

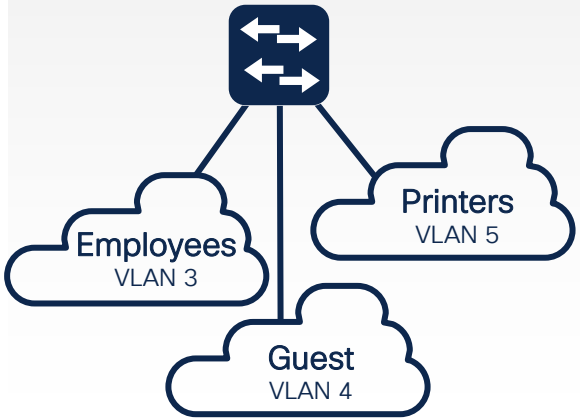
Visibility only

What are our authorization enforcement options?

Beyond RADIUS Access-Accept / Access-Reject

VLANs

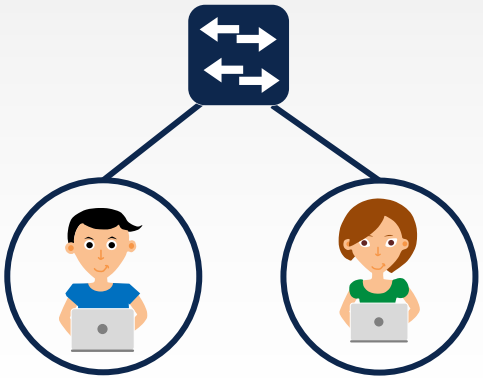
Dynamic VLAN Assignment



per port / per domain / per MAC

Access-Lists

Downloadable ACLs




```
permit ip any any
```

```
deny ip host
permit ip any any
```

Security Group Tags

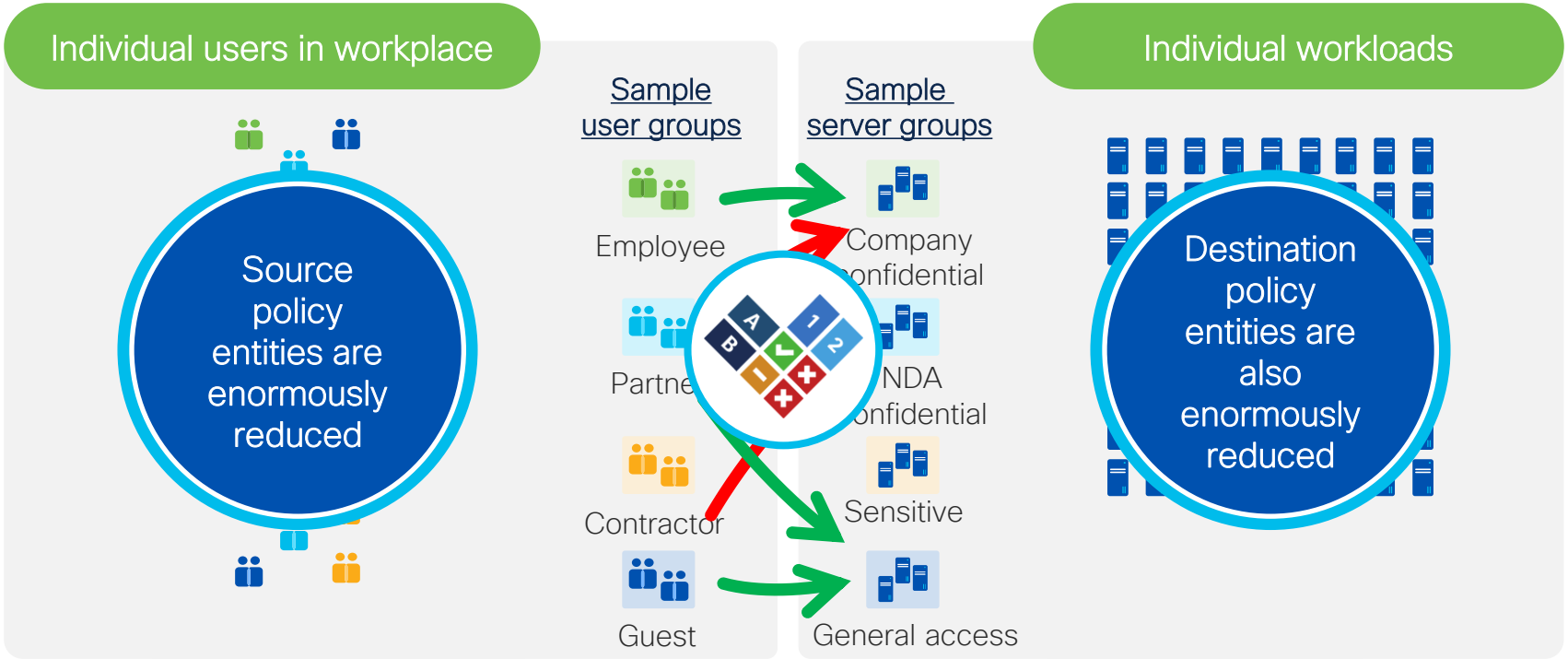
Group-Based Policy

16-bit SGT assignment and
SGT based Access Control

Topology independent

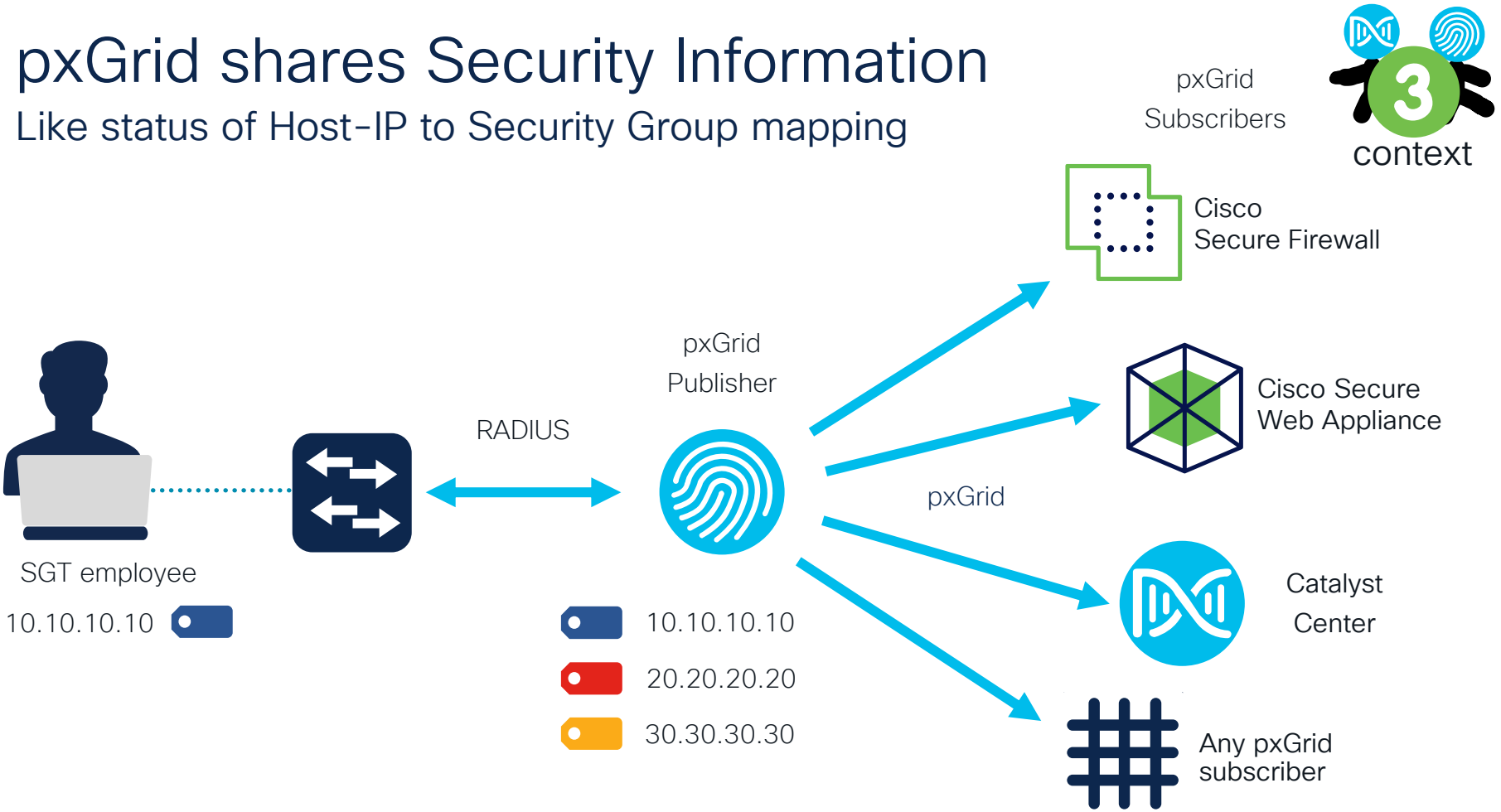
The Value of Group-Based Policies (GBP)

Enhanced simplicity for better enforcement and management



pxGrid shares Security Information

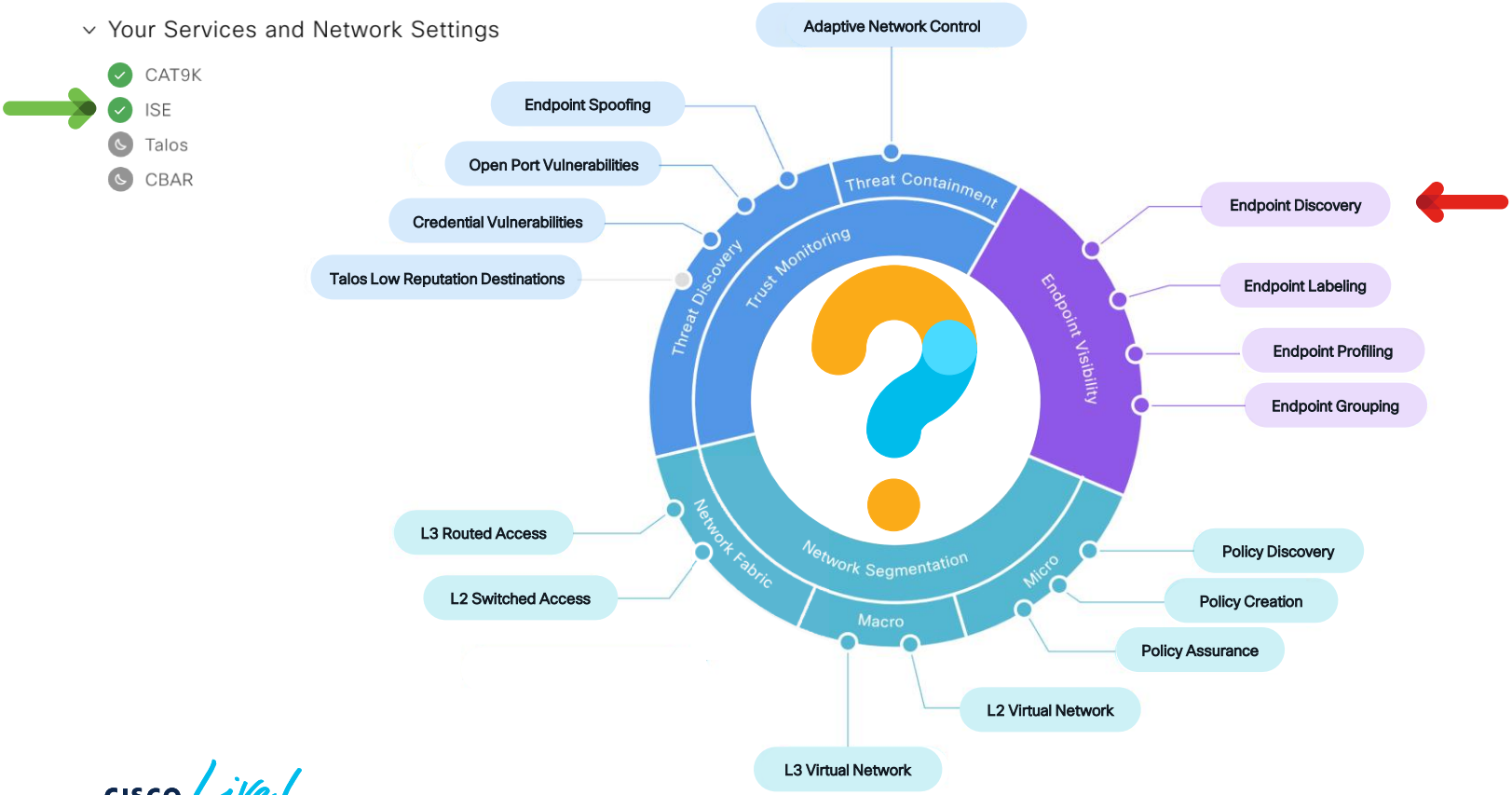
Like status of Host-IP to Security Group mapping



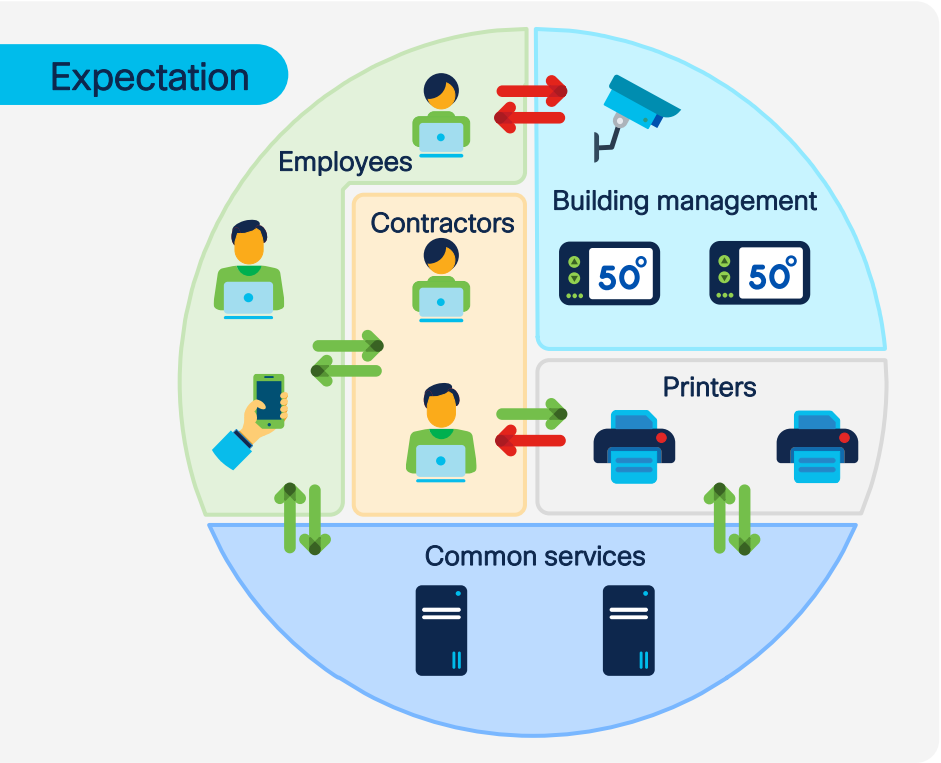
1. Integration of ISE
2. Automation of AAA Config
3. Identity Control Policy
4. Group Based Access Control
5. Context Sharing

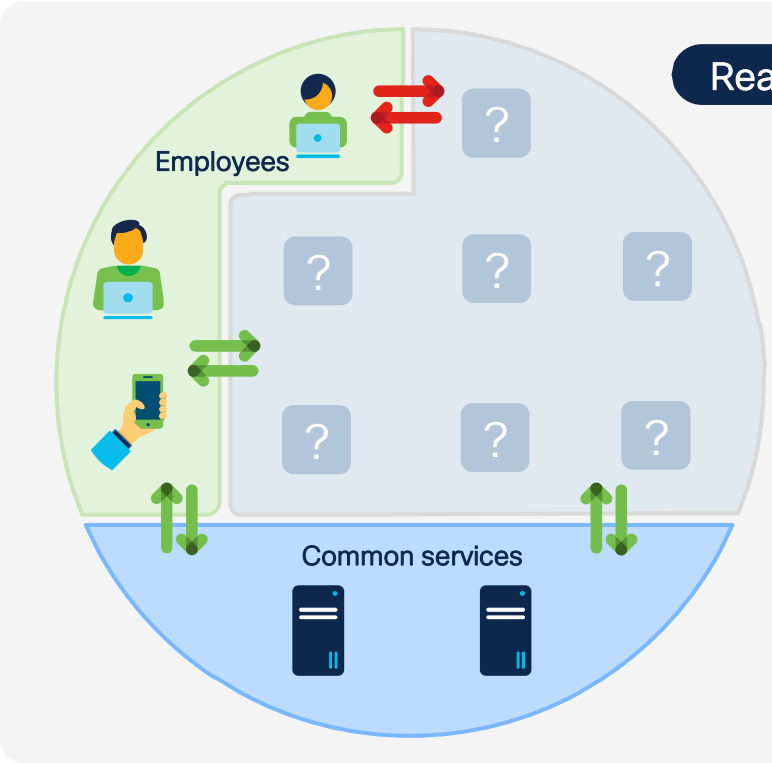
1. Integration of ISE — ✓ Connected ISE
2. Automation of AAA Config — ✓ Pushed AAA
3. Identity Control Policy — ✓ Controlled access
4. Group Based Access Control — ✓ Grouped endpoints
5. Context Sharing — ✓ Shared context

We integrated ISE into Catalyst Center

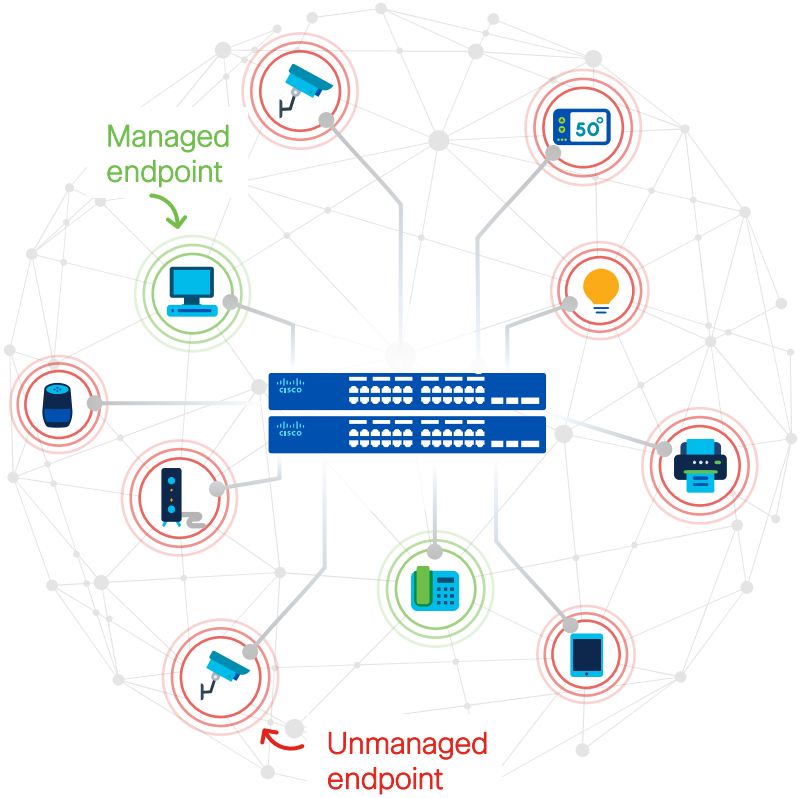


Do we really know all endpoints in our network?





What's really happening in the workplace?



