

The background features a vibrant, abstract design with a color gradient from dark blue on the left to bright yellow and white on the right. The design consists of overlapping, wavy horizontal bands and a series of radiating lines that create a sense of motion and energy, resembling a stylized sunburst or a dynamic wave pattern.

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 diagram illustrates a network security and management strategy for Amsterdam, featuring a map with various locations and overlaid text boxes representing different security concepts. The map shows a blue route with red dots and blue location pins. Overlaid text boxes include:

- AI Endpoint Analytics
- Onboard endpoints smoothly
- Threat Containment
- Assign the right policies
- Identify Threats
- Micro Segmentation
- Group-Based Policy
- Trust Monitoring
- SD-Access Fabric
- Endpoint Visibility
- Identify vulnerable endpoints
- Group Classification
- Group-Based Policy Analytics
- Group Propagation
- Macro Segmentation
- ISE

The map also features images of Amsterdam beer cans (Detonator, Navigator, Maximator) and a plate of food.

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

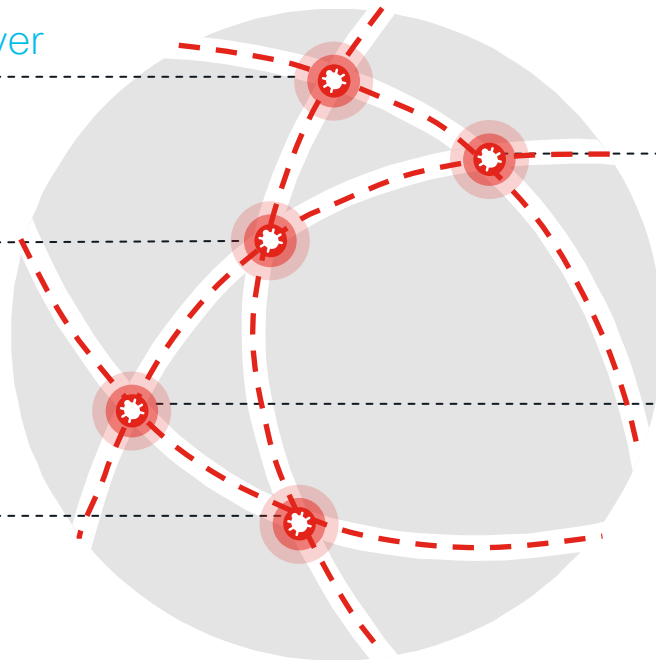
Loss of access control

Multi-cloud reality

Gaps in visibility

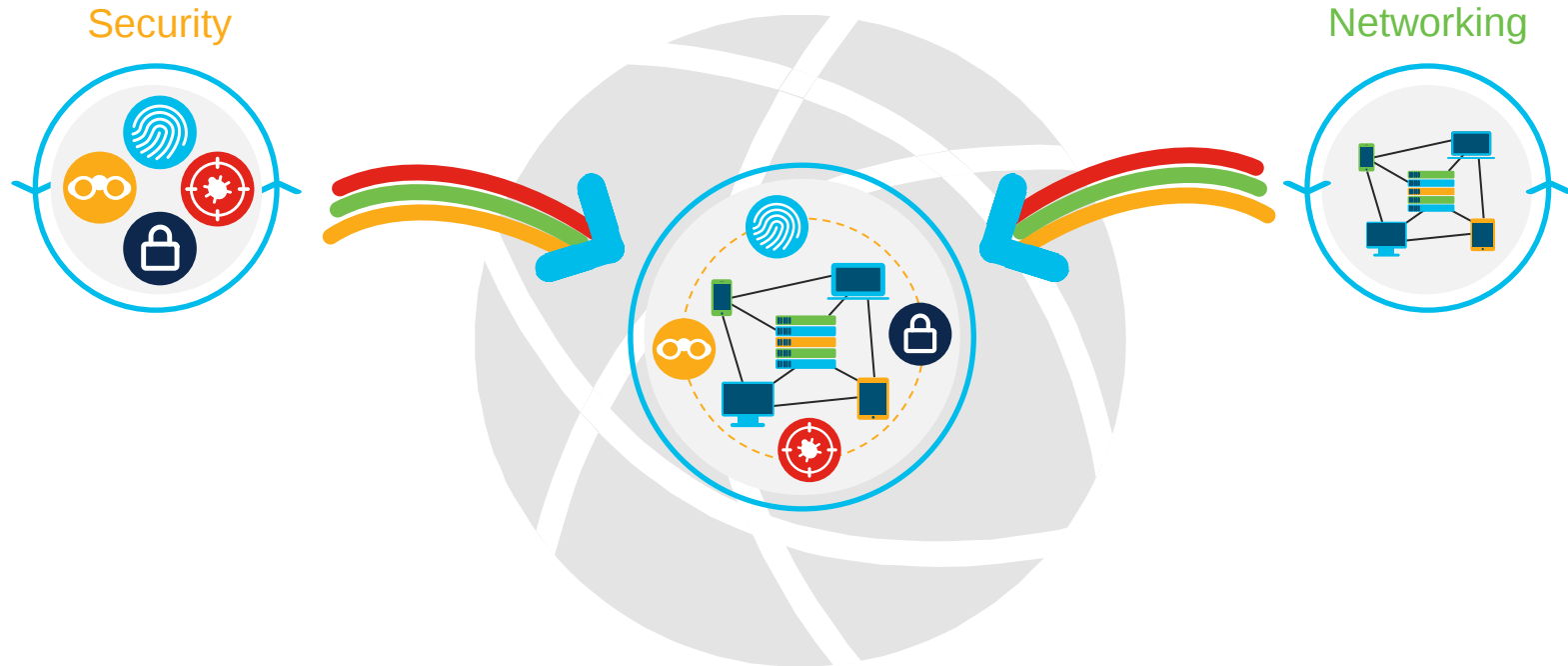
Rapid innovation

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

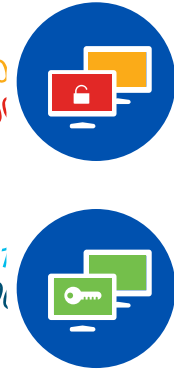
Identify who and what
is on the network



Understand how
they're communicating

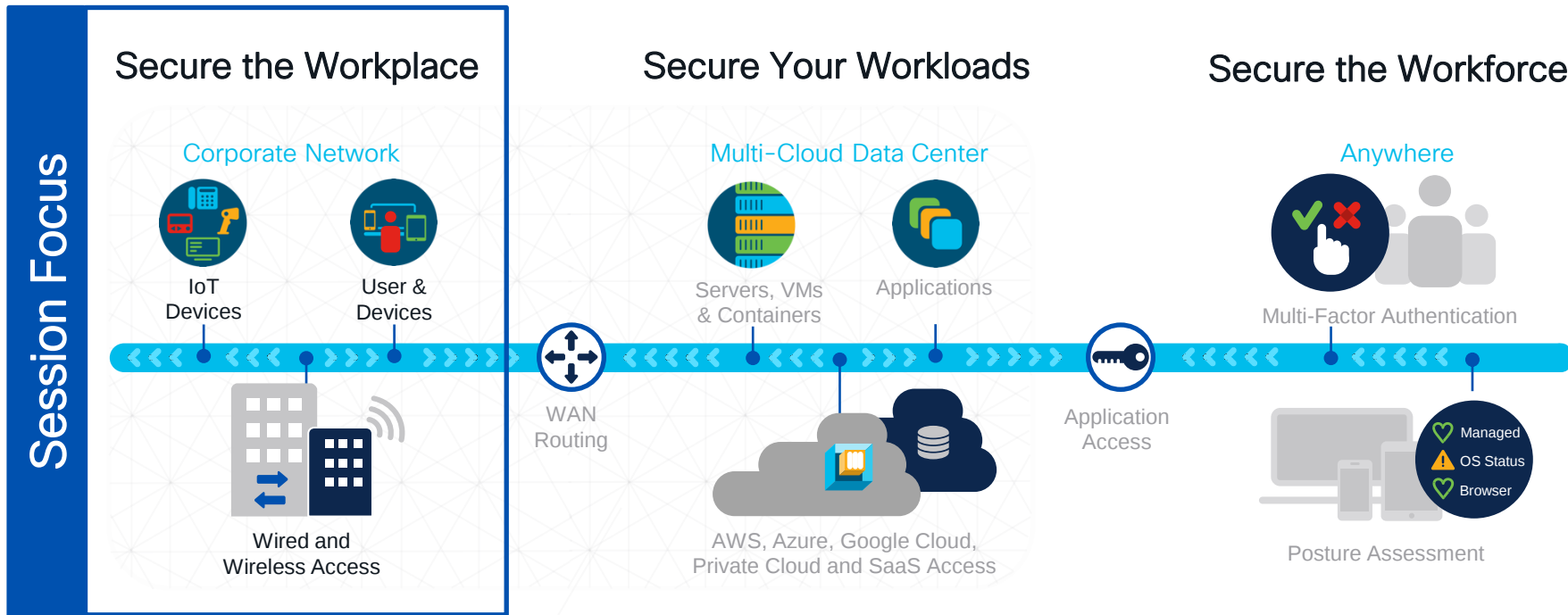


Determine risk profile
and compliance



Zero-Trust Network Access

Use segmentation and verification to proactively stop breaches



Constant Protection

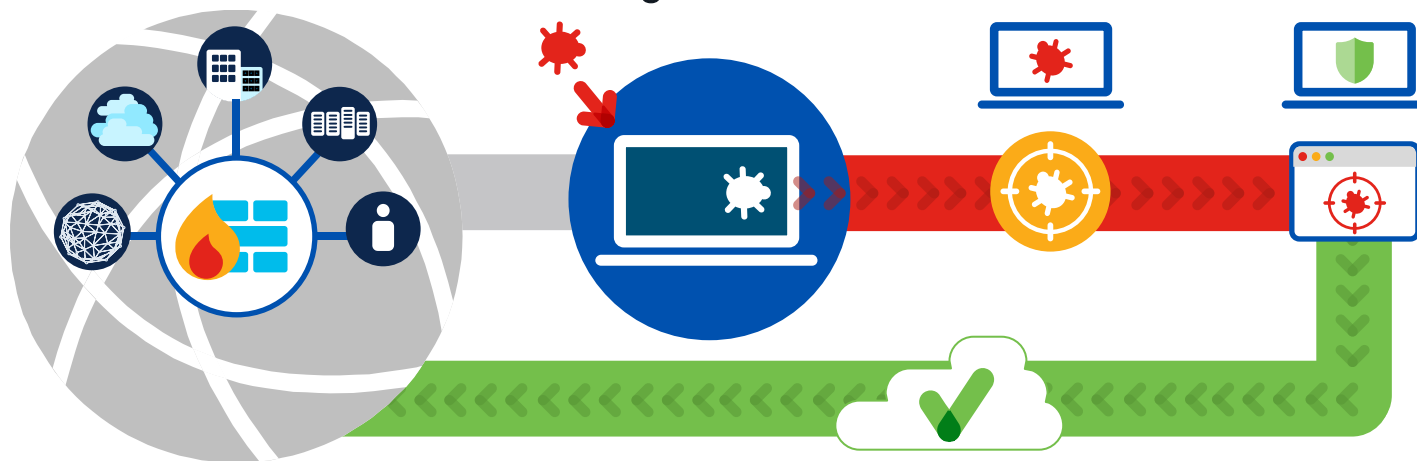
Stop chasing threats - identify risks and vulnerabilities through automation

Most effective prevention
across the network

If malware
gets in

Shortest time
to detection

Shortest time
to remediation



Threat prevention



Threat detection



Threat response

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

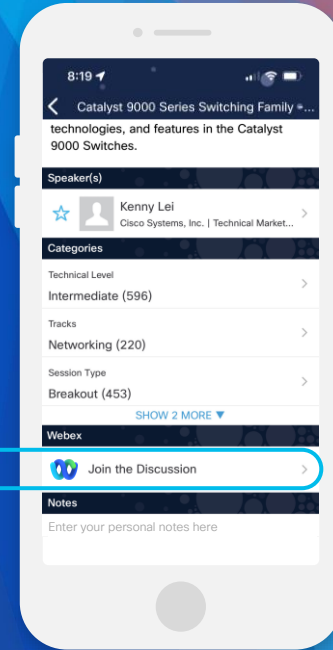
Questions?

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.