1:5

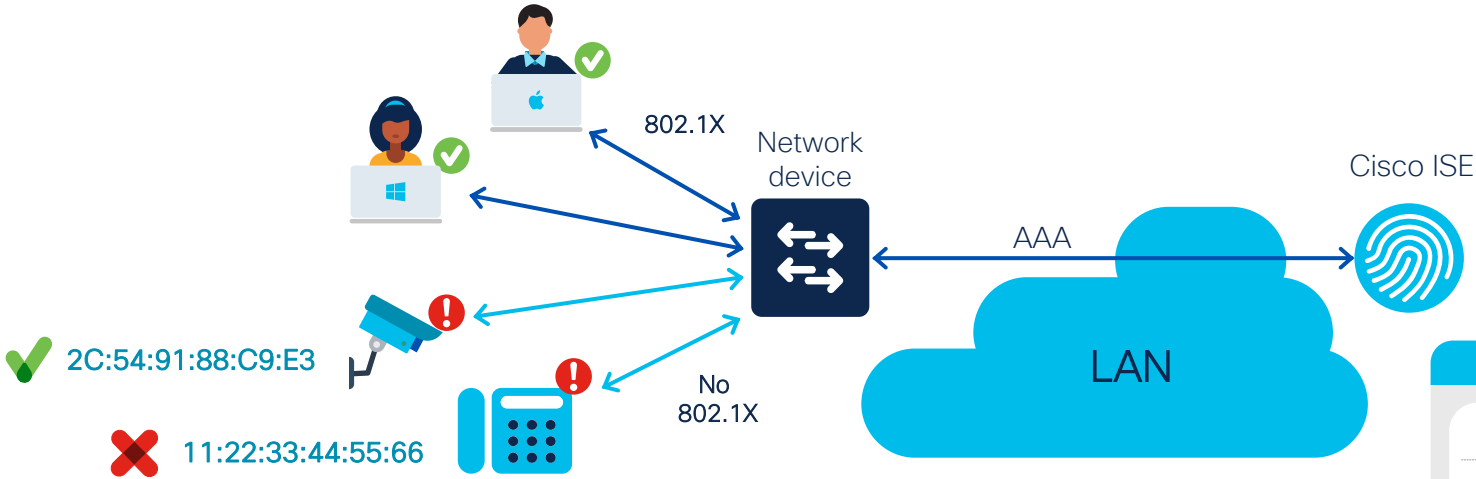
Unmanaged device proliferation.
1:5 managed to **unmanaged endpoint ratio**

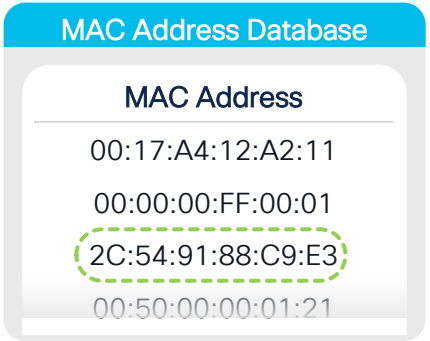
Unmanaged endpoints are difficult to patch and **most vulnerable to cyber attacks.**

Secure authentication mechanisms unusable on unmanaged endpoints

Open, unsegmented networks with IOT devices put organizations at risk

Authentication of unmanaged assets is insecure



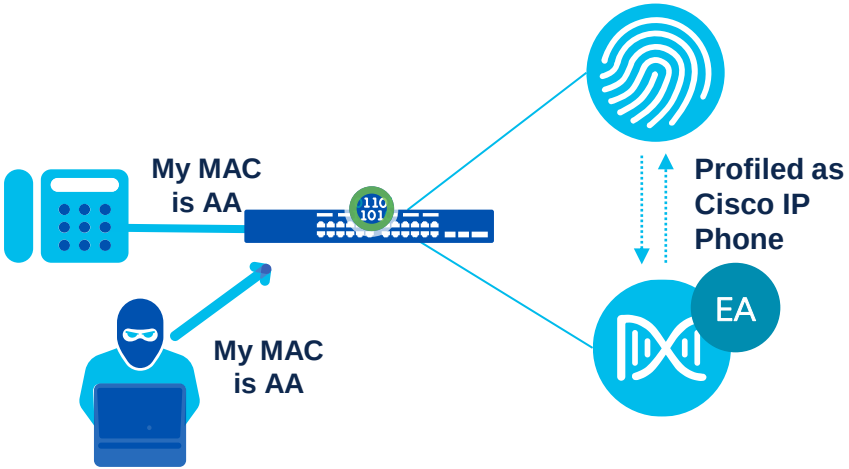


- Endpoints without supplicant will fail 802.1X authentication
- They fall back to MAC Authentication Bypass (MAB)
- MAB requires a MAC address database
- Unknown MACs use default authorization policy (catch-all)

Problem to solve: Impersonation Attacks

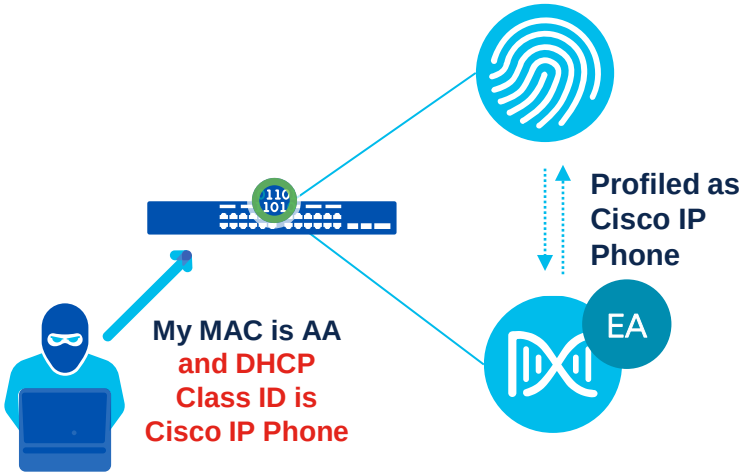
MAC address must not be the only source of truth

MAC Spoofing



Impersonate the MAC address of another authorized endpoint in order to gain the same privileges

Attribute Spoofing

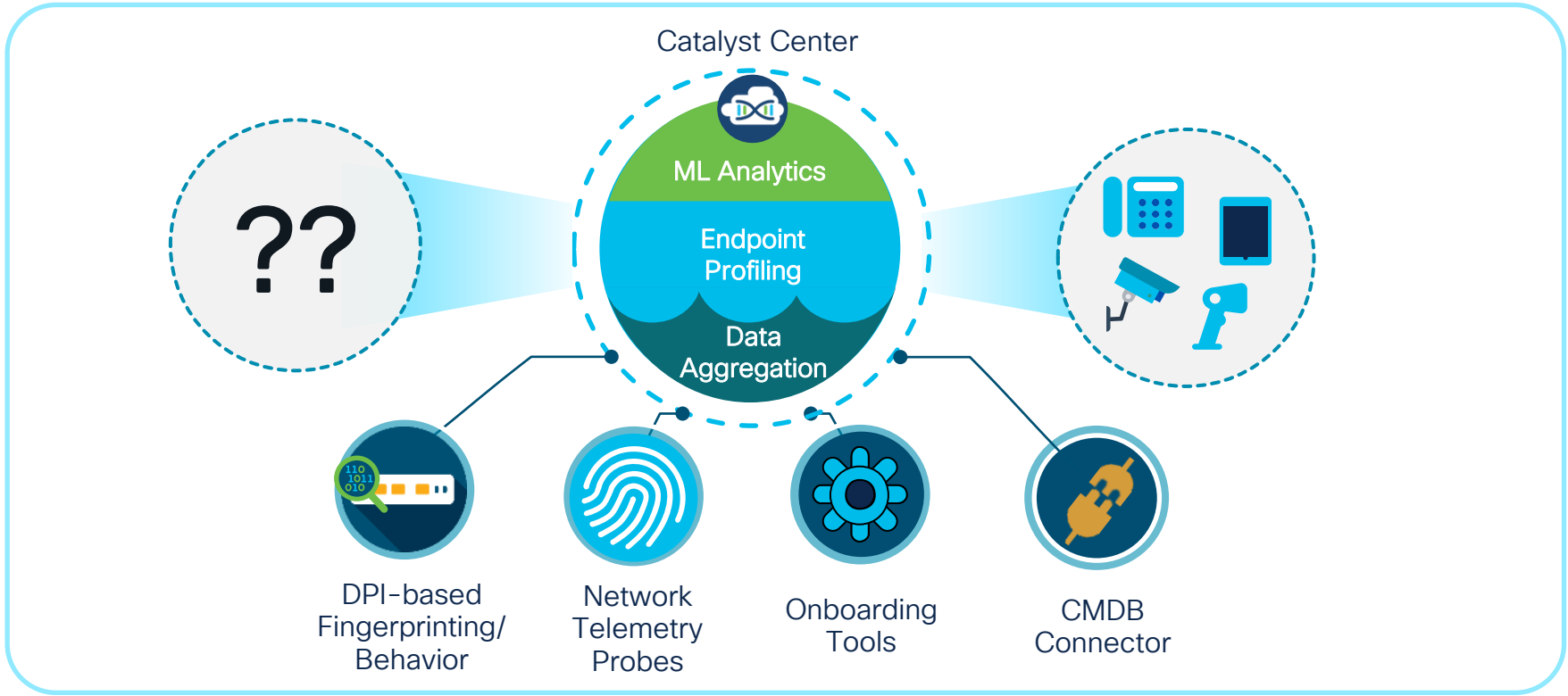


Impersonate class/type of the device in order to get privileged network access

AI Endpoint Analytics in Catalyst Center

Rapidly reducing the unknowns by aggregating data from different sources

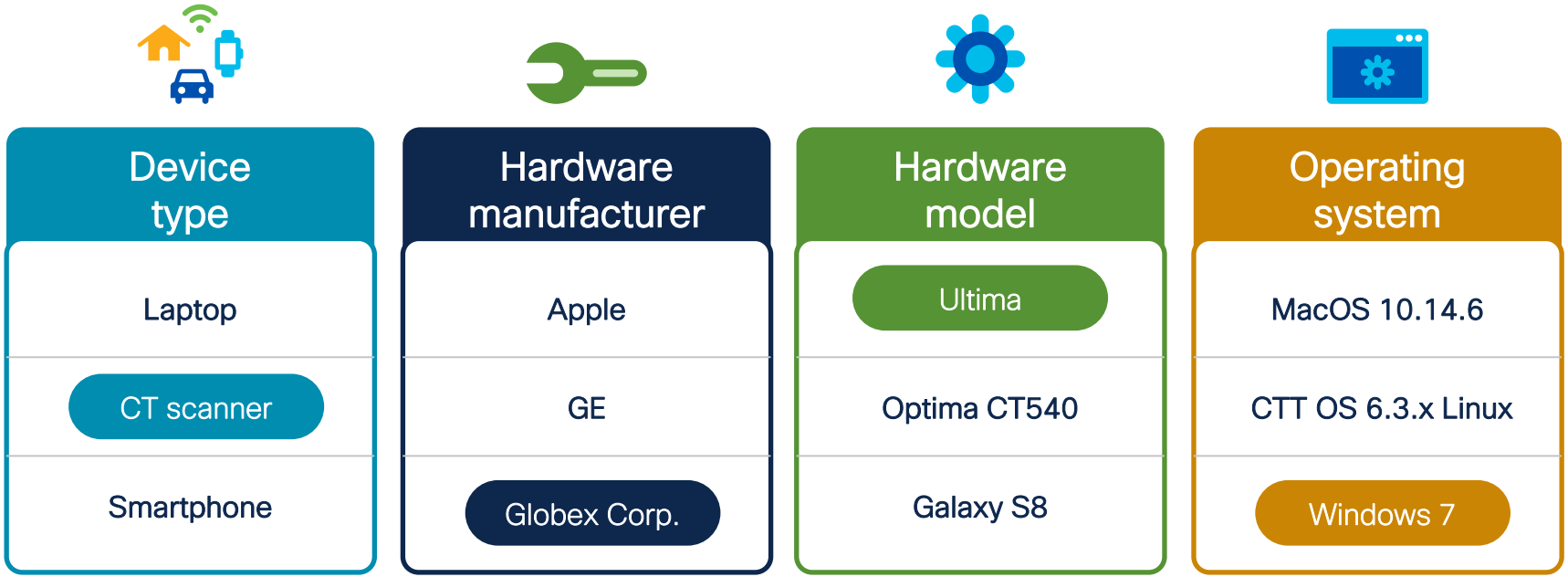
Connected Catalyst



CMDB = Configuration management database

Endpoint Analytics uses multifactor classification

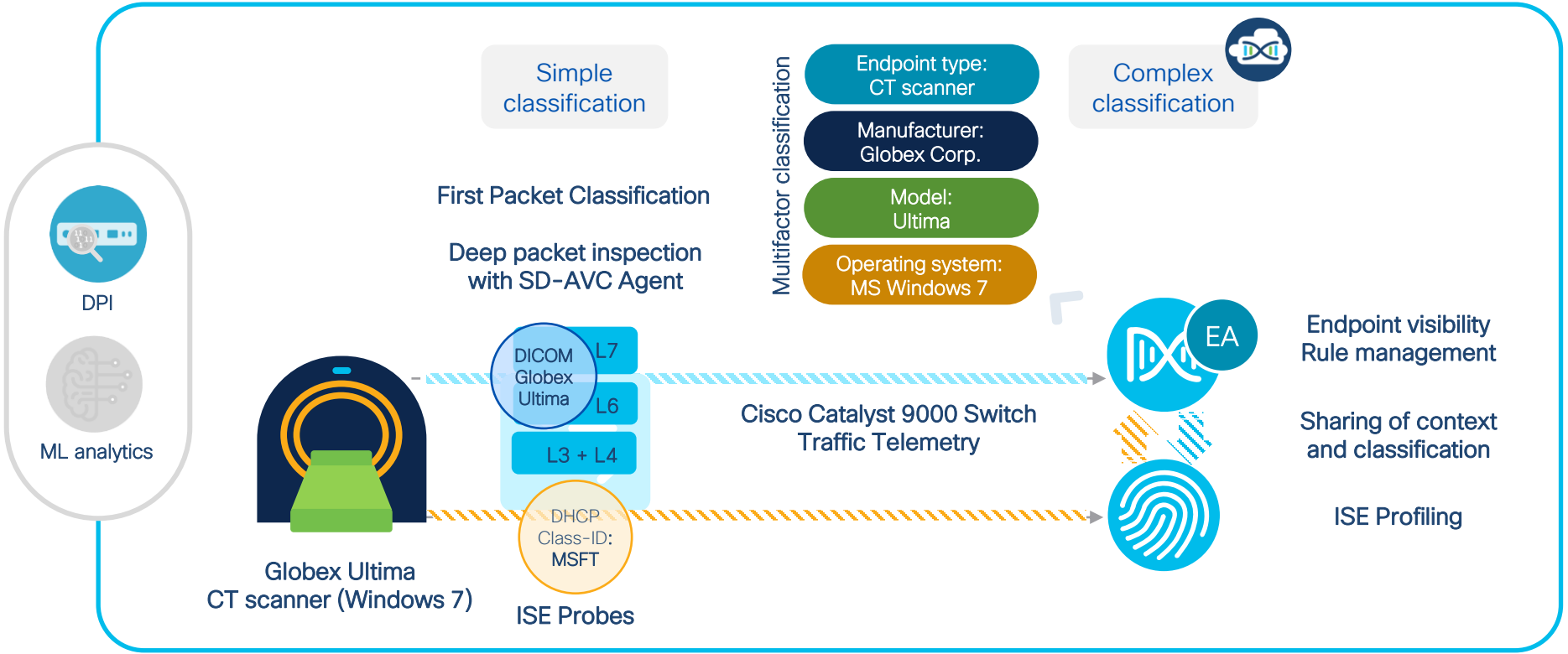
EA classifies endpoints using four independent label categories



Multifactor Classification (MFC) results are shared between Catalyst Center and ISE

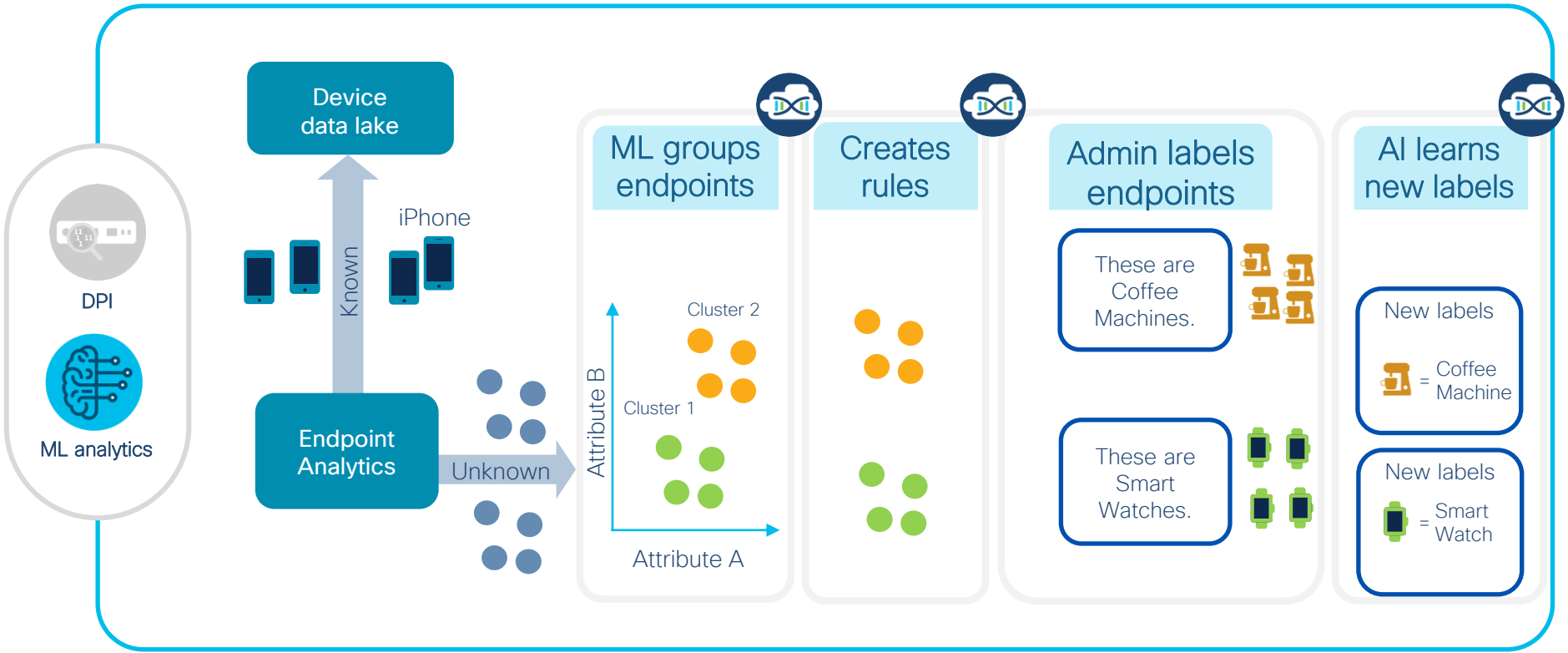
EA classifies based on Deep Packet Inspection

Connected Catalyst



Reduce Unknowns with Machine Learning (ML)

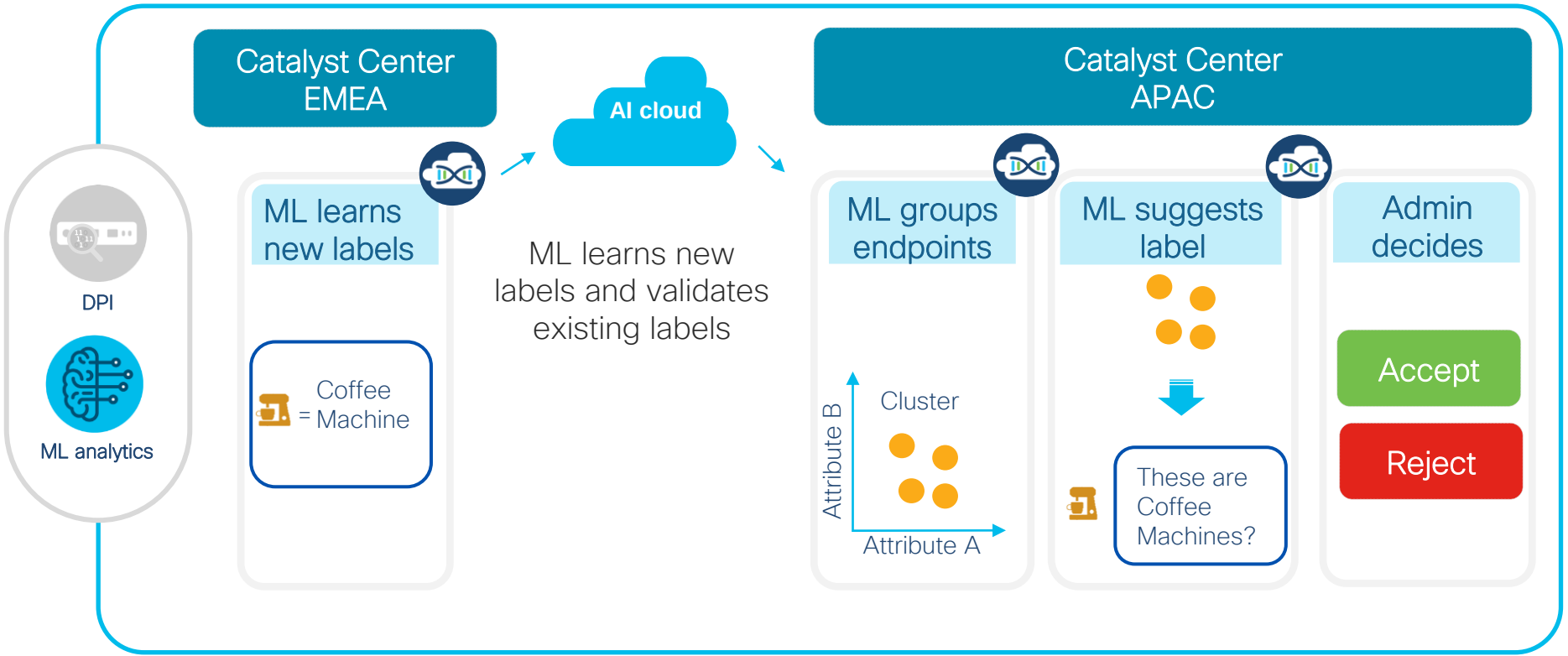
Connected Catalyst



Crowdsourcing improves Machine Learning

Keep your global Catalyst Center deployments synchronized

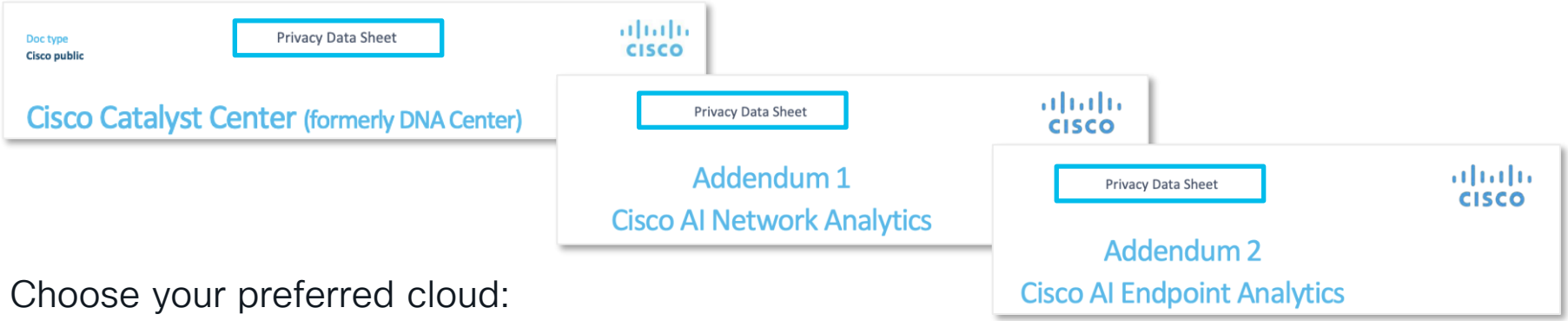
Connected Catalyst



Cisco Connected Catalyst

Optional cloud service that enhances Catalyst Center AI/ML functionality

Connected Catalyst



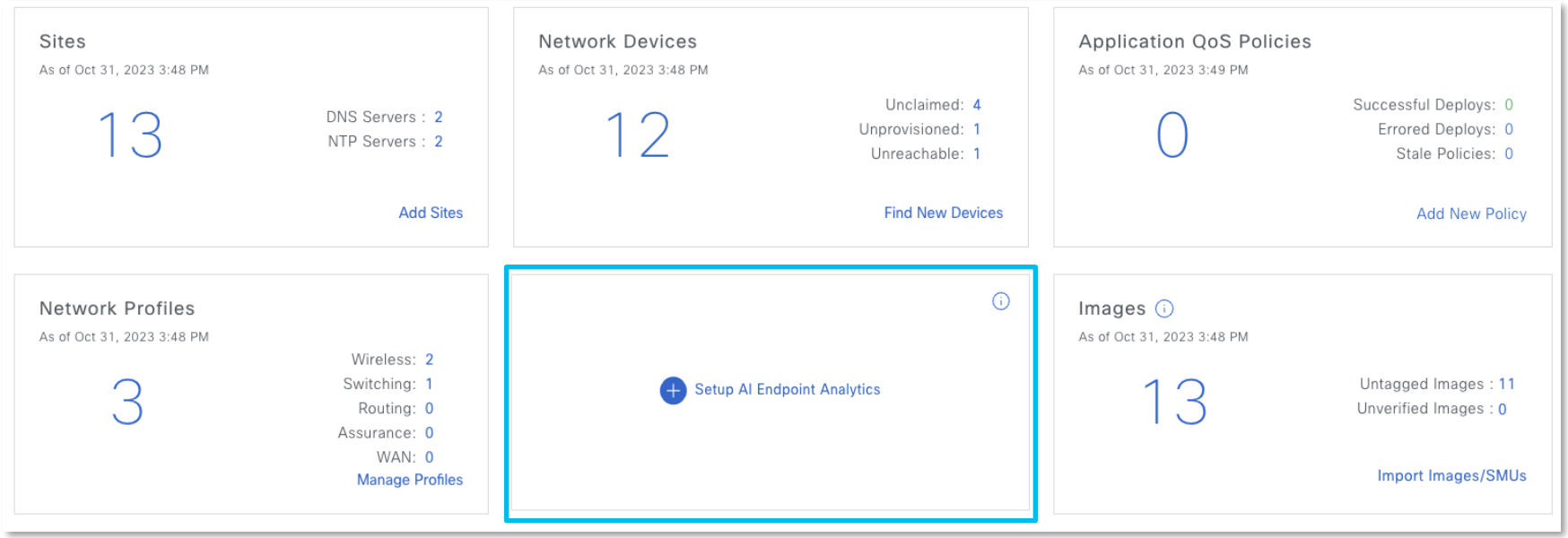
Choose your preferred cloud:

Cloud Use-Case	EU (Germany)	Asia (Singapore)	US / Canada
Cisco Connected Catalyst	✓	✓	✓
Network Analytics	✓	-	✓
AI machine learning	✓	-	✓
Endpoint Profiling Data	✓	✓	✓
Talos Threat Intelligence	✓	✓	✓

https://trustportal.cisco.com/c/dam/r/ctp/docs/privacydatasheet/DNA/cisco-dna-center-privacy-data-sheet.pdf

Endpoint Analytics Dashlet on Landing Page

Before setup, dashlet shows link to Day 0 Interactive Setup for EA

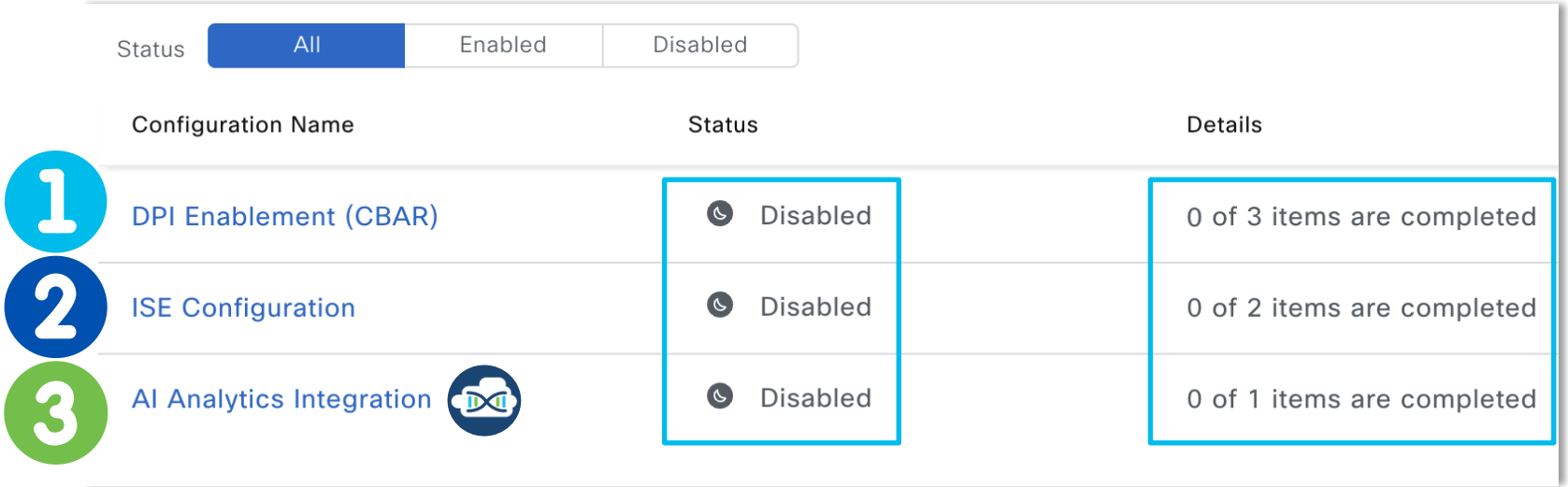


The landing page has a dashlet that takes you to Day 0 interactive setup for EA

Required Configuration Steps to enable EA

Policy > Endpoint Analytics – Manage Sources – Manage Configurations

Connected Catalyst

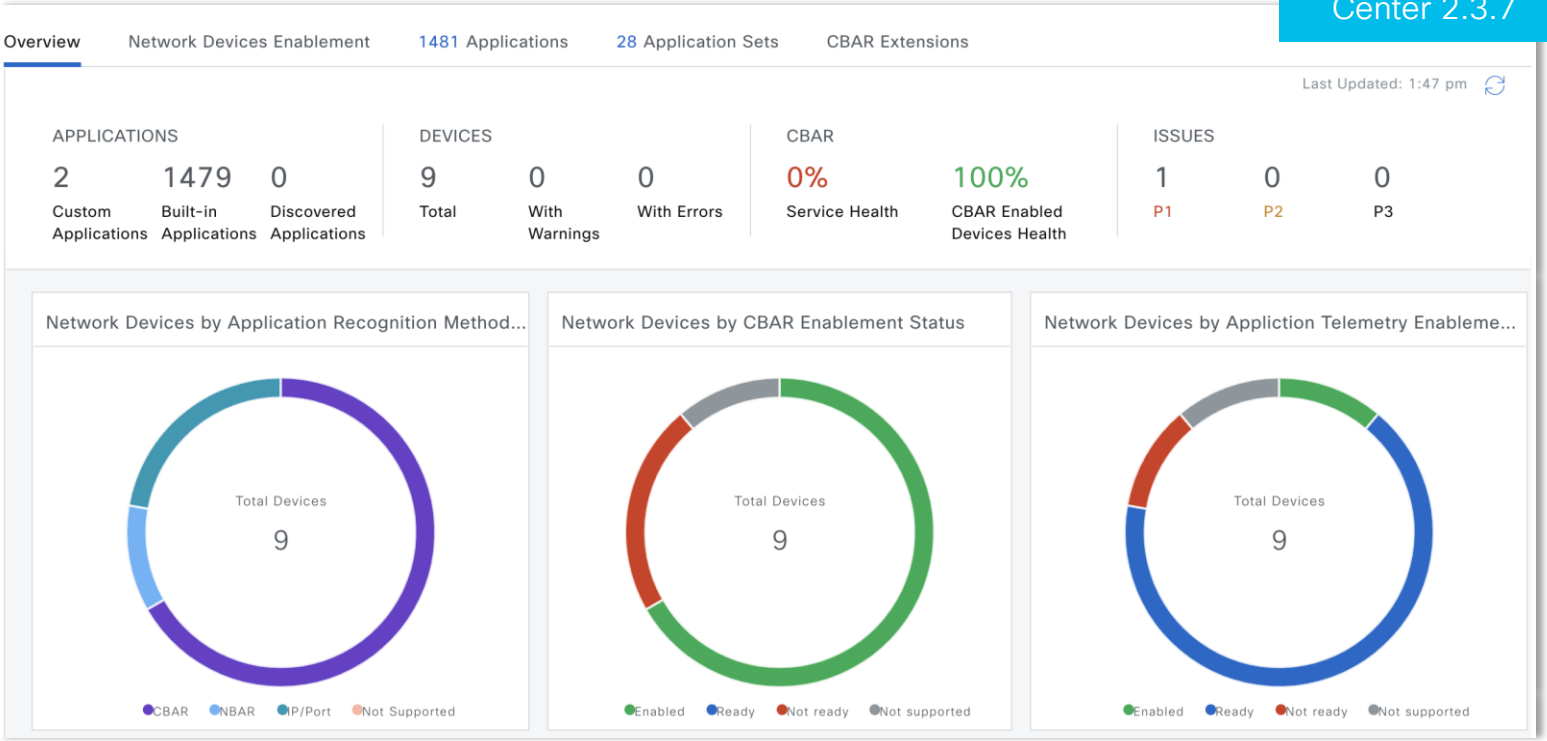


- Check the status of required configurations for EA
- Use links to follow steps to enable all three required configurations

Enable CBAR on C9K Devices

Provision > Services > Application Visibility Setup > Overview

*New in Catalyst Center 2.3.7

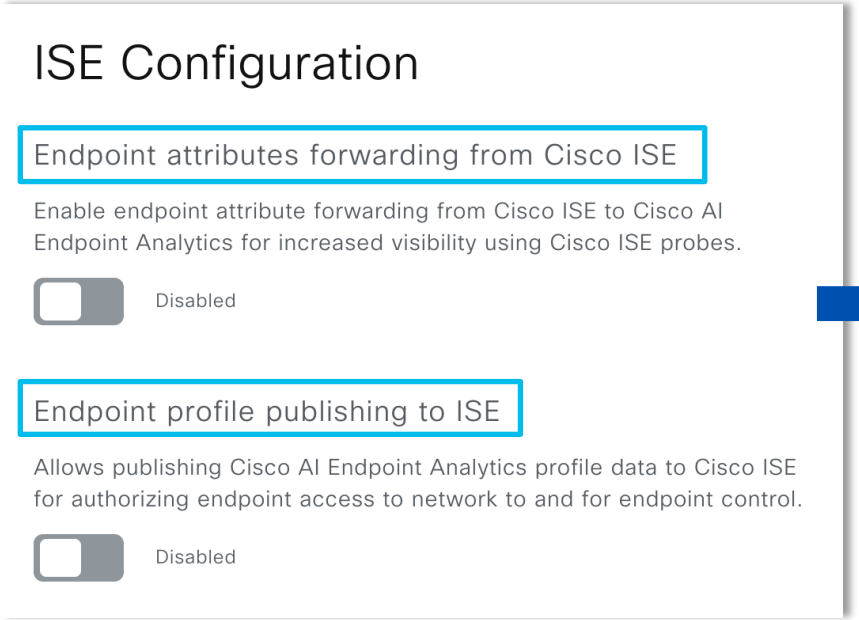


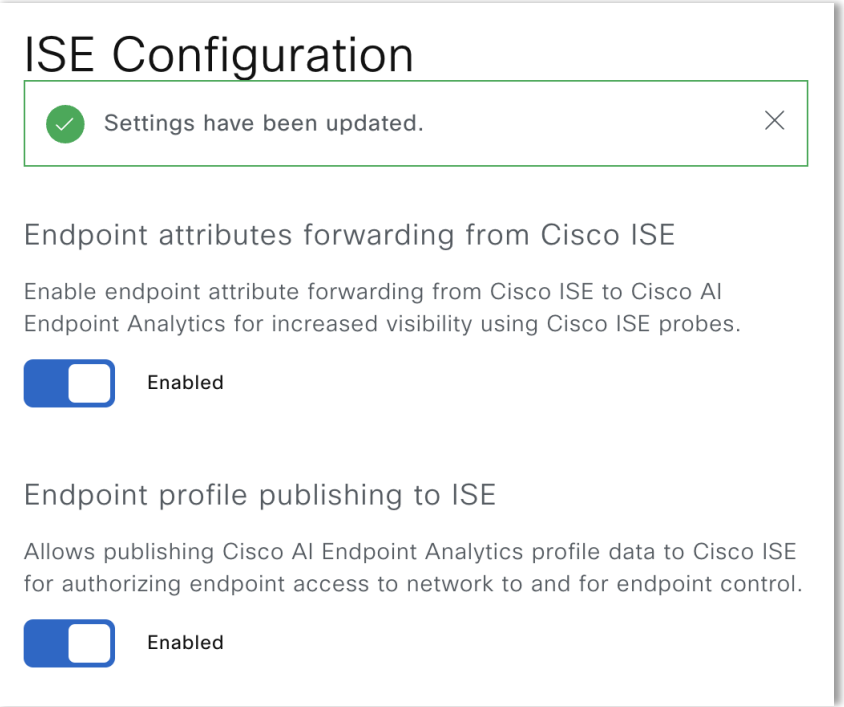
*Application Visibility is enabled by default on C9K switches during the site assignment workflow

Enable Enhanced ISE Integration

Using Day 0 Interactive Setup Workflow

2

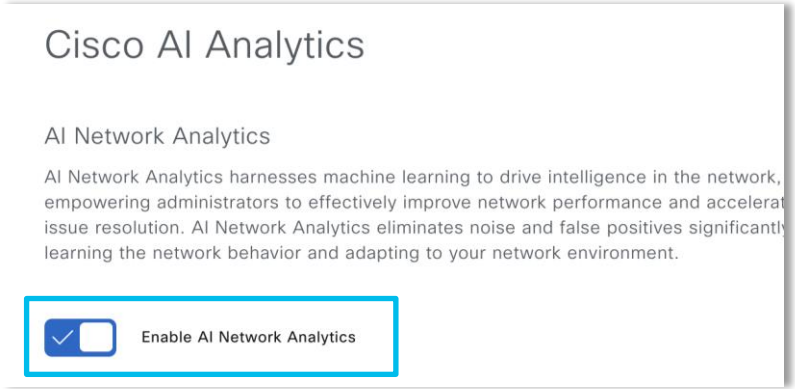




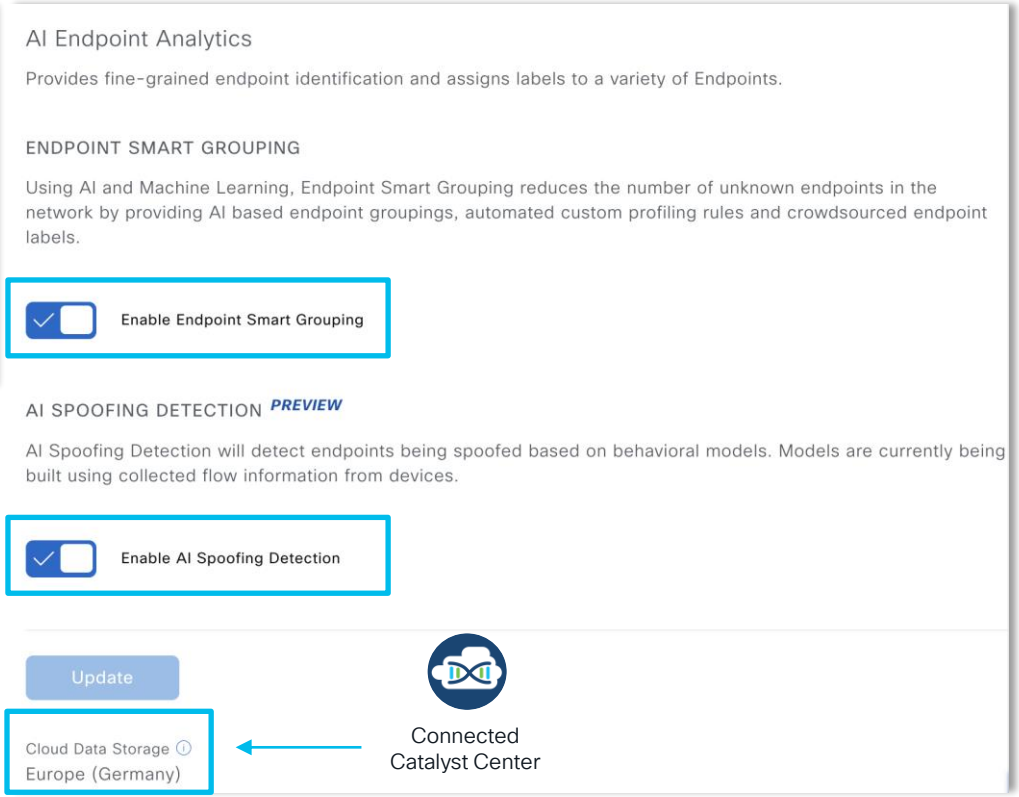
Enable bi-directional publication and consumption of EA attributes in ISE and Catalyst Center

Enable Catalyst Center AI Analytics

System > Settings > Cisco AI Analytics



Enable AI **Network** Analytics



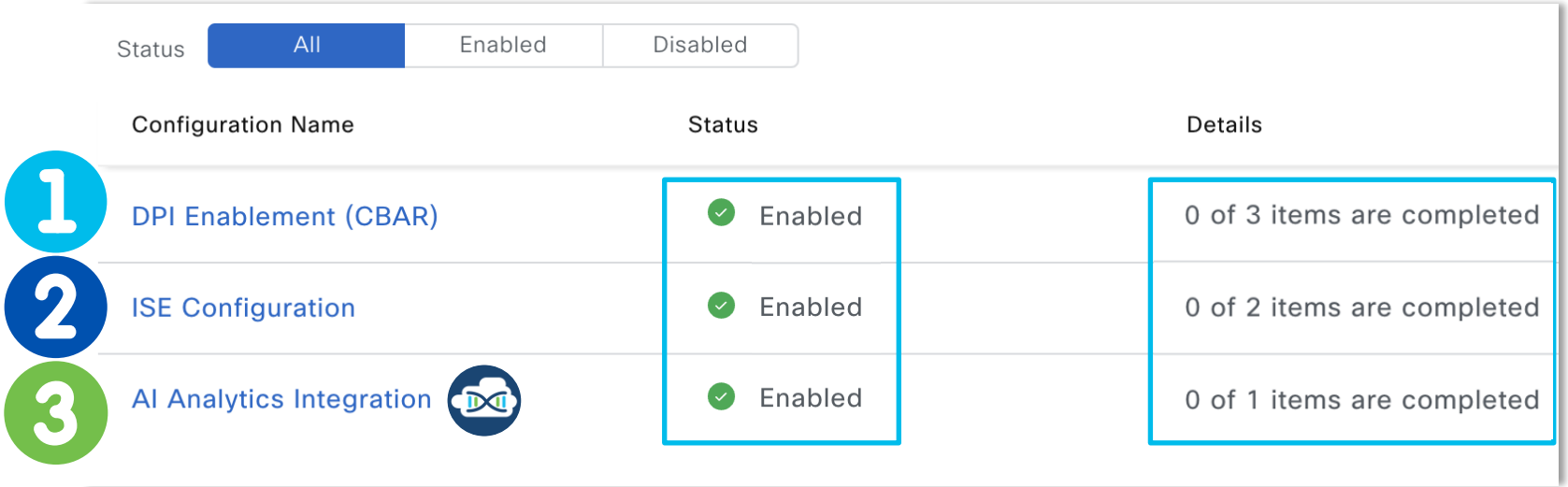
Enable AI **Endpoint** Analytics settings

- Endpoint Smart Grouping
- AI Spoofing Detection
- Choose Cloud Data Storage location

Required Configuration Steps to enable EA

Policy > Endpoint Analytics – Manage Sources – Manage Configurations

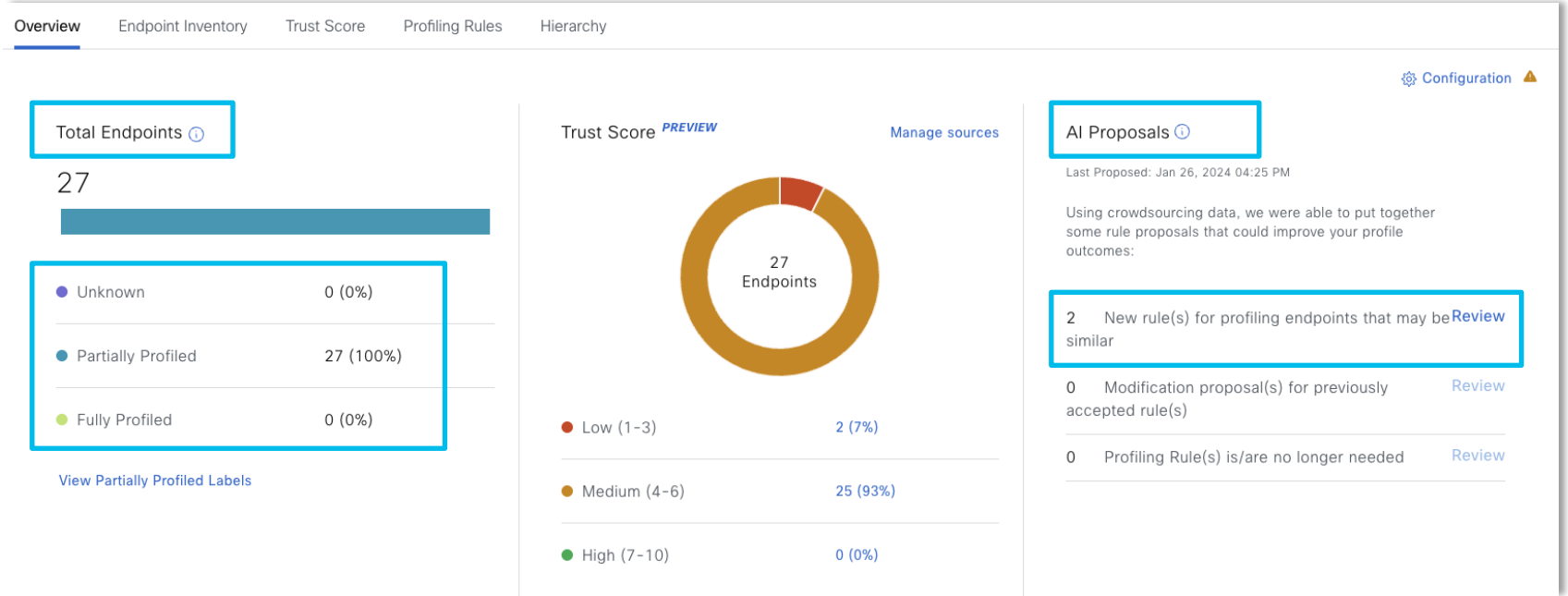
Connected Catalyst



- After Day 0 setup check the status of required configurations for EA
- Required configurations should all be in status enabled for best results

View the Endpoint Analytics Outcomes

Policy > AI Endpoint Analytics > Overview

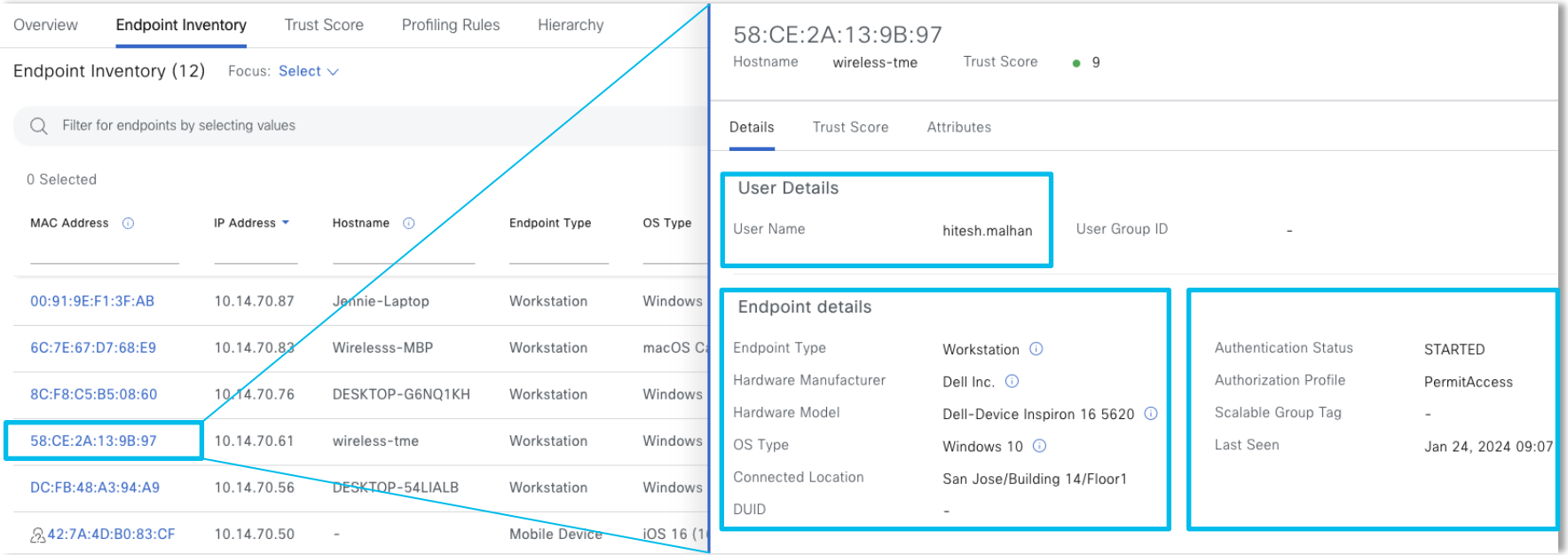


Overview shows endpoint profiling status, trust score distribution and AI Proposals

View Endpoint Inventory

Policy > AI Endpoint Analytics > Endpoint Inventory

Endpoint visibility



Endpoint Inventory shows all known endpoint MAC addresses and classification

EA Attributes are integrated into Assurance

Assurance > Dashboards > Health > Client

New in Catalyst Center 2.3.7

Client Devices (5)

★ Tracked Clients

LATEST TREND

TYPE Wireless Wired OVERALL HEALTH All Poor Fair Good Inactive No Data

DATA Onboarding Time >= 10s | Association >= 5s | DHCP >= 5s | Authentication >= 5s | RSSI <= -72 dBm | SNR <= 9 dB

Export

Search Table

0 Selected Actions

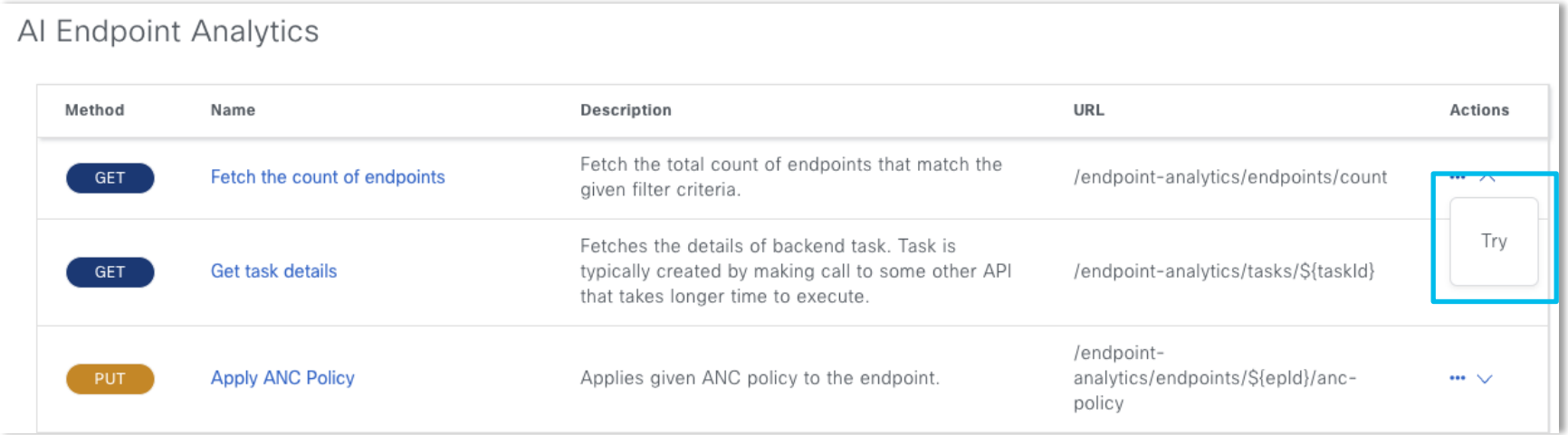
Identifier	Device Type	Health	Trust Score	Onboarding Health	Connected Health	Hardware Manufacturer	OS	Endpoint Type
anna	Intel-Device	10	9	●	●	Intel Corporation	Windows	Workstation
greg	Intel-Device	10	9	●	●	Intel Corporation	Windows	Workstation
Ingrid	RaspberryPi-Device	10	9	●	●	Raspberry Pi Foundation	Linux	IOT Device

Client Devices table in Assurance shows additional Endpoint Analytics information

AI Endpoint Analytics REST APIs

New in Catalyst Center 2.3.5

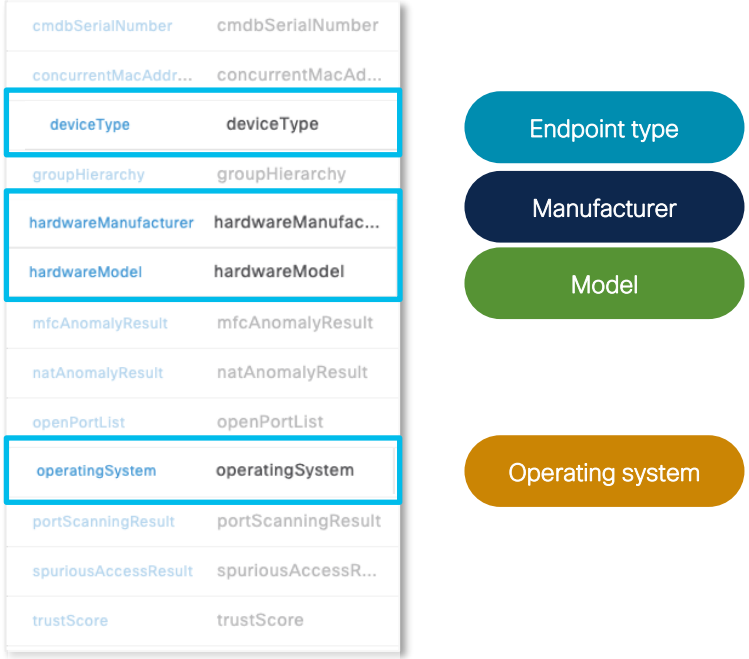
Platform > Developer > Toolkit > APIs



Use the Catalyst Center APIs to operate AI Endpoint Analytics

Endpoint Analytics brings new dictionary to ISE

ISE: Policy > Policy Elements > Dictionaries > System > Endpoint-Analytics



Several new endpoint attributes available for identification in authorization policies

Use Endpoint Analytics attributes in ISE policy

Authorization policy for **HP Printers**:

If
- Endpoint Group: Printer MAC Addresses
- Endpoint Analytics: device type is Printer
- Endpoint Analytics: HardwareManufacturer is HP

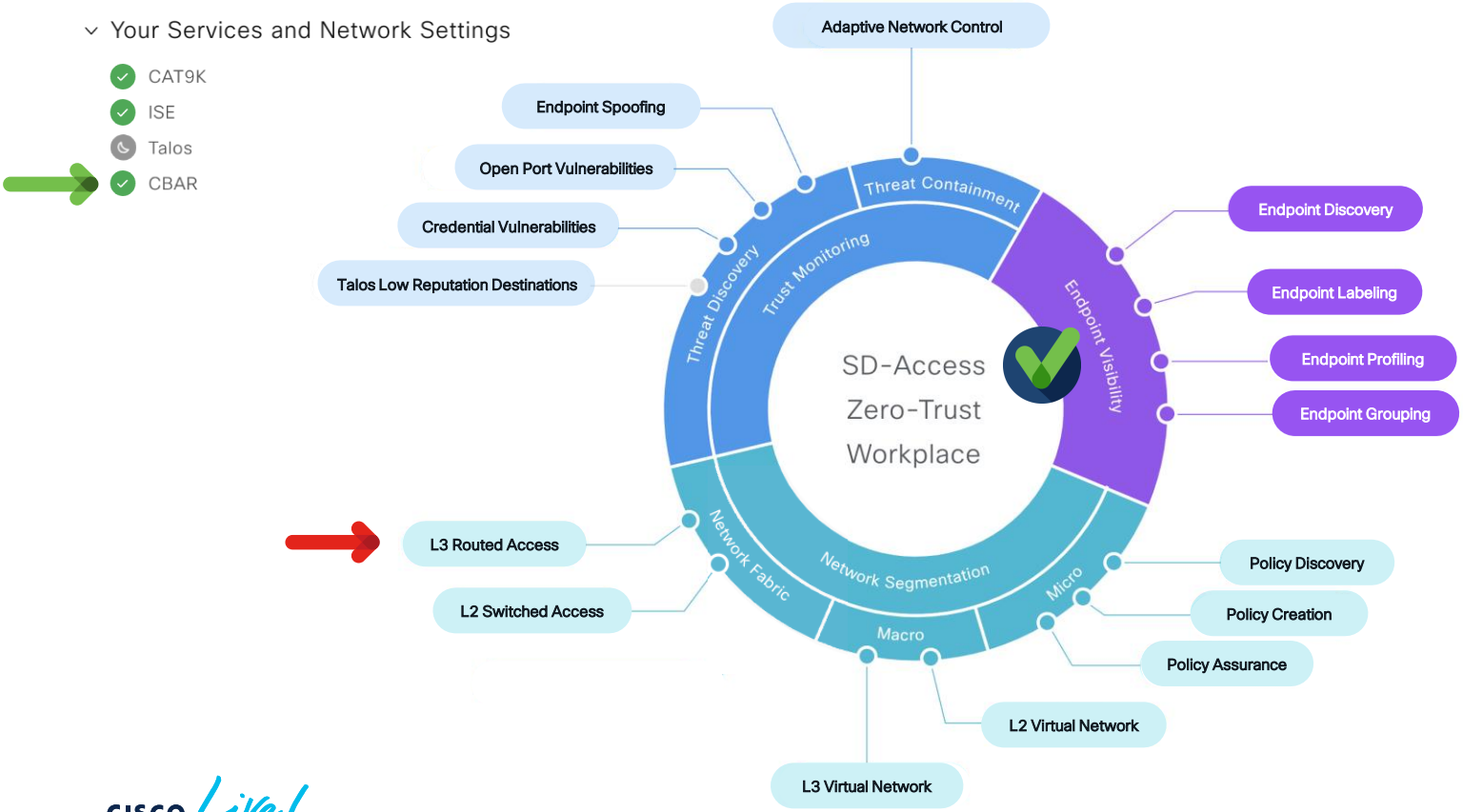
,Then Assign SGT Printer

Authorization policy for legacy **printers**

If
- Endpoint Group: Printer MAC Addresses
- Endpoint Analytics: device type is Printer
- Endpoint Analytics: HardwareManufacturer is not HP

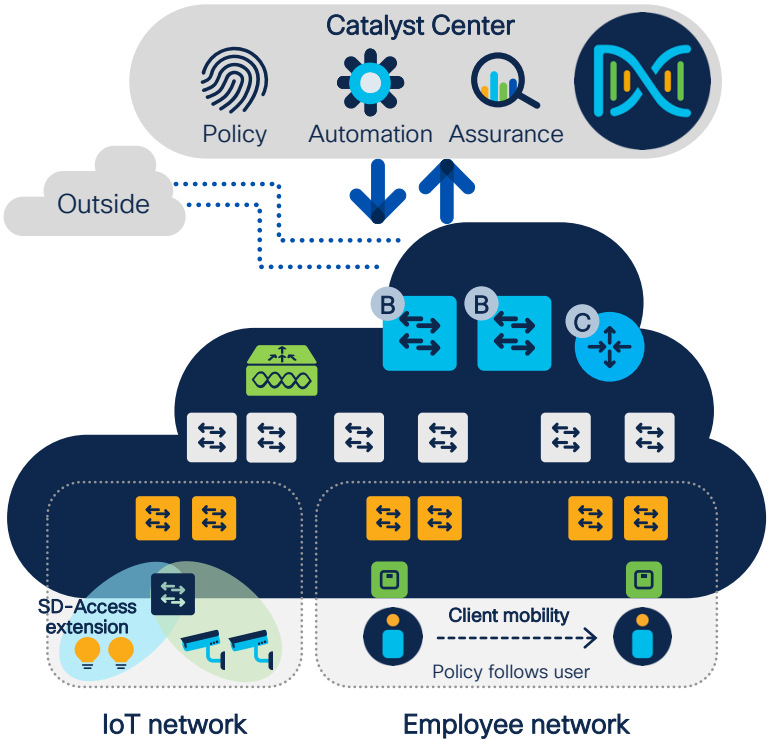
,Then Assign SGT Legacy

We gained deep visibility of our endpoints



Why use SD-Access for network segmentation?

See the benefits of SDA for Zero Trust



Deep visibility

Identify and **group** endpoints. Map their interactions and define access policies

Group-based policy and segmentation

Enforce group-based access policies and secure network through segmentation

Policy consistency throughout

Use **Cisco's multidomain architecture** for consistent access and security policies throughout the enterprise

SD-Access – Solid Underlay with Flexible Overlay

Separation of “Forwarding Plane” from “Services Plane

Overlay Network

- **Control Plane** based on LISP
- **Data Plane** based on VXLAN
- **Policy Plane** based on TrustSec

Underlay Network

- **Control Plane** based on IS-IS

LAN Automation deploys underlay automatically

Prerequisites for LAN Automation listed in Overview

Overview

LAN Automation is an alternative to manual deployments for new networks. It helps simplify network operations by freeing network administrators from time-consuming and repetitive network configurations tasks need to create a standard error-free network. LAN Automation uses the IS-IS routing protocol to deploy a Layer 3 routed access design.

Prerequisites

- Create Network Hierarchy
- Define Network Settings
- Define Device Credentials
- Define IP Address Pool at Global Level
- Reserve IP Address Pool at Site-Specific Level
- Discover Seed Devices
- Start LAN Automation

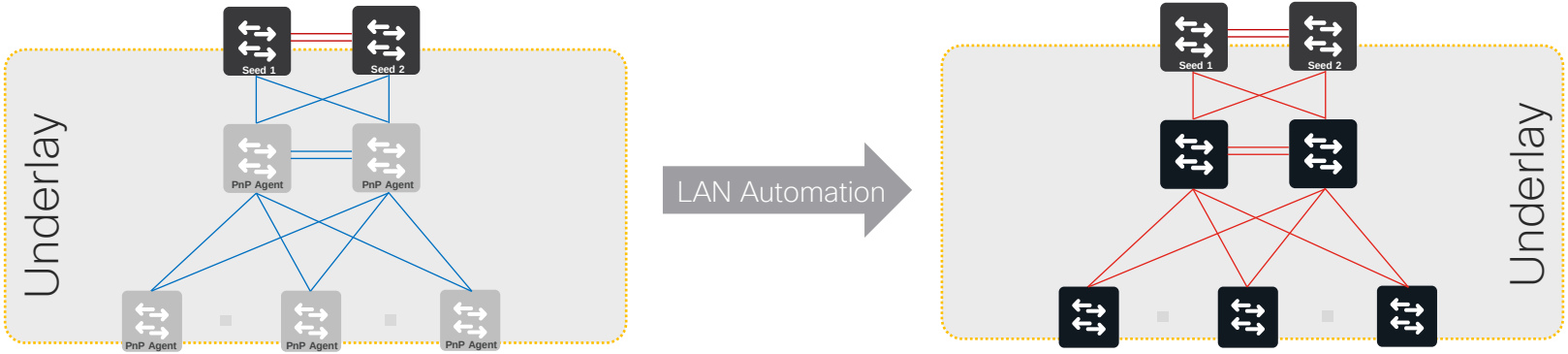
Why should we use LAN Automation?

Explaining the LAN Automation

LAN automation leverages PnP and configures for you:

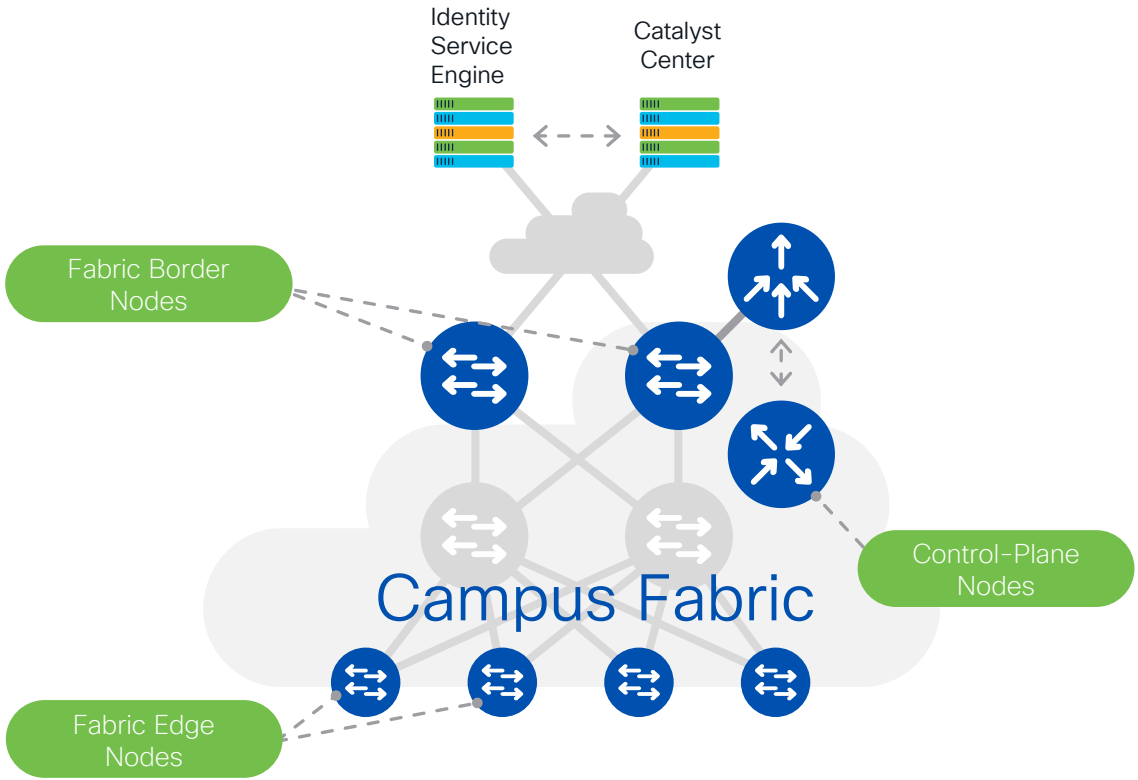
- Routed interconnections
- Loopback0
- IS-IS routing protocol
- Host names