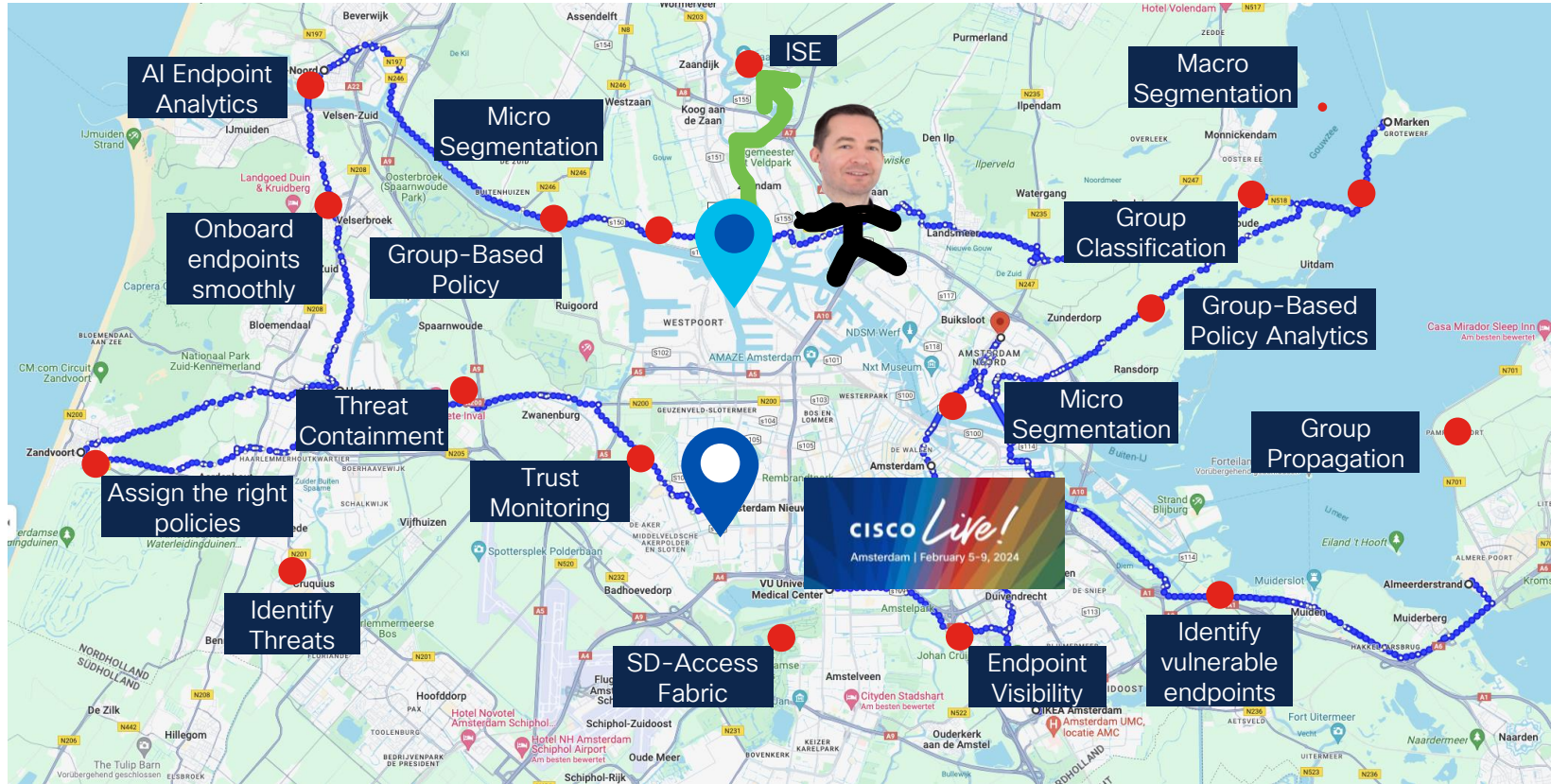
<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKOPS-2683>

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!