Prescriptive. You need to start from a seed device



Main Roles to establish SD-Access Overlay

Explaining Fabric Roles & Terminology



Control-Plane Nodes

Map System that manages Endpoint to Device relationships

Fabric Border Nodes

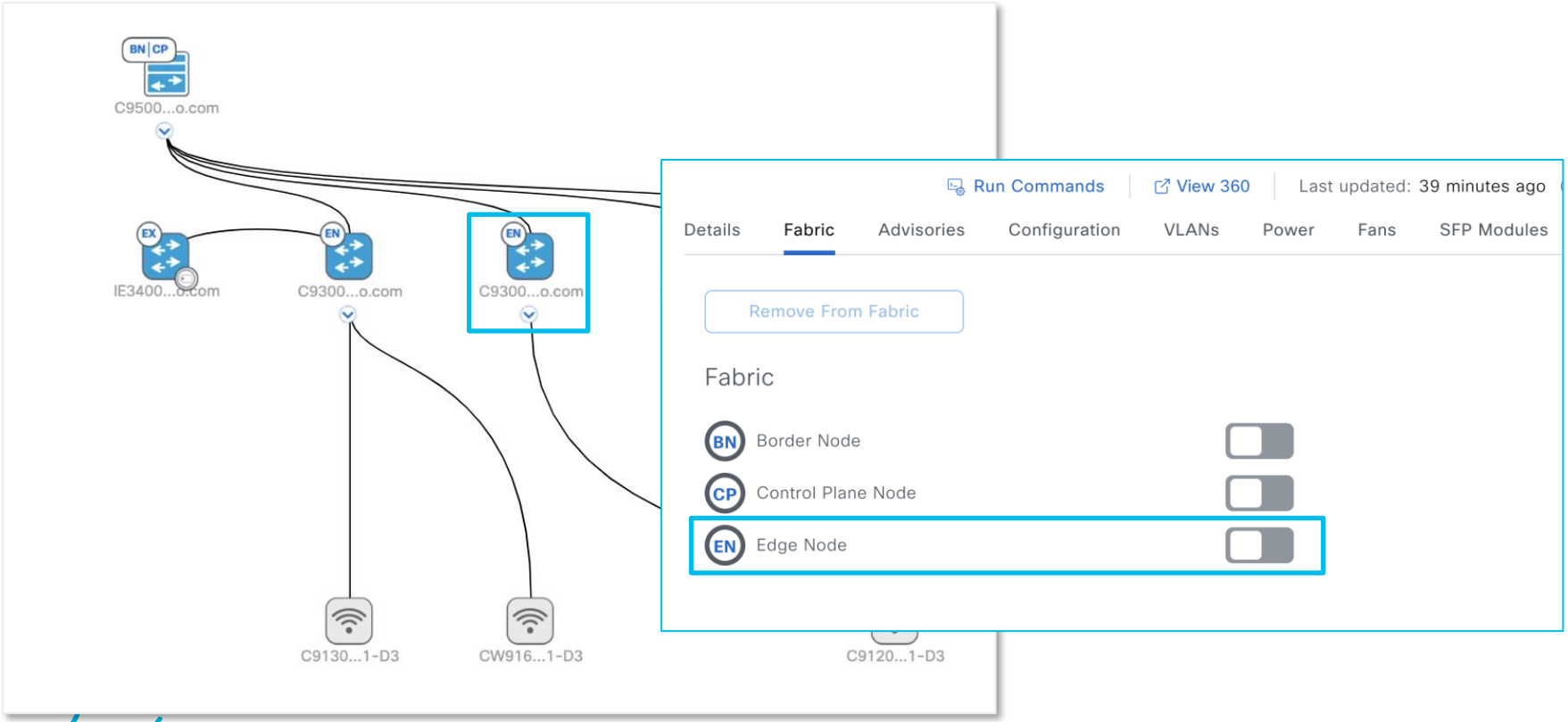
A fabric device (e.g. Core) that connects External L3 network(s) to the SD-Access fabric

Fabric Edge Nodes

A fabric device (e.g. Access or Distribution) that connects Wired Endpoints to the SD-Access fabric

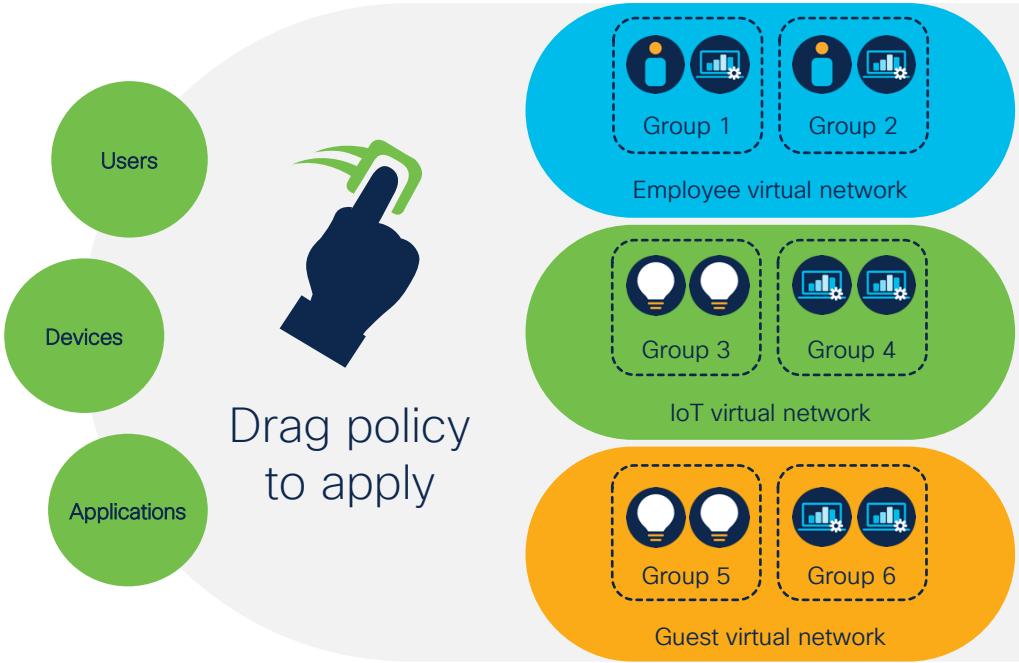
Assign Fabric Roles to Fabric Devices

Assign Fabric Control Plane, Border Node and Edge Roles



Segmentation Simplicity

Catalyst Center: SD-Access



IT simplicity

- No VLAN, ACL, or IP address management required
- Single network fabric
- Define one consistent policy

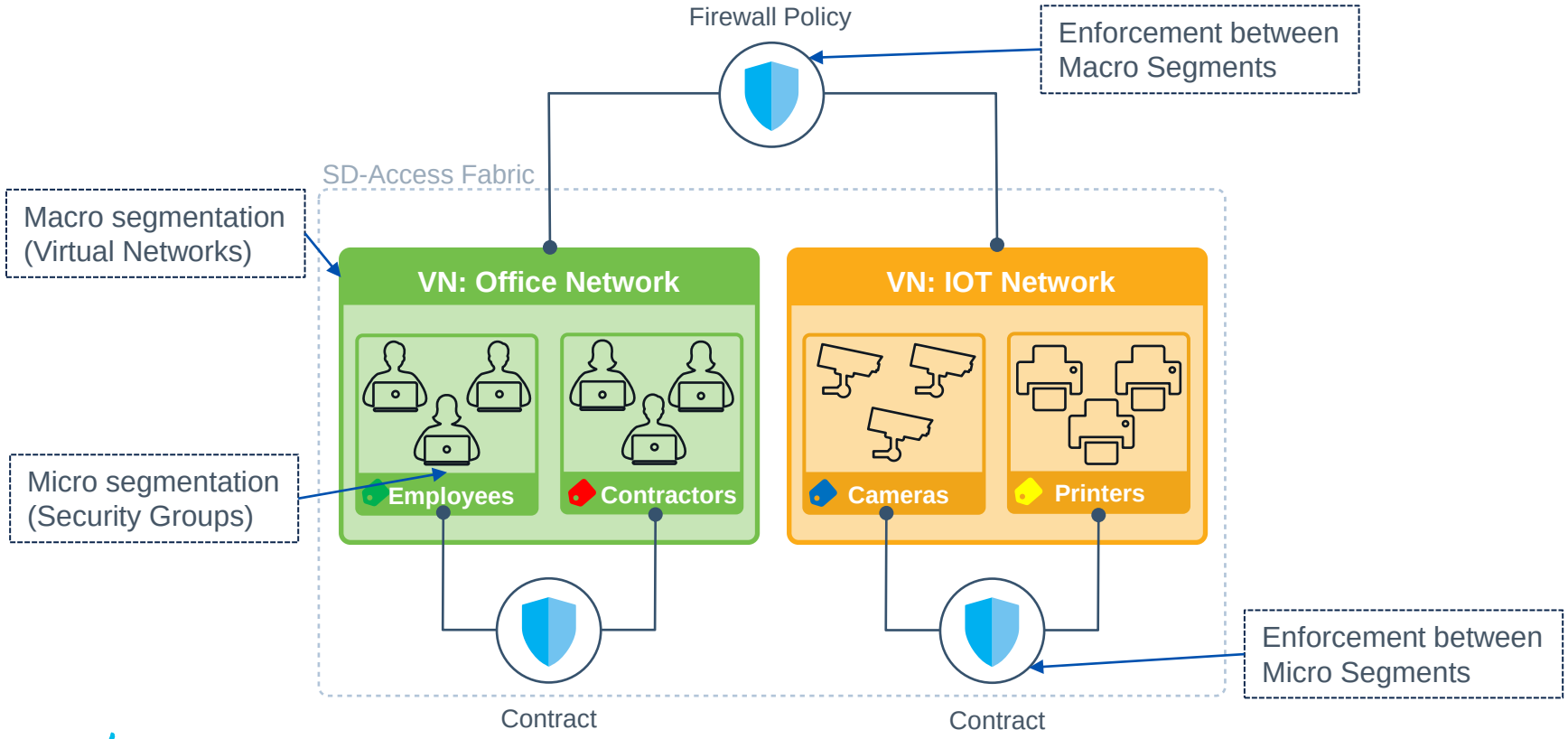
Security

- Simplified micro segmentation
- Policy enforcement
- Policy follows identity

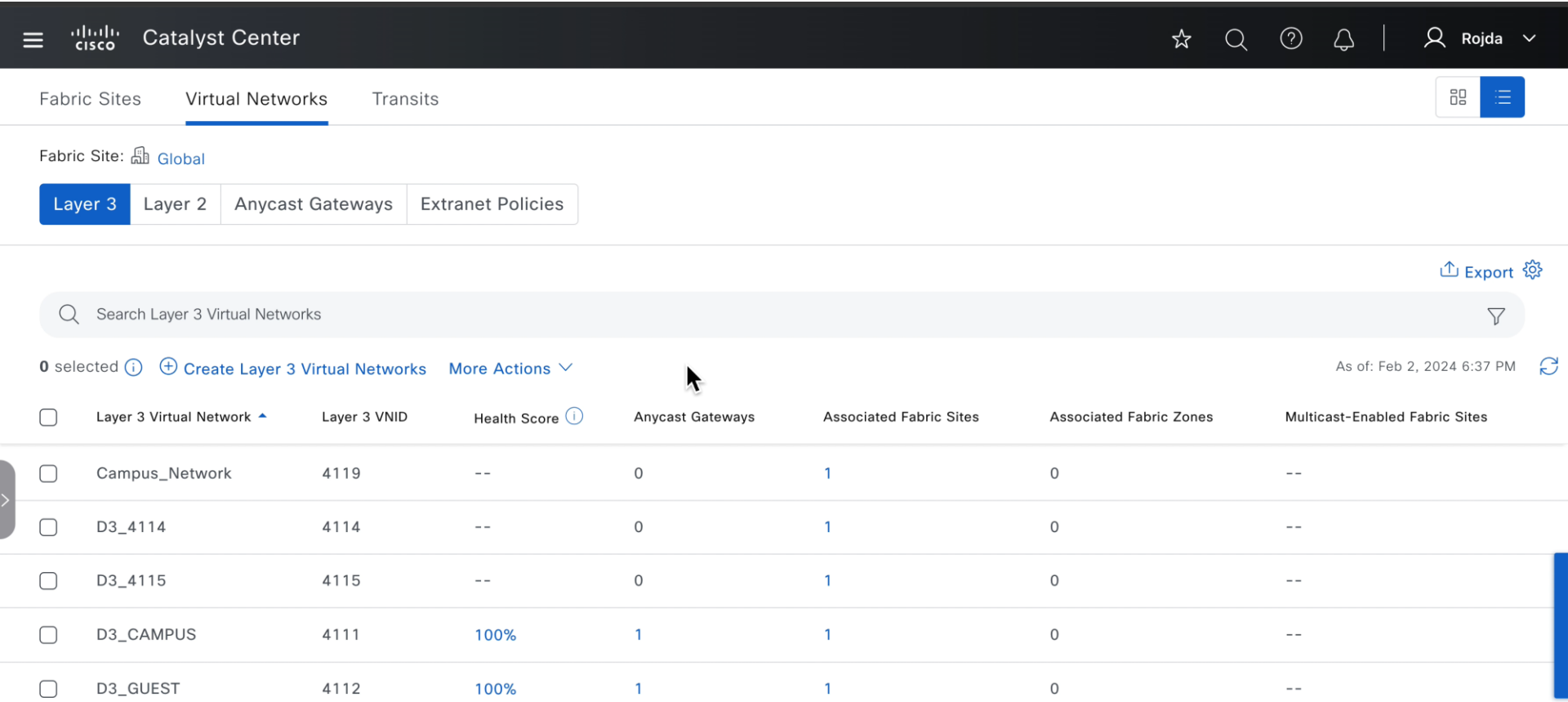
Completely automated | Consistent policy | Minimize lateral threat movement

SD-Access enables Multi-Level Segmentation

Macro and Micro Segmentation

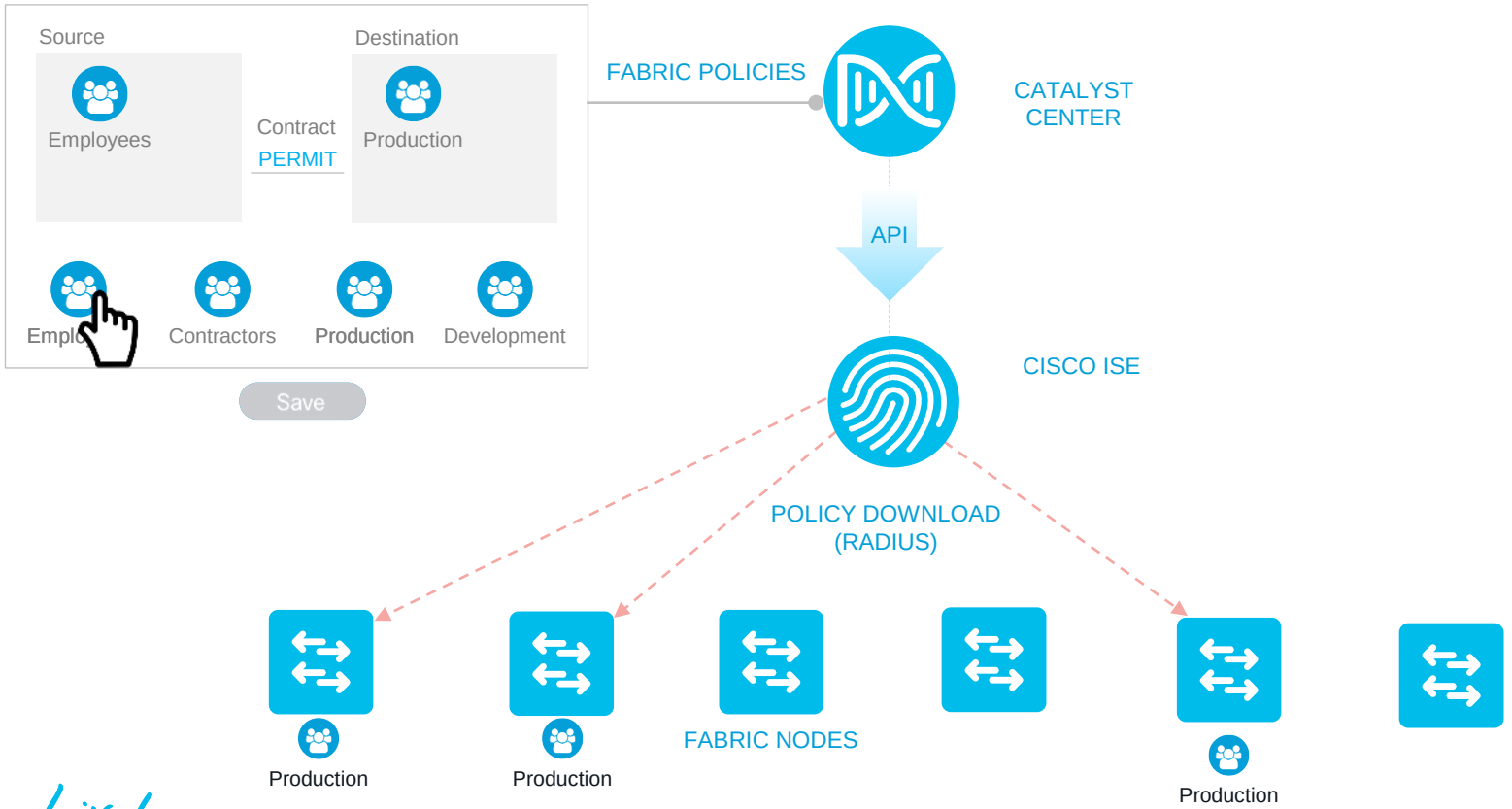


Demo



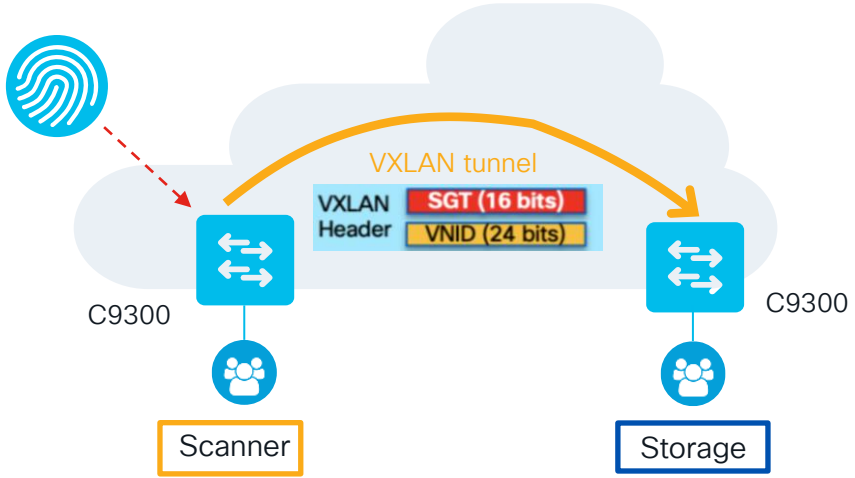
SD-Access Policy

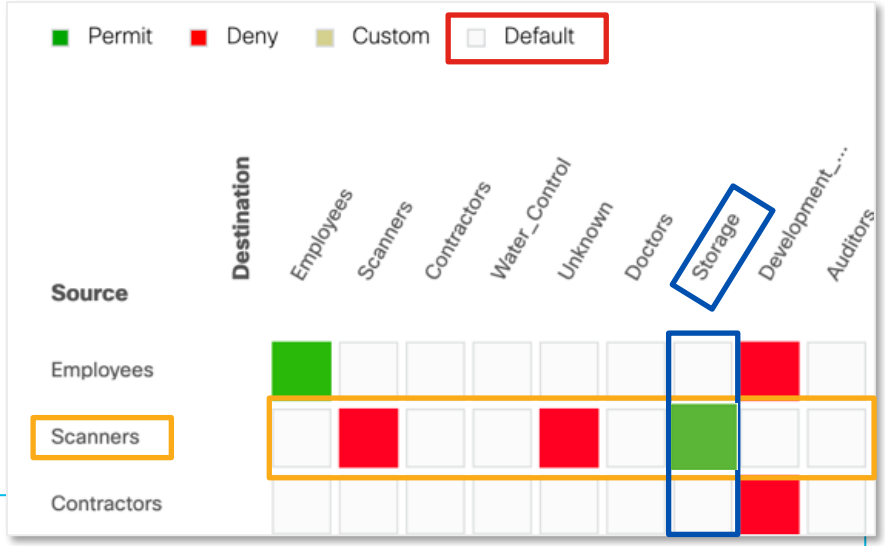
Security Group Policy Rollout



The Value of Group-Based Policies

Create meaningful group-based policies aligned to business needs



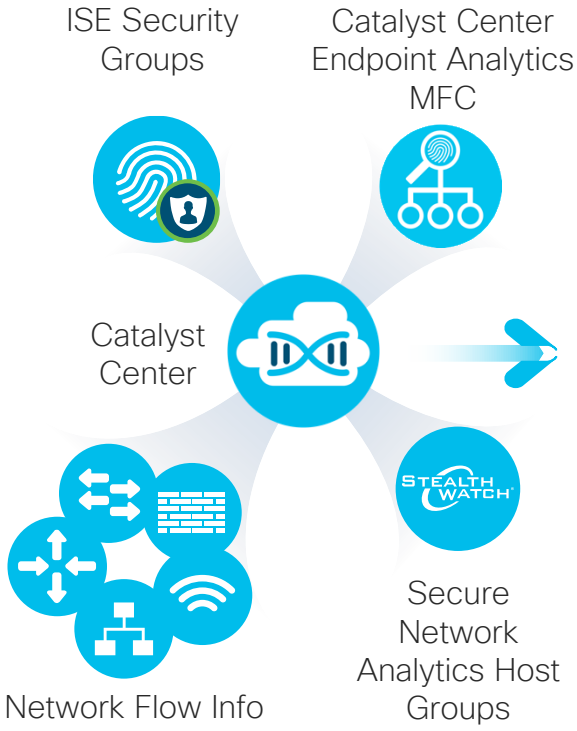


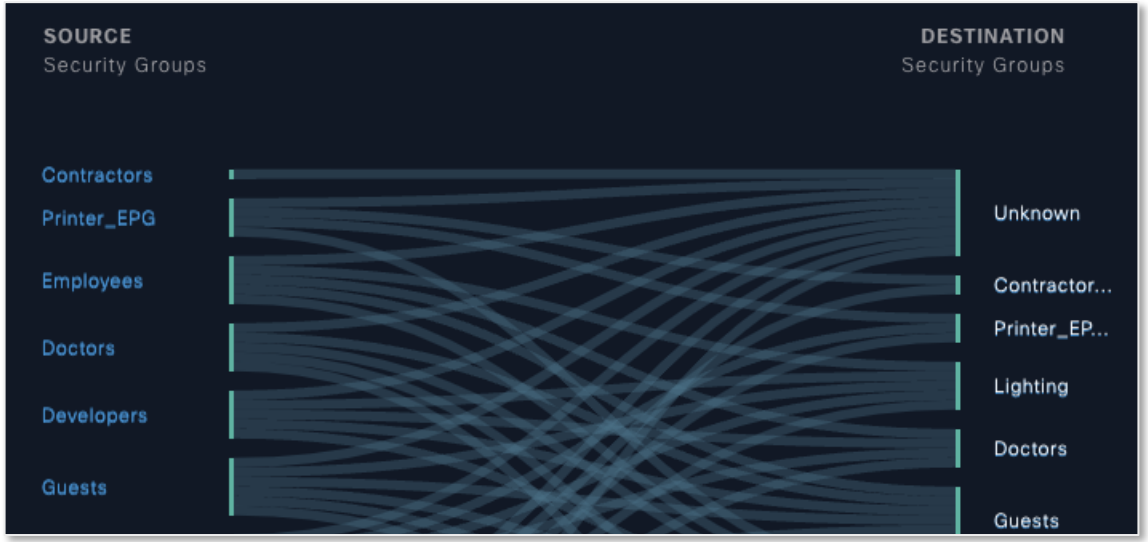

```
Edge-Cat9300#show cts role-based permissions

IPv4 Role-based permissions default:
        Deny IP-00
IPv4 Role-based permissions from group 36 Scanners to group 27 Storage_PACS:
        Permit_IP_Log-01
```

Group Based Policy Analytics shows real flows

Displays traffic between groups



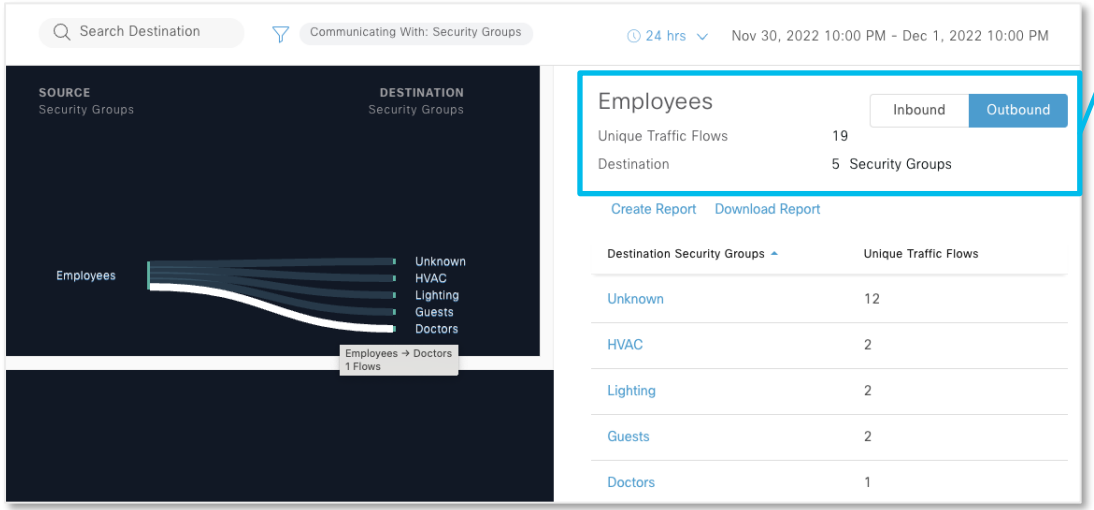


Default permit → Default deny

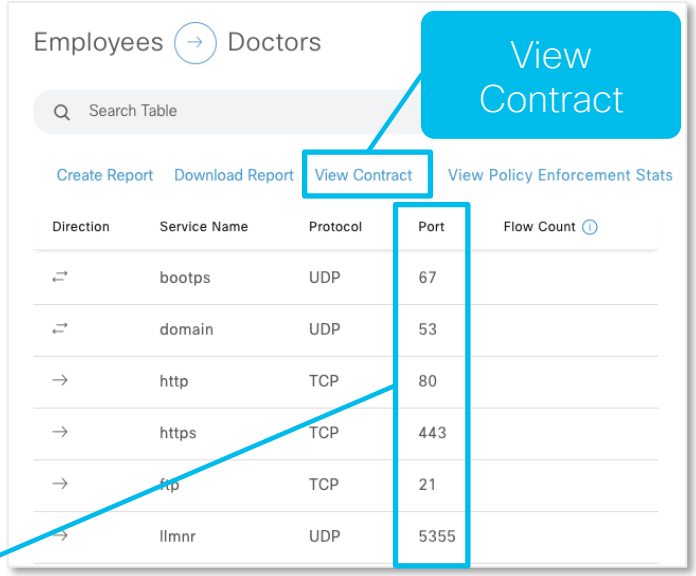
Cisco ISE TrustSec Allow-List Model (Default Deny IP) With SDA
https://www.cisco.com/c/en/us/support/docs/cloud-systems-management/dna-center/215516-trustsec-whitelist-model-with-sda.html

Explore Flows for Security Groups

Detecting used ports and protocols for communication between groups



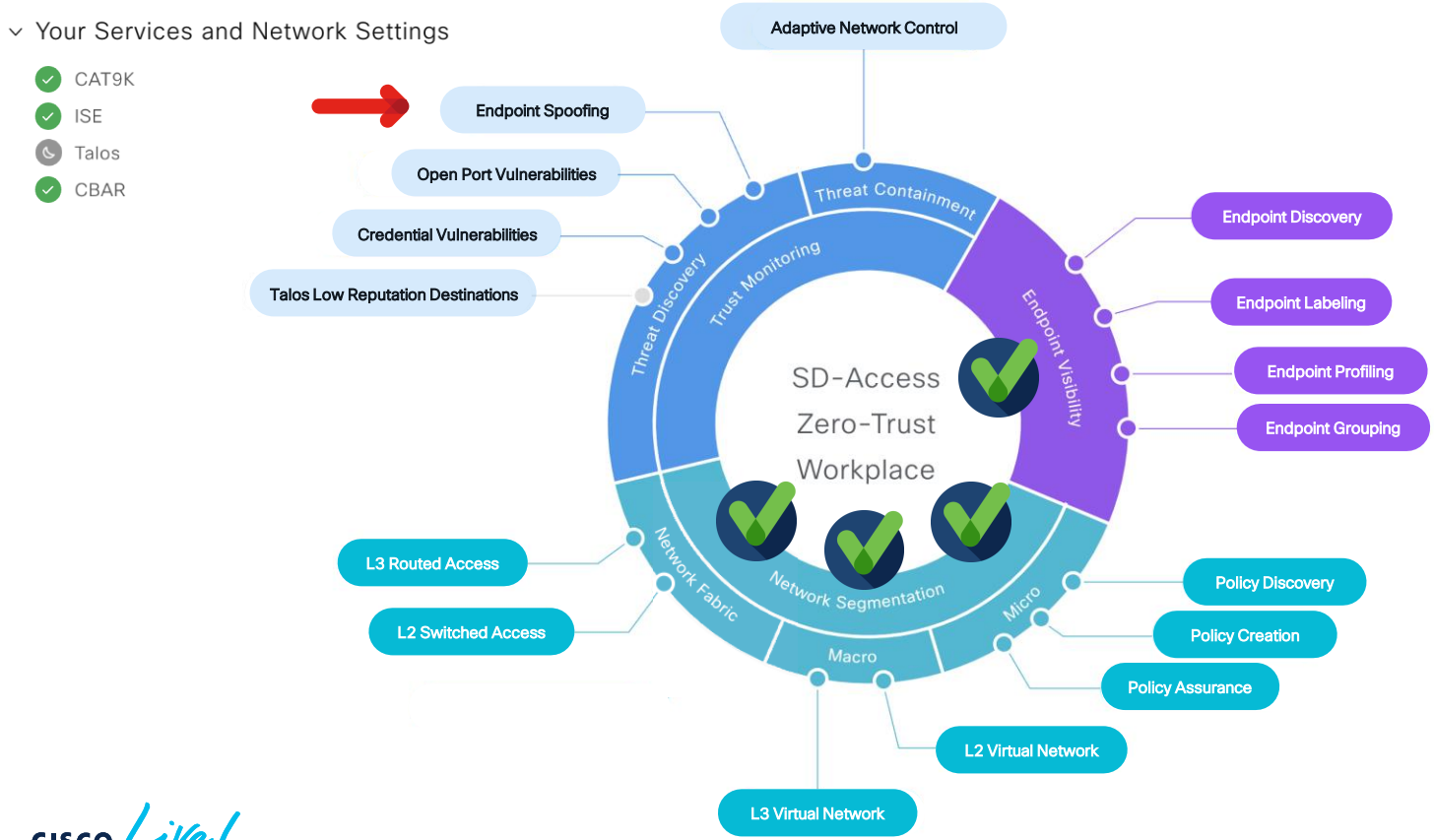
Traffic flows to 5 destination security groups



View Contract

Ports detected from group Employees to group Doctors

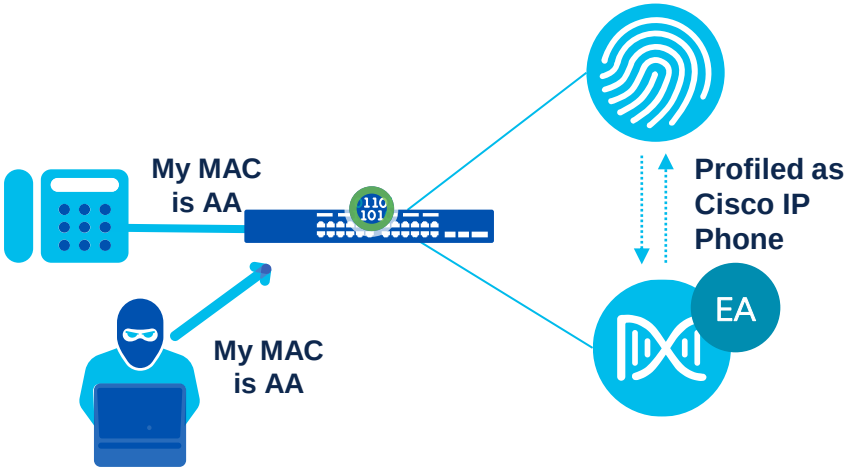
We segmented our network on multiple levels



Problem to solve: Impersonation Attacks

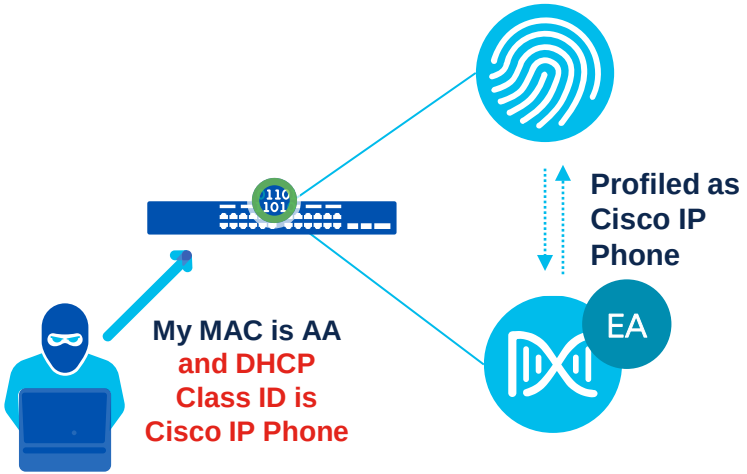
MAC address must not be the only source of truth

MAC Spoofing



Impersonate the MAC address of another authorized endpoint in order to gain the same privileges

Attribute Spoofing



Impersonate class/type of the device in order to get privileged network access

Trust based network access with Trust Analytics

Trust Score assesses the trustworthiness of a given endpoint on the network

Positive Influence

- ✓ Secure Authentication
- ✓ Posture Compliance

Trust-based ISE Policies

1-3	Deny access
4-7	Limited access
7-10	Full access

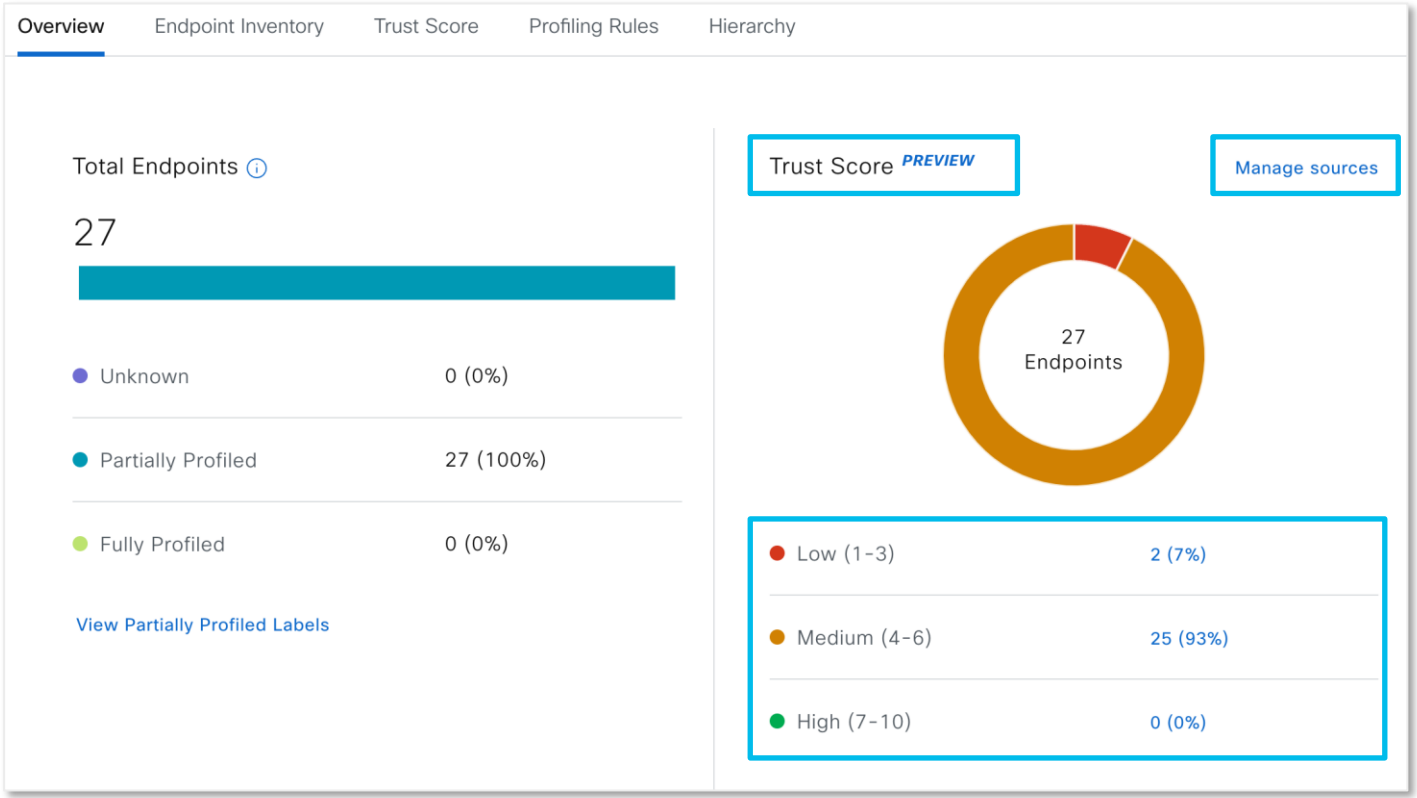
Negative Influence

- ✘ Impersonation Attacks
- ✘ Insecure software interface
- ✘ Unauthorized clients behind NAT
- ✘ Endpoints accessing bad IP sites

Trust Score values range from 1 (low trust) to 10 (high trust)

Trust Scores can be viewed

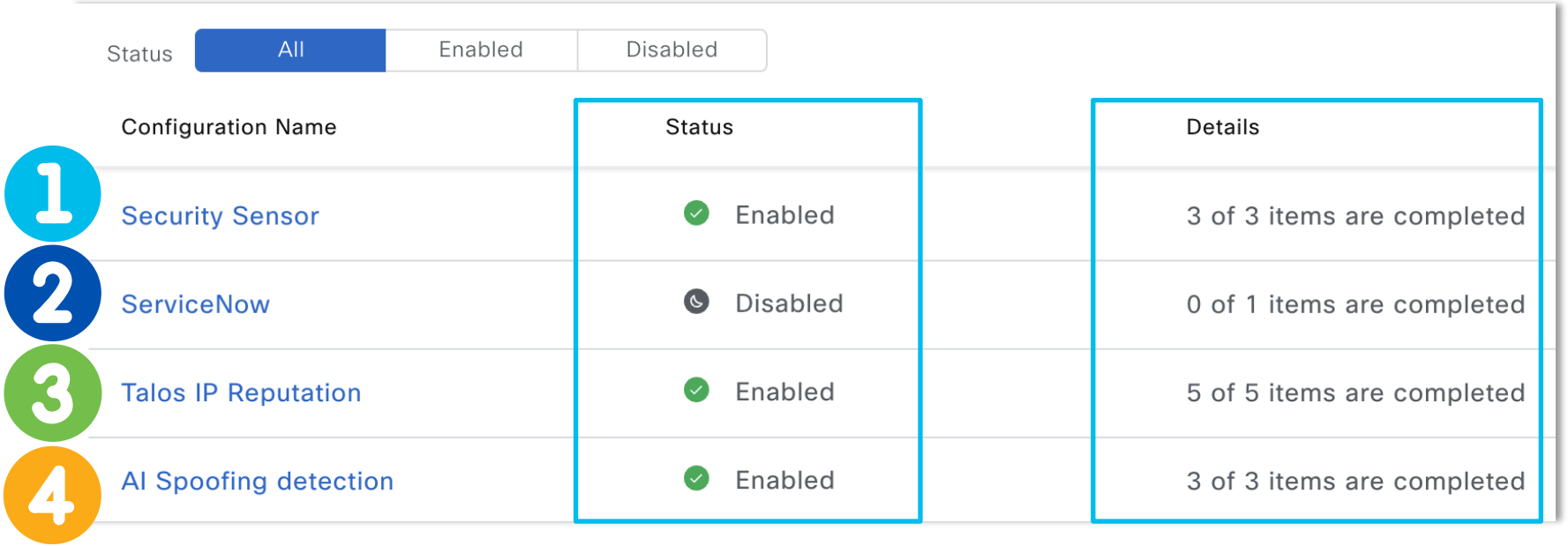
Policy > AI Endpoint Analytics > Overview



EA Overview shows trust score distribution

Optional Configuration Steps to enable EA

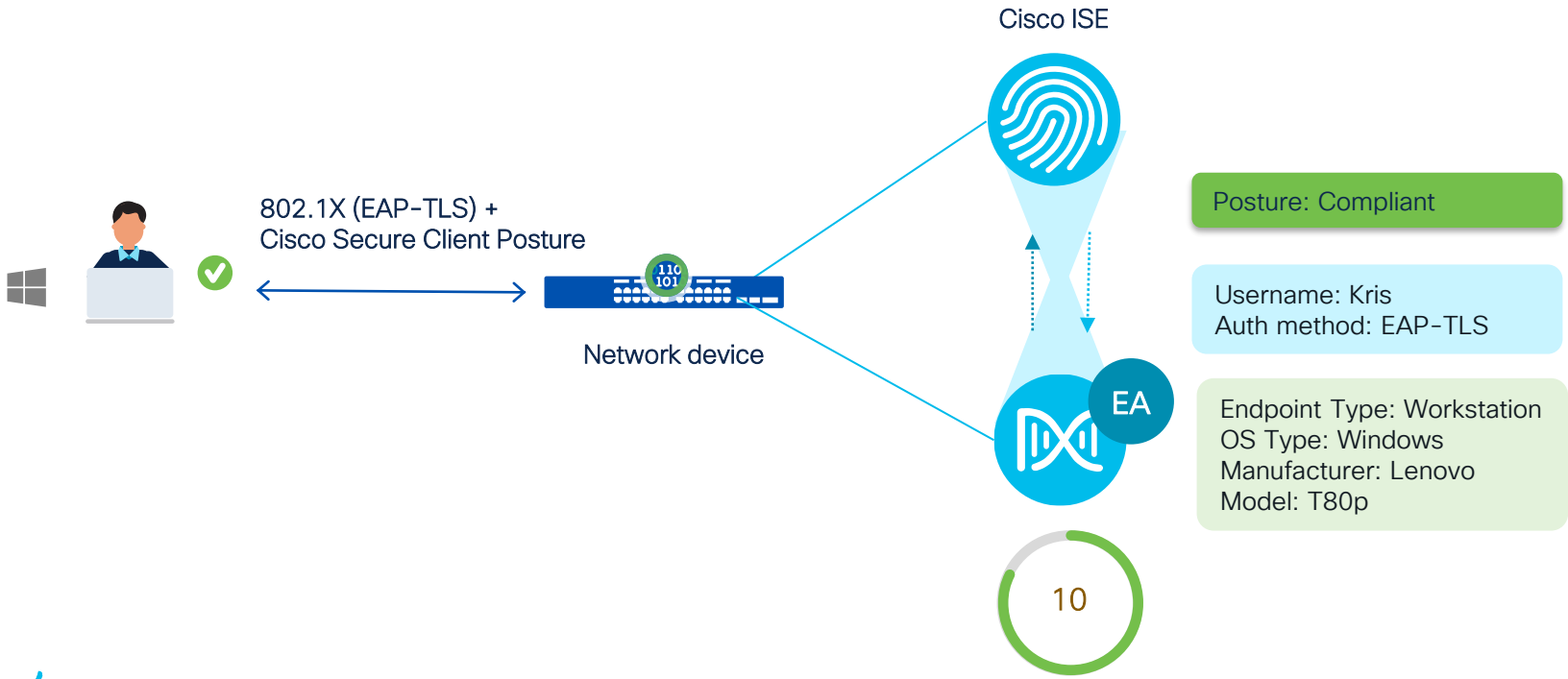
Policy > Endpoint Analytics – Manage Sources – Manage Configurations



After Day 0 setup user can check the status of optional and required configurations for EA