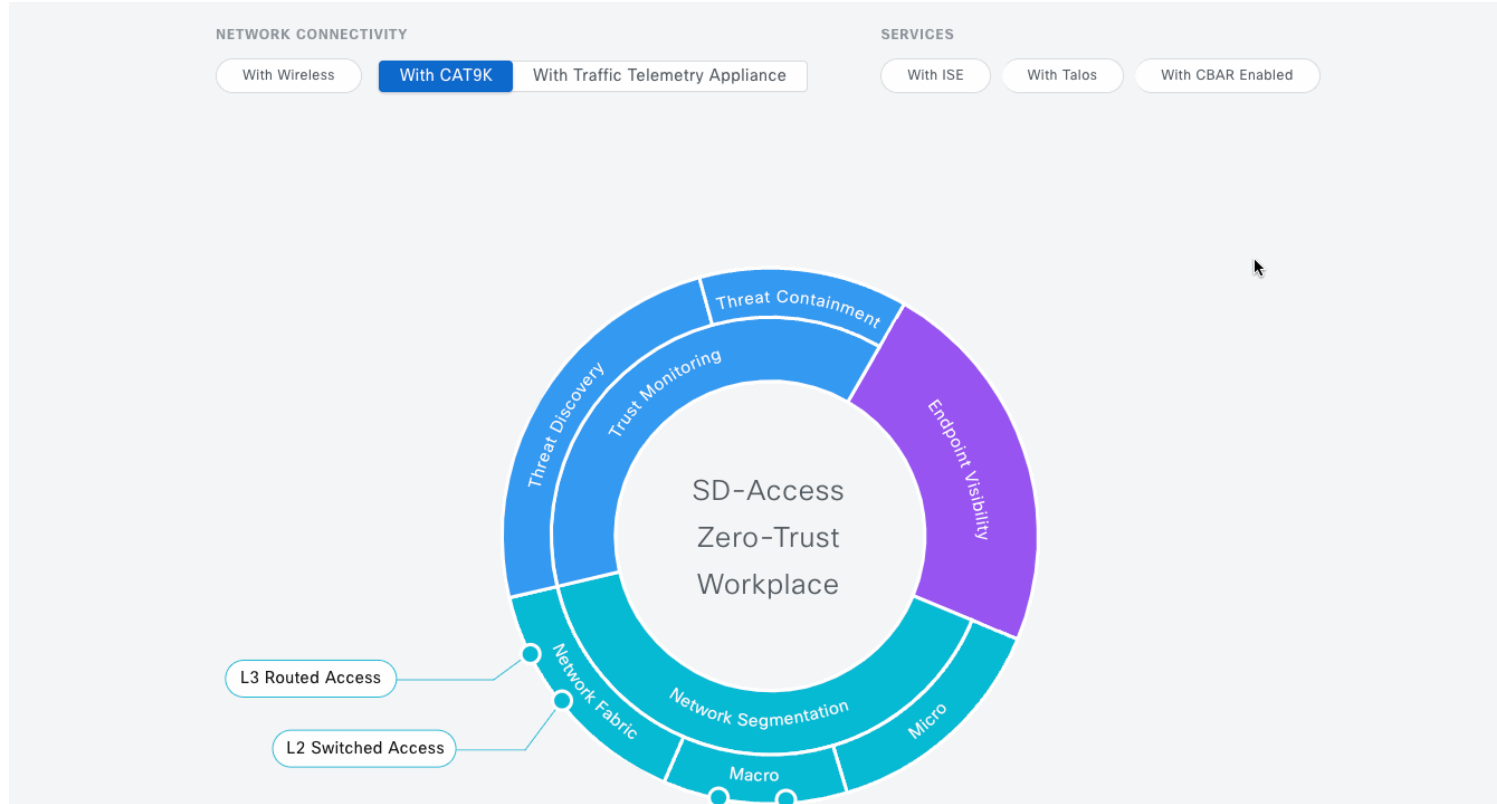


Catalyst Center guides your journey to zero-trust

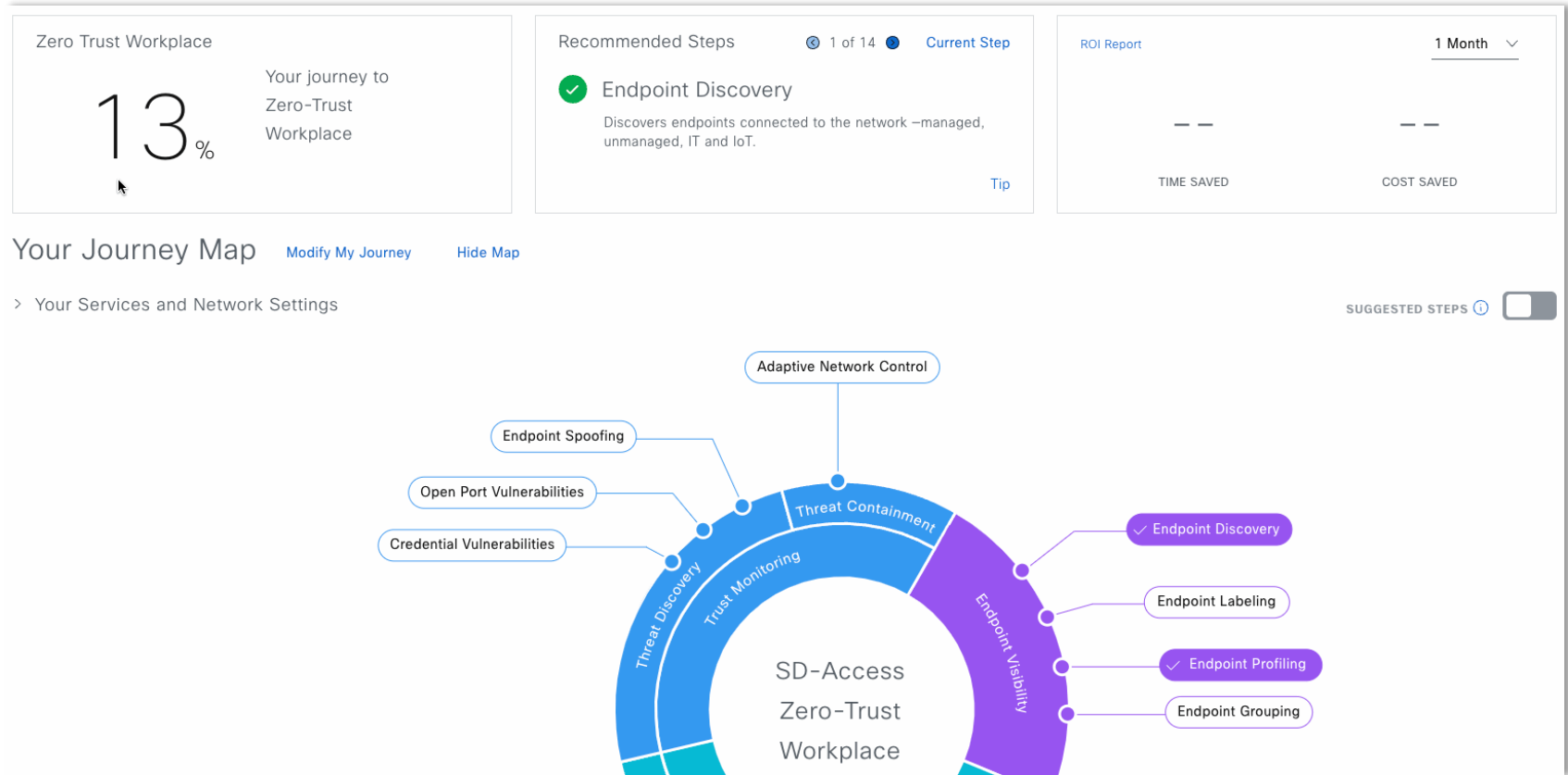
Zero-Trust Journey Map



Select the components of your journey



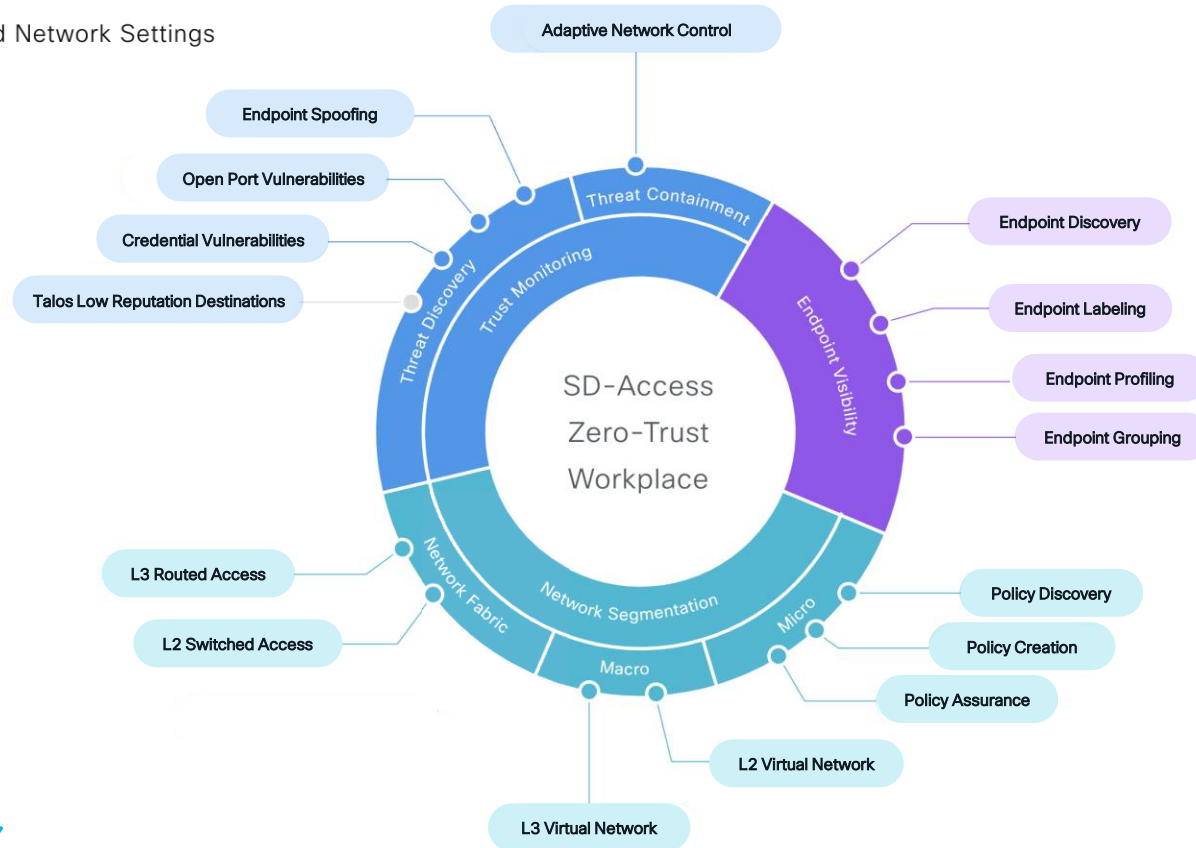
Explore the status of your journey



Start your journey to zero-trust workplace

✓ Your Services and Network Settings

- ✓ CAT9K
- ISE
- Talos
- CBAR



Everyone needs a best friend to share things



The bridge to possible



context

trust

network devices

interests

policies

secrets

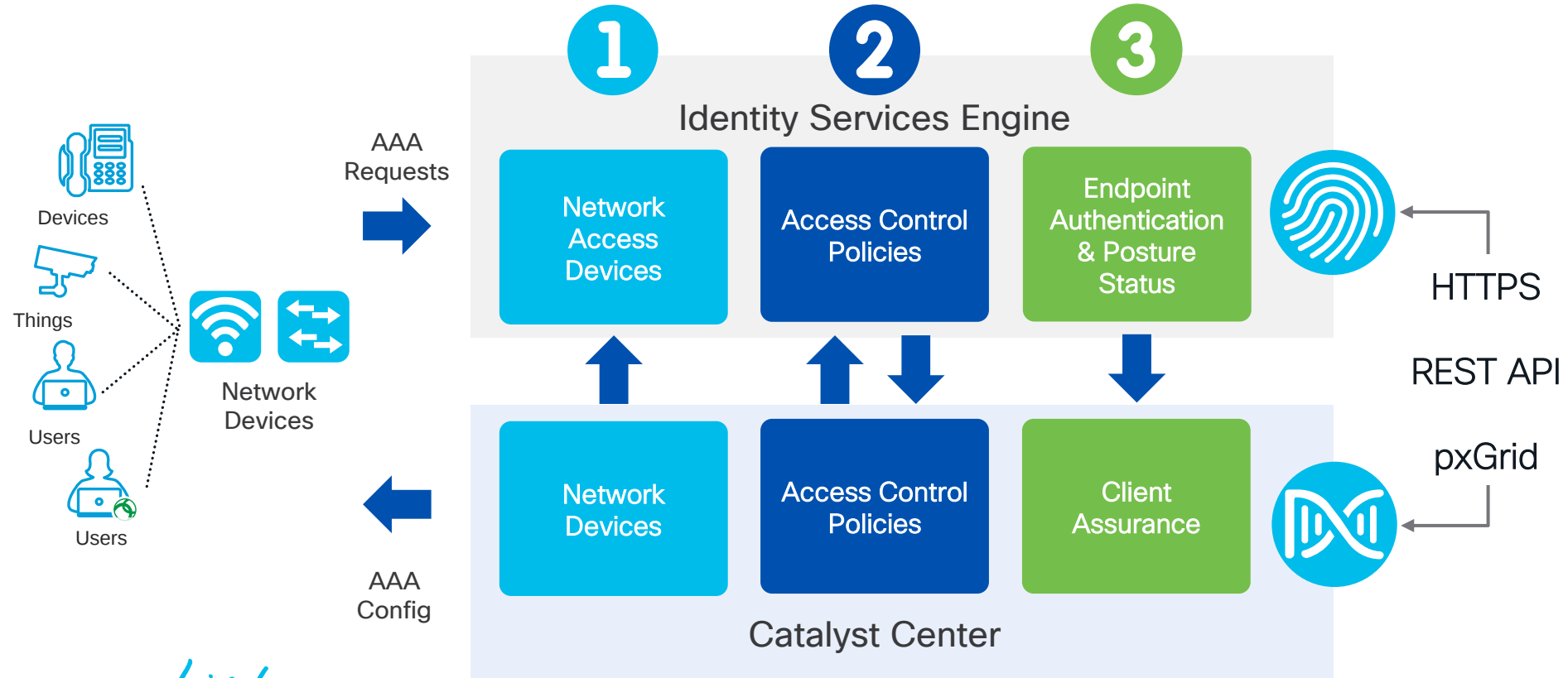
endpoint
visibility

workload

status

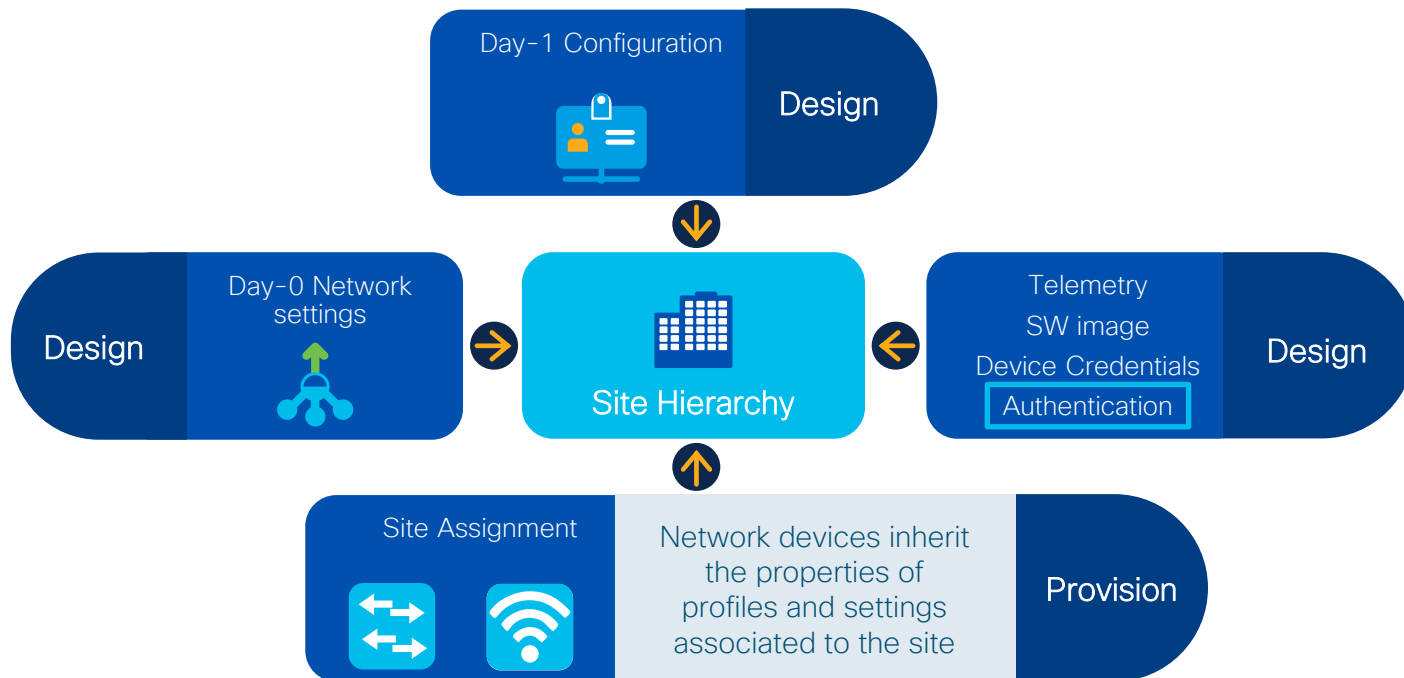
Best friends share workload

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



Servers | Device Credentials | IP Address Pools | Wireless | Telemetry | Security and Trust

Find Hierarchy Search Help

Global

- CLEUR24
- DEU
- CLEUR
- MUC
- MUC07** (4th)

inheritance

AAA (Success)

Configure external network servers, assign time zones to sites, and custom system will deploy these settings when devices are provisioned.

Select AAA or Cisco Identity Services Engine (ISE) servers for network,

Network Access Control

Network | **Client/Endpoint**

☒ Add AAA servers

Server Type

☒ ISE ☐ AAA

Protocol

☒ RADIUS ☐ TACACS

ISE PAN

PAN*

10.49.147.166

ISE PSN 1

Primary Server*

10.49.147.166

ISE PSN 2

Secondary Server*

10.49.147.167

Provision Device

Task • admin • PROVISION

Completed • Success

Start	Feb 5, 2024 9:11 AM
Update	Feb 5, 2024 9:12 AM
End	Feb 5, 2024 9:12 AM

03-FIAB.munlab.