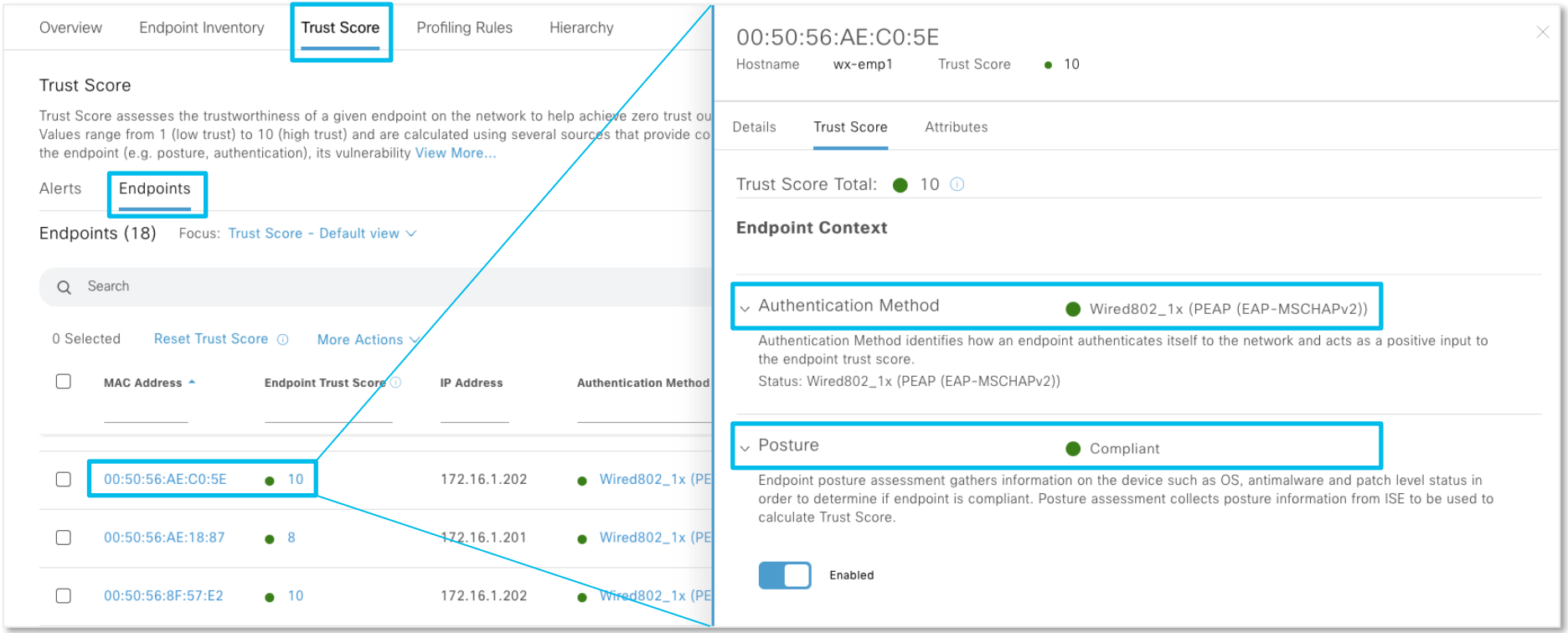
Secure Authentication and Posture Compliance

Positive Influence on Trust Score



Secure Authentication and Posture Compliance

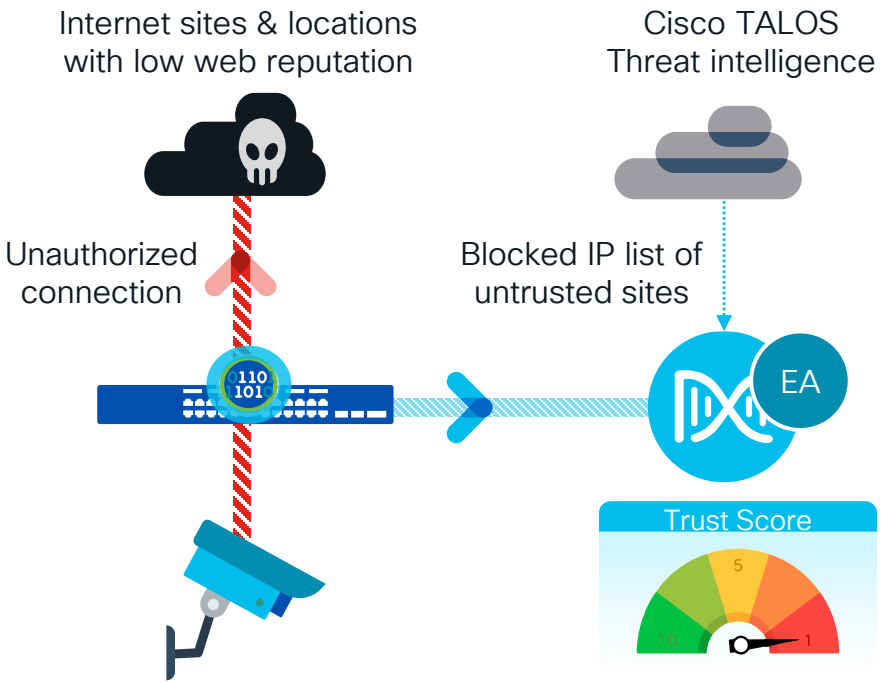
Positive Influence on Trust Score



Low reputation IP connections

Detecting endpoint connections to low reputation sites.

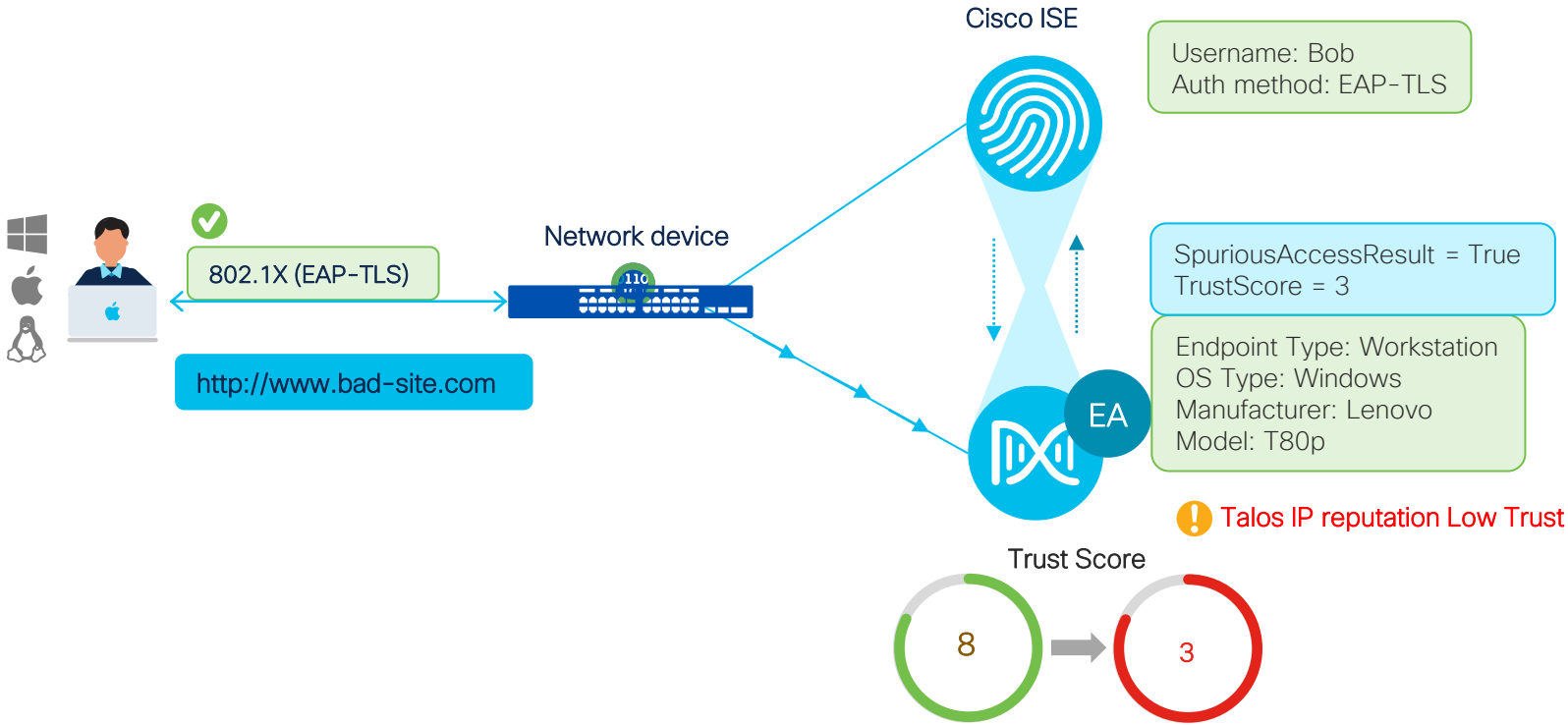
Connected Catalyst



- Catalyst Center pulls IP Reputation data from TALOS
- Application Telemetry enabled via NetFlow configuration on network devices
- Unauthorized connections to bad reputed sites indicates anomalous behavior
- Mitigation via ISE using Adaptive Network Control APIs

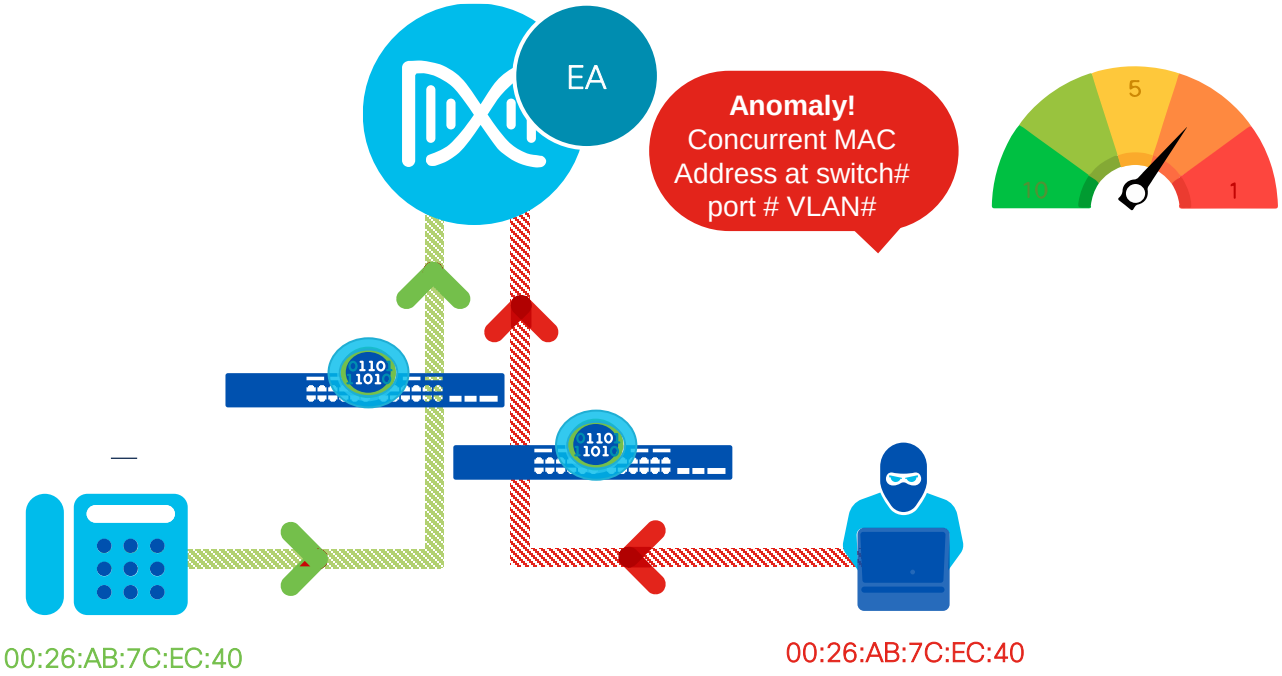
Trust Score changes after anomaly

Negative Influence on Trust Score



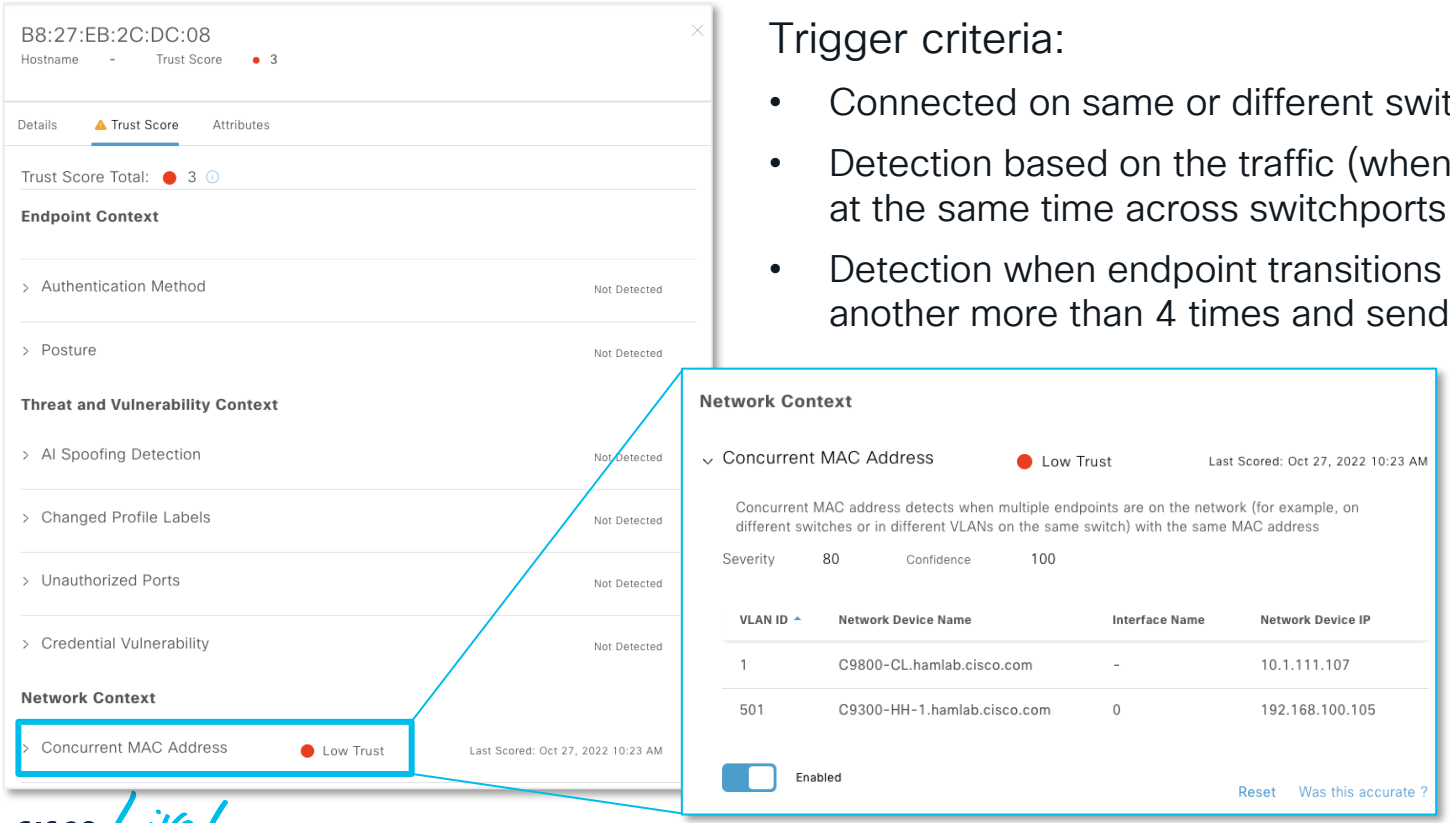
AI Spoofing Detection

Detects concurrent instances of the same MAC address



AI Spoofing Detection

Detects concurrent instances of the same MAC address



Trigger criteria:

- Connected on same or different switches.
- Detection based on the traffic (when endpoint appears at the same time across switchports and sends traffic)
- Detection when endpoint transitions from one port to another more than 4 times and sends traffic

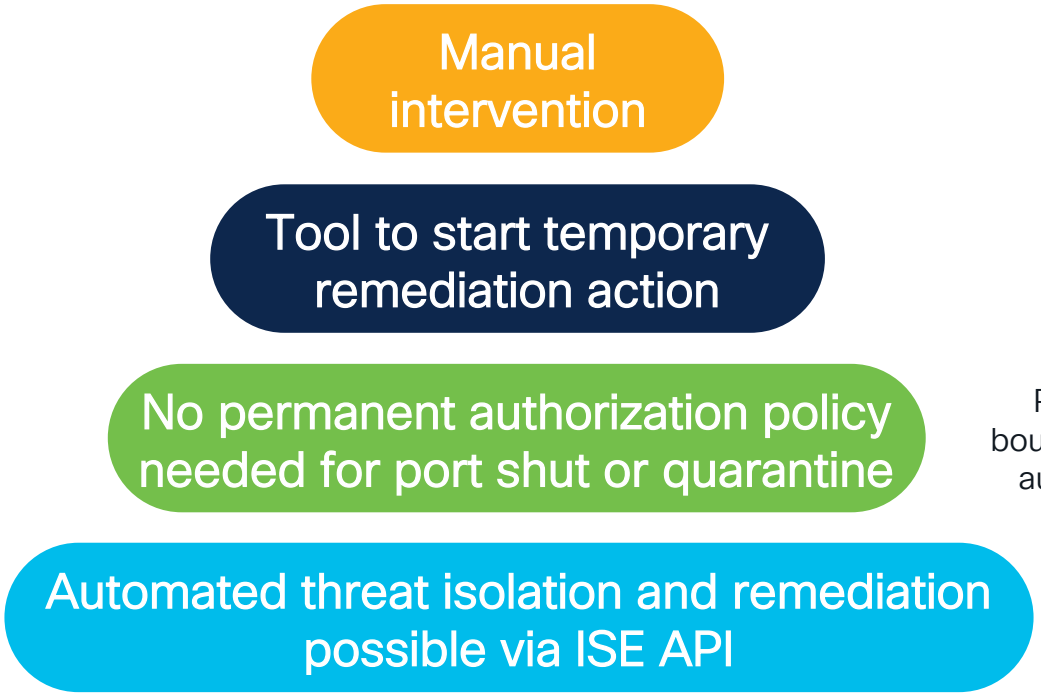
Adaptive Network Control offers four actions

ANC is an additional tool to mitigate risks

Quarantine	Move the endpoint to a quarantine Security Group
Shut Down	Shut down switchport where endpoint is connected
Port Bounce	Cycle switchport where endpoint is connected
Re-Authenticate	Demand the switch to restart authentication process

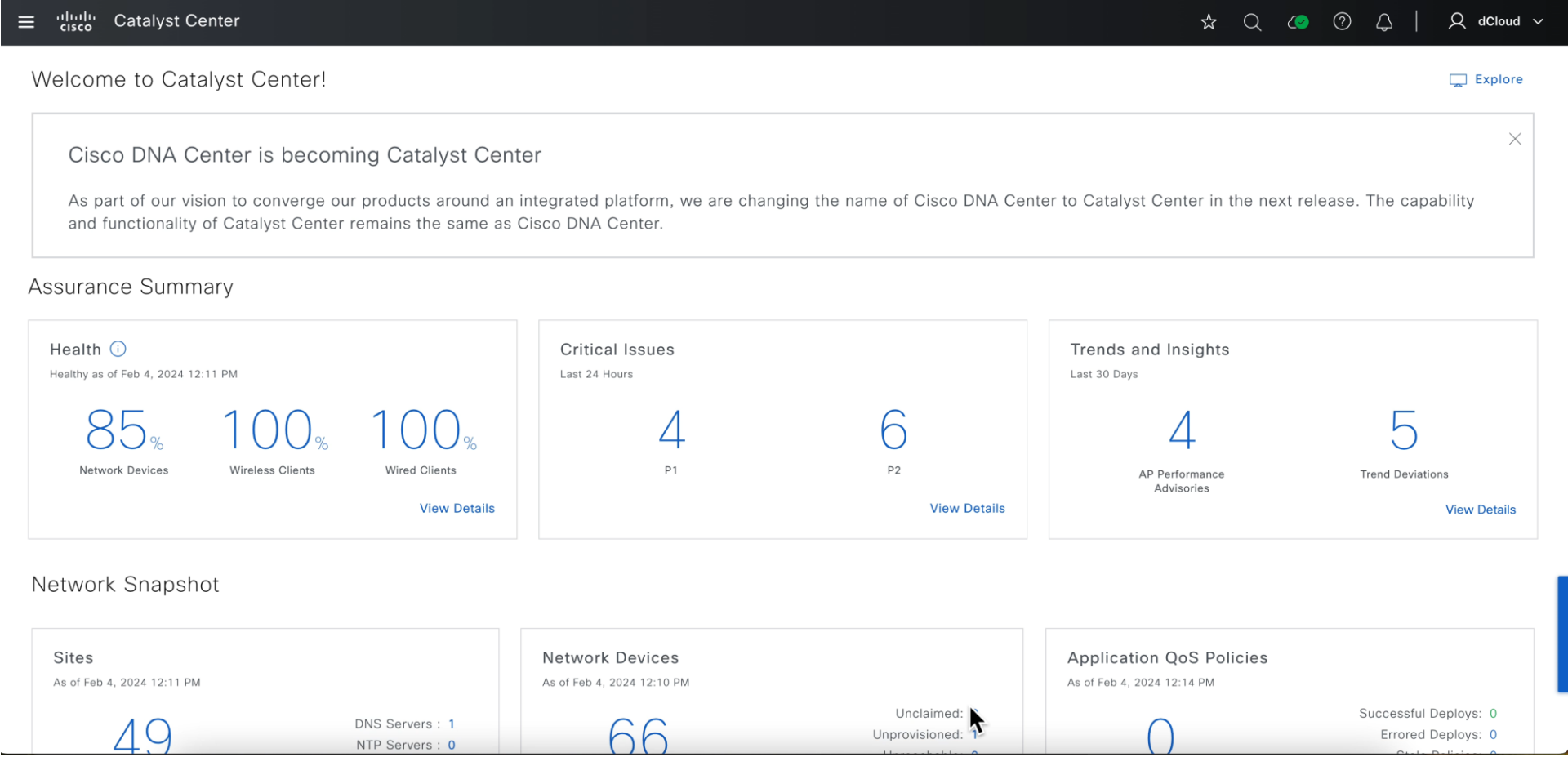
Rapid Threat Containment (RTC) using Cisco ISE

Using Adaptive Network Control (ANC)