08/MUC08



Provision

Network Settings

NTP Server: 10.49.144.1, 173.38.201.115

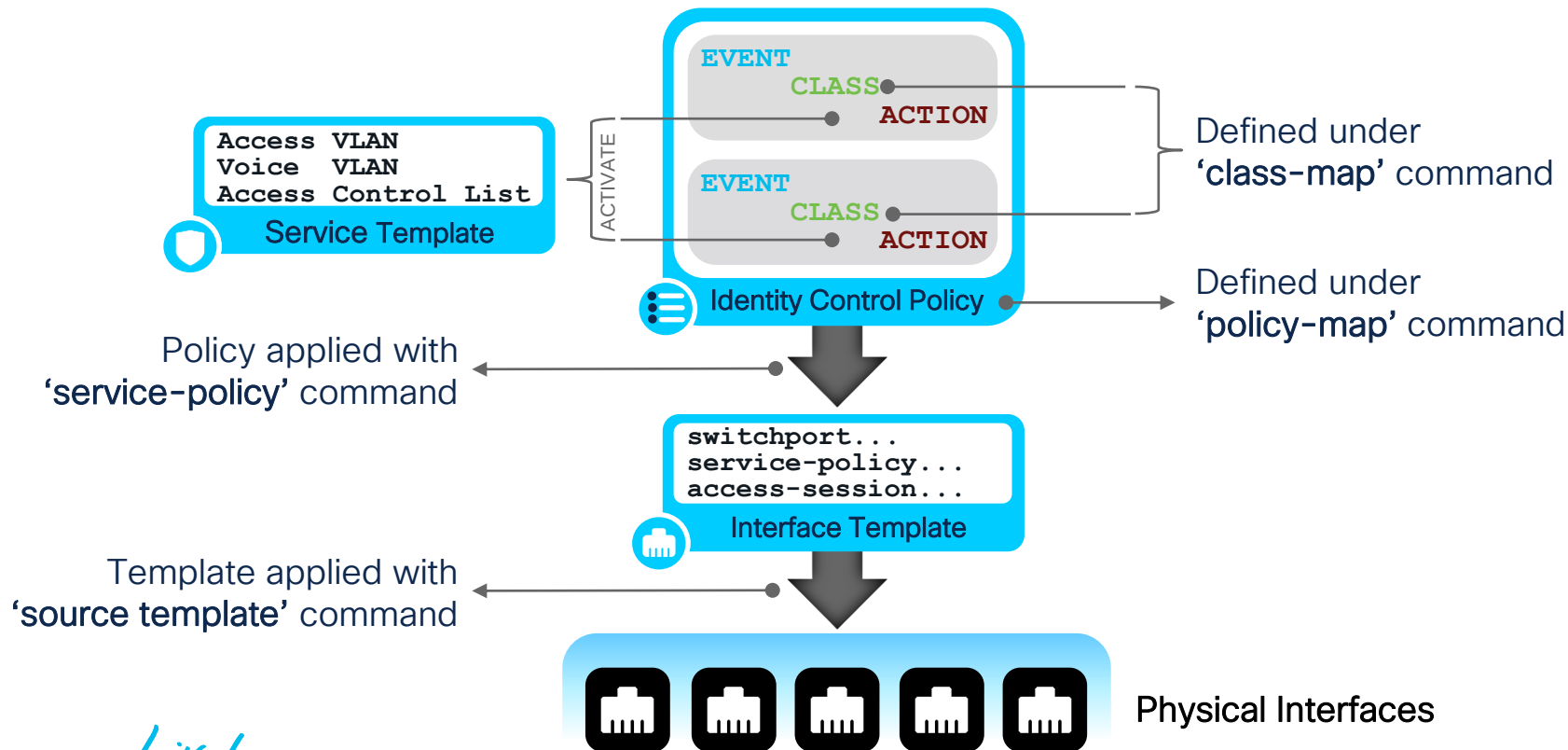
AAA Client ISE Server 10.49.147.166

AAA Client 10.49.147.166 (RADIUS) Primary Server:

AAA Client 10.49.147.167 (RADIUS) Secondary Server:

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



Event

Class

Action

Identity Control Policy

session-started

always

authenticate via 802.1X

AAA-DOWN

Terminate 802.1X

authorize port

authentication-failure

FIRST

NO-RESPONSE

Assign GUEST VLAN

1X-FAIL

Assign FAIL VLAN

ALL

```
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?

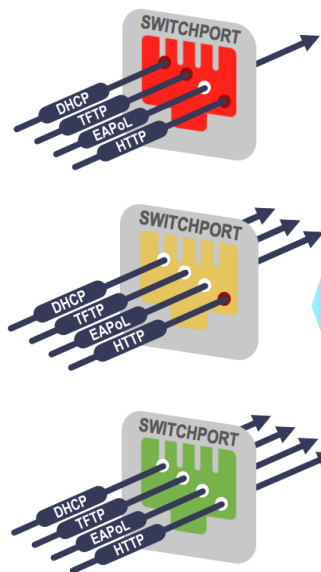
potential for typos

platform and code dependencies



The easy way: SDA Authentication Templates

Templates for each phase of policy rollout



Closed Authentication

Deployment Mode	Closed
First Authentication Order	☒ 802.1x ☐ MAC Auth
802.1x to MAB Fallback (in seconds)	21 3
Wake on LAN	☒ Yes ☐ No
Number of Hosts	☐ Single ☒ Unlimited

```
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

Low-Impact

Open

no access before authentication

limited access before authentication

network access always authorized

Visibility and Control

Visibility only

CISCO Live!

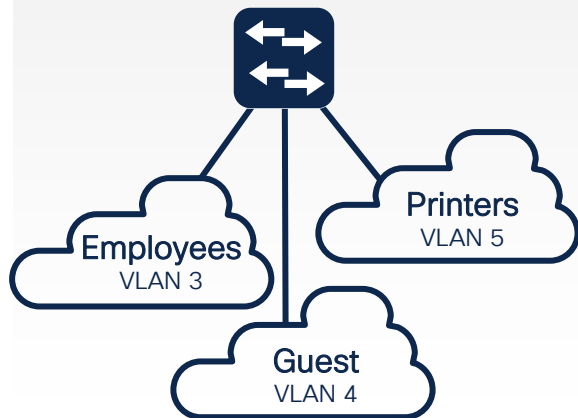
What are our authorization enforcement options?

Beyond RADIUS Access-Accept / Access-Reject



VLANs

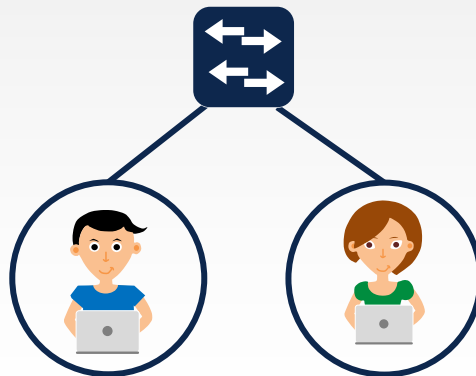
Dynamic VLAN Assignment



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

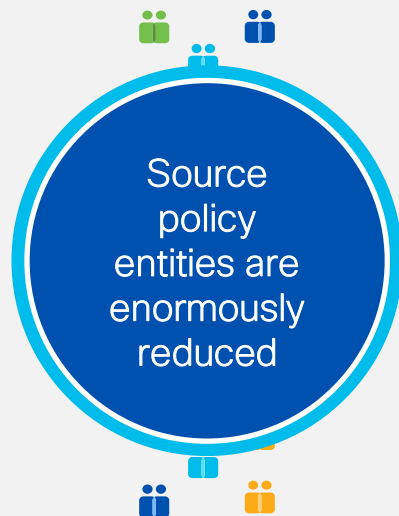
Topology independent

The Value of Group-Based Policies (GBP)

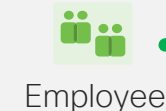
Enhanced simplicity for better enforcement and management



Individual users in workplace



Sample user groups



Employee



Partner



Contractor



Guest

Sample server groups



Company confidential



NDA Confidential



Sensitive



General access



Individual workloads



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
- 2 Automation of AAA Config
- 3 Identity Control Policy
- 4 Group Based Access Control
- 5 Context Sharing