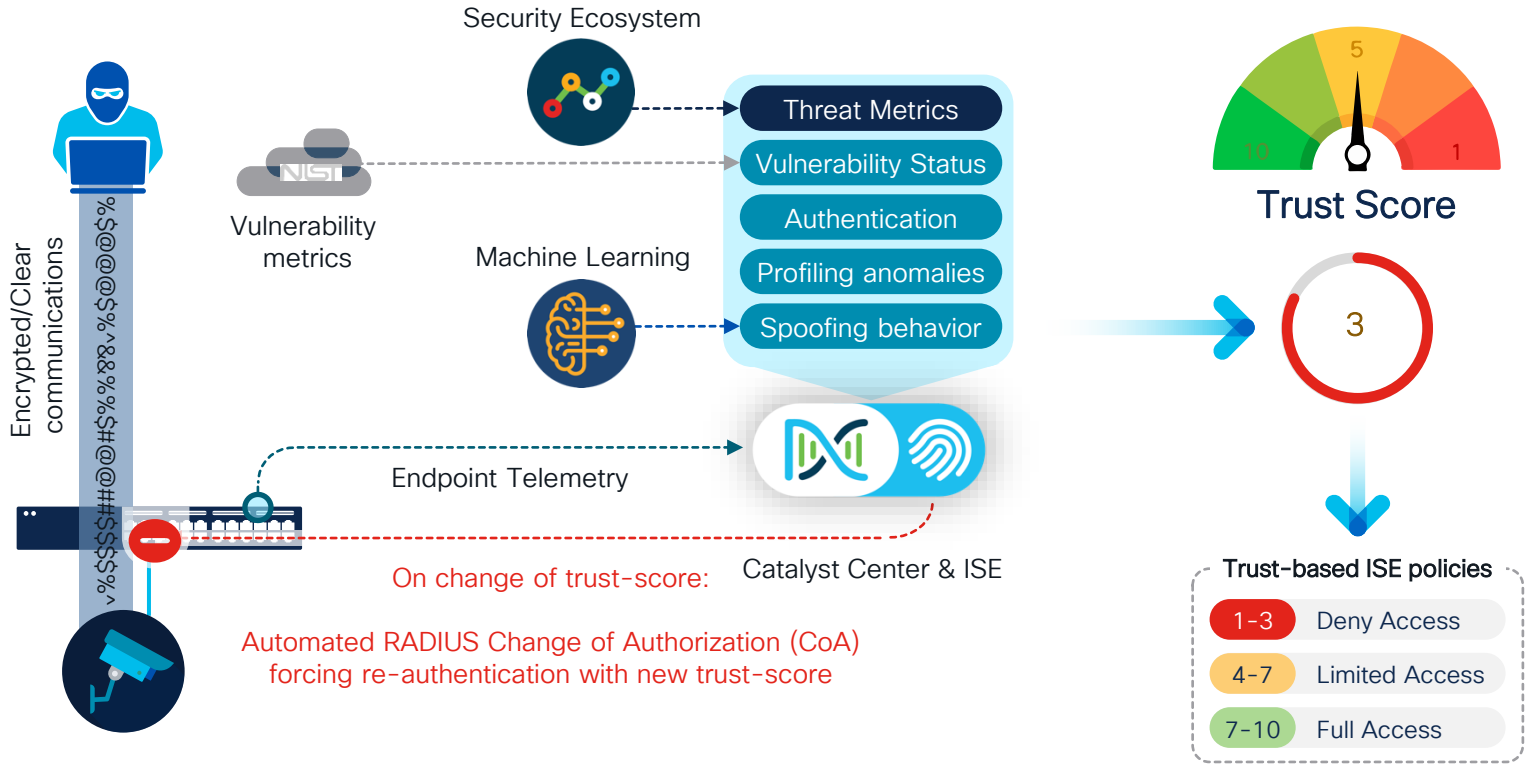
Re-auth and port bounce actions require authorization policy

Demo



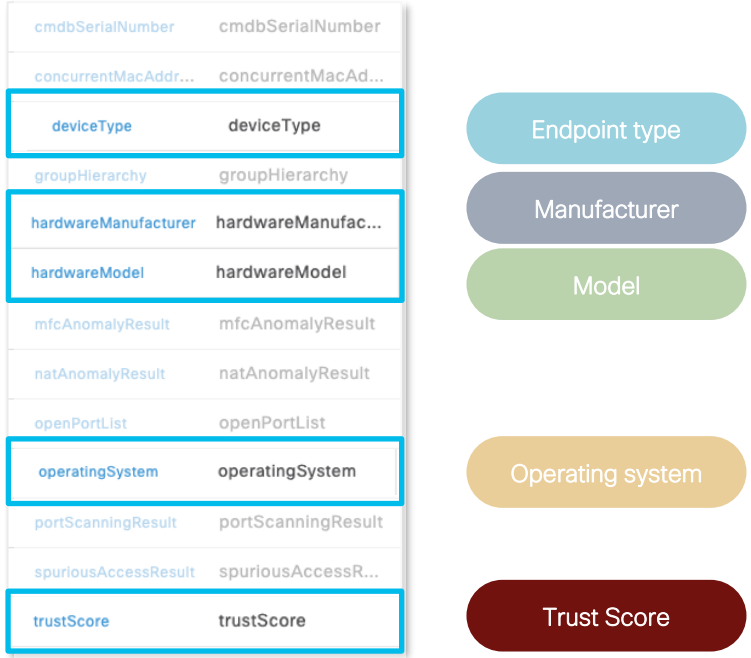
Trust based network access

Continuously monitor anomalies, endpoint trust and restrict access



Endpoint Analytics brings new dictionary to ISE

ISE: Policy > Policy Elements > Dictionaries > System > Endpoint-Analytics



Trust Score available for use in authorization policies

Use Endpoint Analytics attributes in ISE policy

Authorization policy for **HP Printers**:

If
- Endpoint Group: Printer MAC Addresses
- Endpoint Analytics: device type is Printer
- Endpoint Analytics: HardwareManufacturer is HP
- Endpoint Analytics: trustScore greater or equals 6

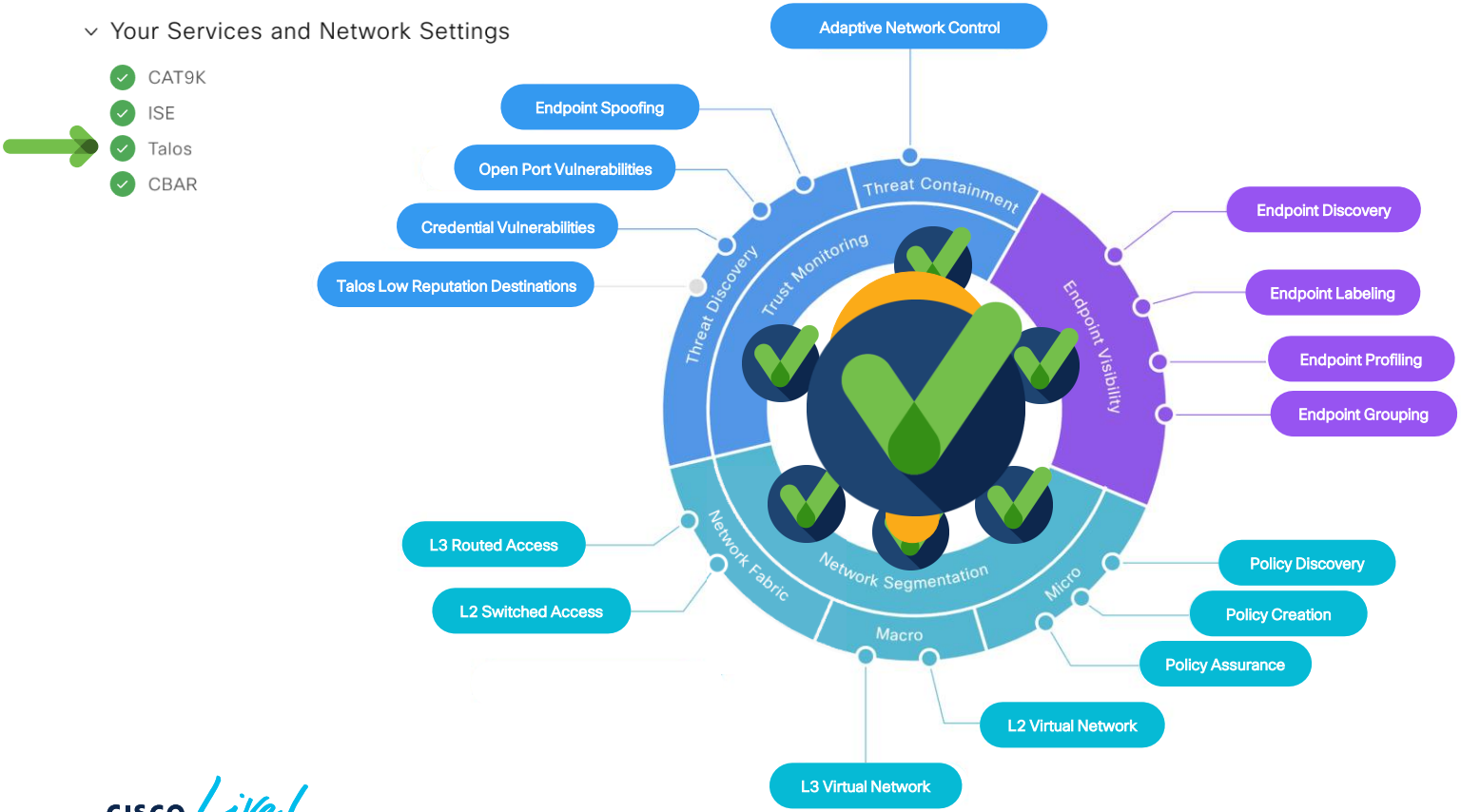
,Then Assign SGT Printer

Authorization policy for untrusted HP **printers**

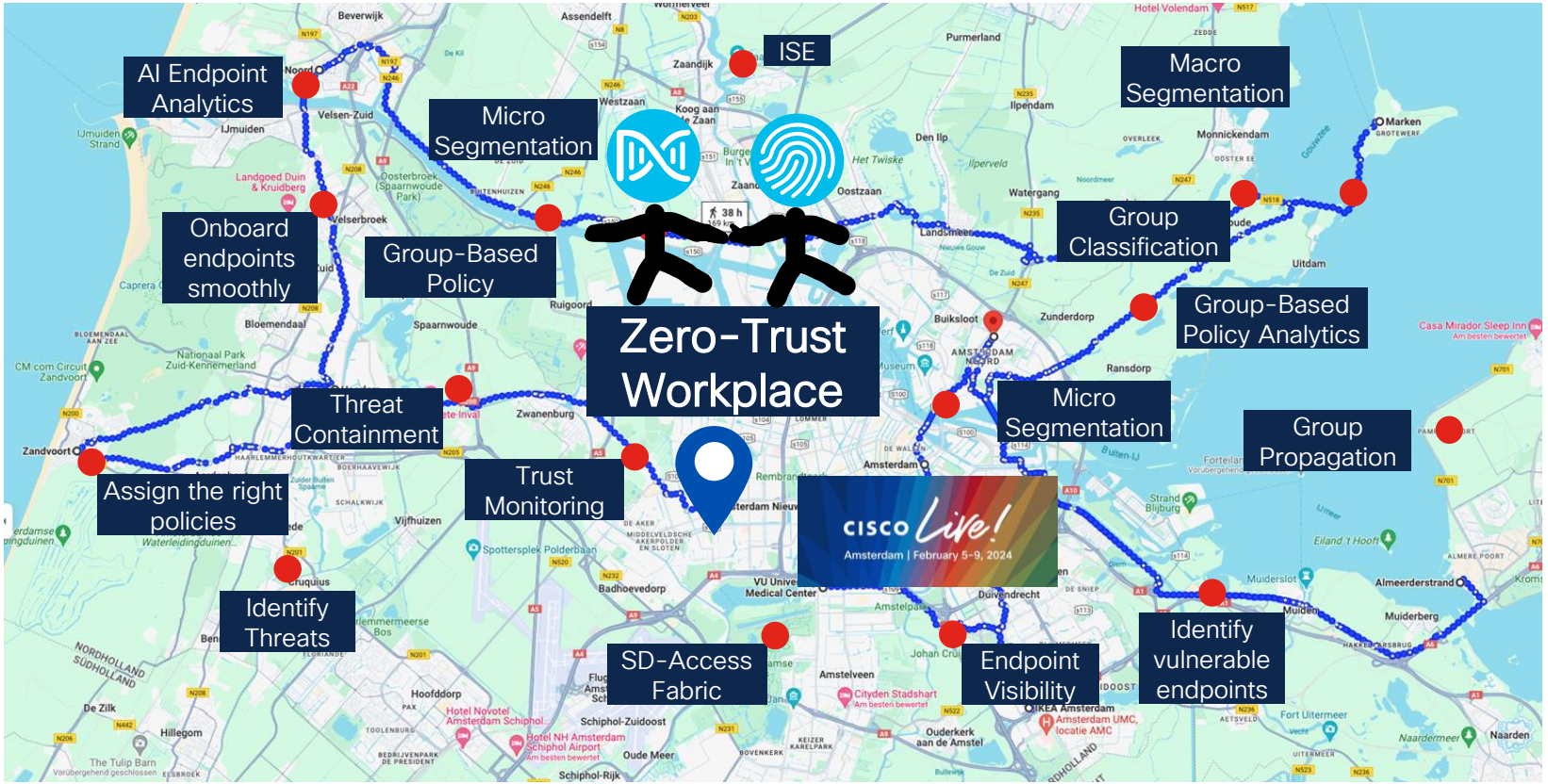
If
- Endpoint Group: Printer MAC Addresses
- Endpoint Analytics: device type is Printer
- Endpoint Analytics: HardwareManufacturer is HP
- Endpoint Analytics: trustScore less than 6

,Then Assign SGT Quarantine

We finished to build a zero-trust campus network



We started our journey with multiple options



We showed you our recommended path today

Endpoint Visibility

- AI Endpoint Analytics
- Group-Based Policy Analytics
- Policy Discovery

Network Segmentation

- SD-Access Fabric
- Multi-level Segmentation
- Endpoint Onboarding

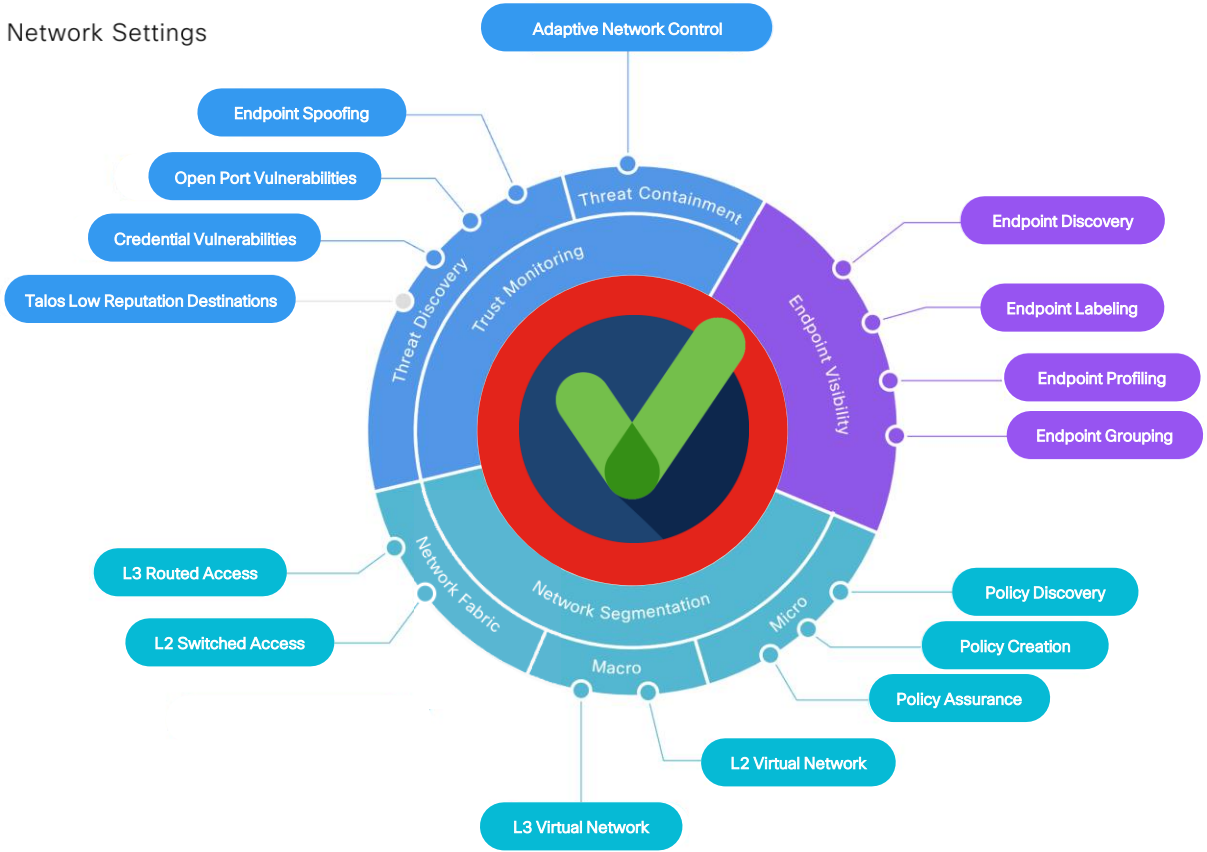
Trust Monitoring

- Trust Score
- Threat Discovery
- Threat Containment

You started your journey today – Keep it going!

Your Services and Network Settings

- CAT9K
- ISE
- Talos
- CBAR



The bridge to possible

Thank you

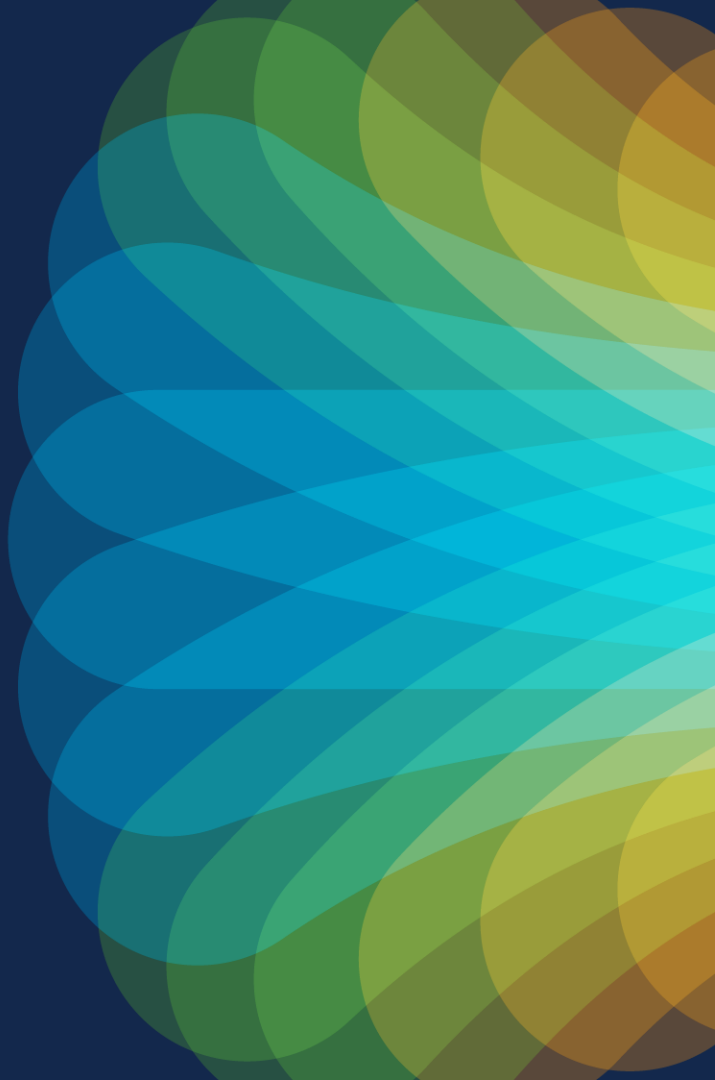
Questions

Enjoy your Lunch

cisco Live!


cisco Live!
Let's go

Additional Resources



Code Recommendations for Endpoint Analytics

As of February 2024

Catalyst Center	Catalyst Center Compatibility Matrix
Catalyst 9000	Recommended Releases for Catalyst 9000 Platforms
SD-Access	Cisco Software-Defined Access Compatibility Matrix
ISE	Catalyst Center User Guide - Cisco AI Endpoint Analytics

Catalyst Center References

Catalyst Center Product Page

https://www.cisco.com/go/dnacenter

Catalyst Center At-A-Glance

https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/dna-center/nb-06-cisco-dna-center-aag-cte-en.html

Catalyst Center Data Sheet

https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/dna-center/nb-06-dna-center-data-sheet-cte-en.html

Catalyst Center Privacy Data Sheet

https://trustportal.cisco.com/c/dam/r/ctp/docs/privacydatasheet/DNA/cisco-dna-center-privacy-data-sheet.pdf

Catalyst Center YouTube Channel

https://www.youtube.com/@CiscoCatalystCenter

Catalyst Center (Physical and Virtual) Resources

https://community.cisco.com/t5/networking-knowledge-base/cisco-dna-center-physical-and-virtual-resources/ta-p/3648009

Catalyst Center Documentation Roadmaps

https://www.cisco.com/c/en/us/support/cloud-systems-management/dna-center/products-documentation-roadmaps-list.html

NBAR2 Protocol Pack Library

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_nbar/prot_lib/config_library/nbar-prot-pack-library.html

AI Endpoint Analytics References

[Introduction: What is AI Endpoint Analytics?]

[Whitepaper: Cisco AI Endpoint Analytics: A New Path Forward]

[Presentation: Advanced Endpoint Visibility with Cisco AI Endpoint Analytics]

[Case Study: Adventist Health]

[Case Study: North Carolina DHHS]

[Blog: Identify Endpoints, Enforce Policies, and Stop Threats with Network Segmentation]

[Video: AI Endpoint Analytics Demo]

[Deployment Guide: Cisco AI Endpoint Analytics]

Cisco ISE & SD-Access References

ISE Webinars
cs.co/ise-webinars

ISE YouTube Channel
cs.co/ise-videos

ISE Resources
cs.co/ise-resources

ISE Community
cs.co/ise-community

ISE Security Integration Guides
cs.co/ise-guides

ISE Compatibility Guides
cs.co/ise-compatibility

Network Access Device Capabilities
cs.co/nad-capabilities

ISE Licensing & Evaluations
cs.co/ise-licensing

SD-Access Product Page

cisco.com/go/sdaccess

SD-Access Ordering Guide

https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/software-defined-access/guide-c07-739242.html

SD-Access Solution Data Sheet

https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/software-defined-access/solution-overview-c22-739012.html

Cisco EN&C Validated Design and Deployment Guides

cs.co/en-cvds

SD-Access TrustSec Allow-List Model (Default Deny)

https://www.cisco.com/c/en/us/support/docs/cloud-systems-management/dna-center/215516-trustsec-whitelist-model-with-sda.html


cisco Live!
Let's go