Connected ISE



Pushed AAA



Controlled access



Grouped endpoints



Shared context

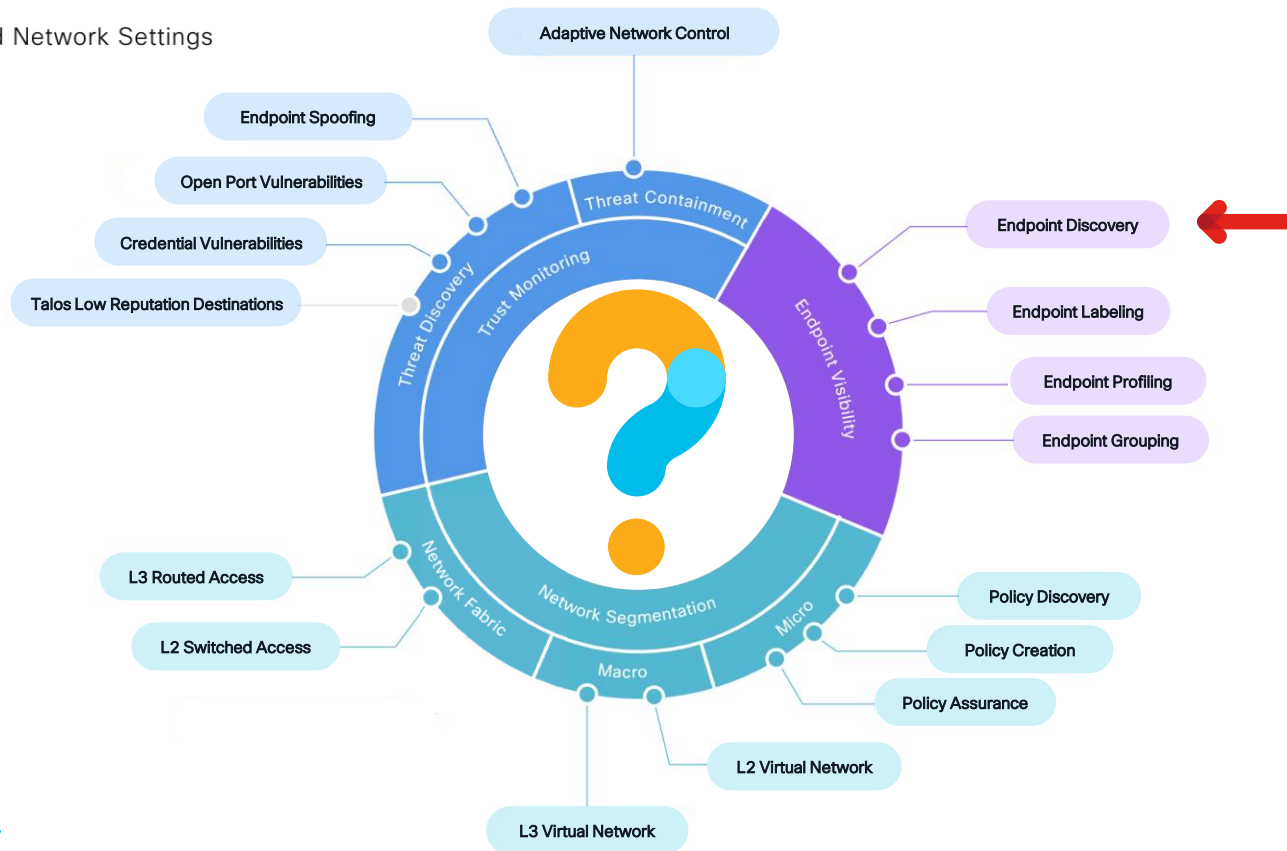


We integrated ISE into Catalyst Center



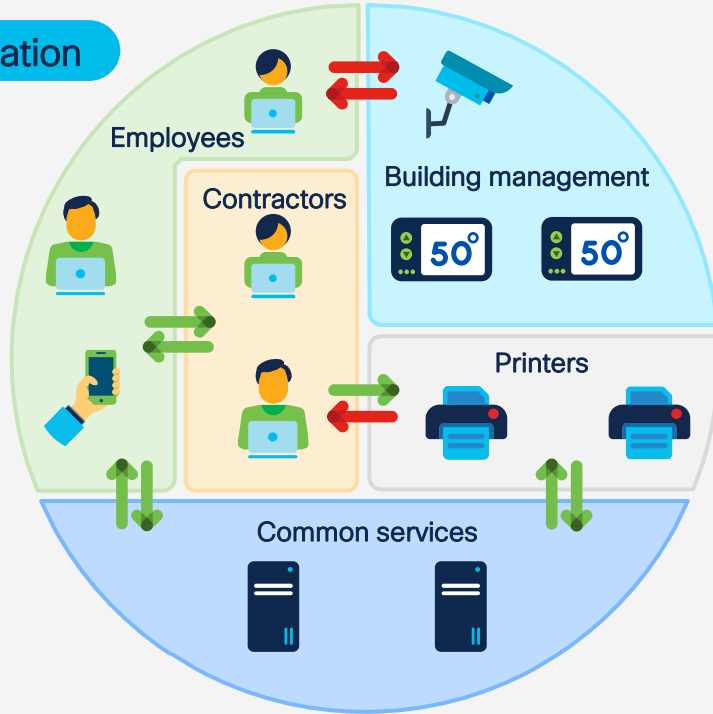
✓ Your Services and Network Settings

- ✓ CAT9K
- ✓ ISE
- ☾ Talos
- ☾ CBAR

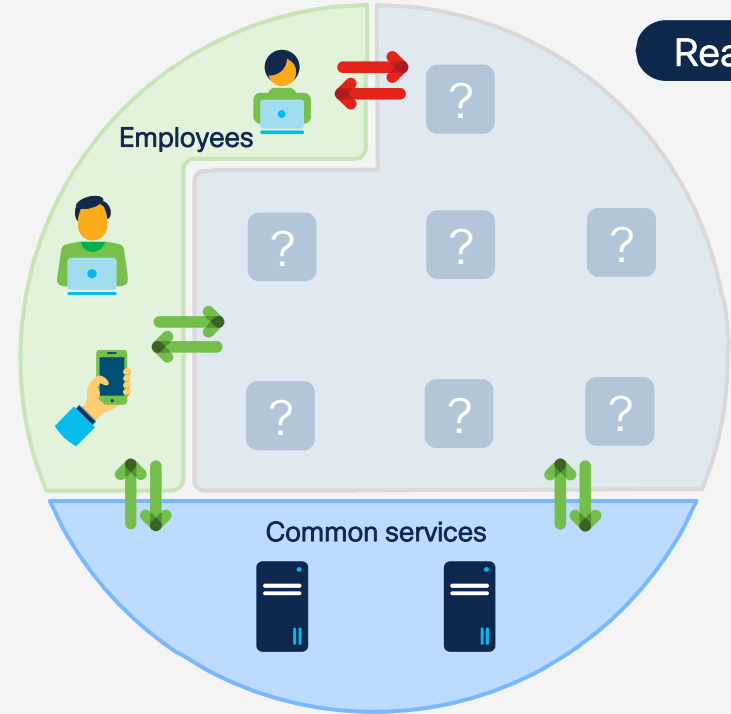


Do we really know all endpoints in our network?

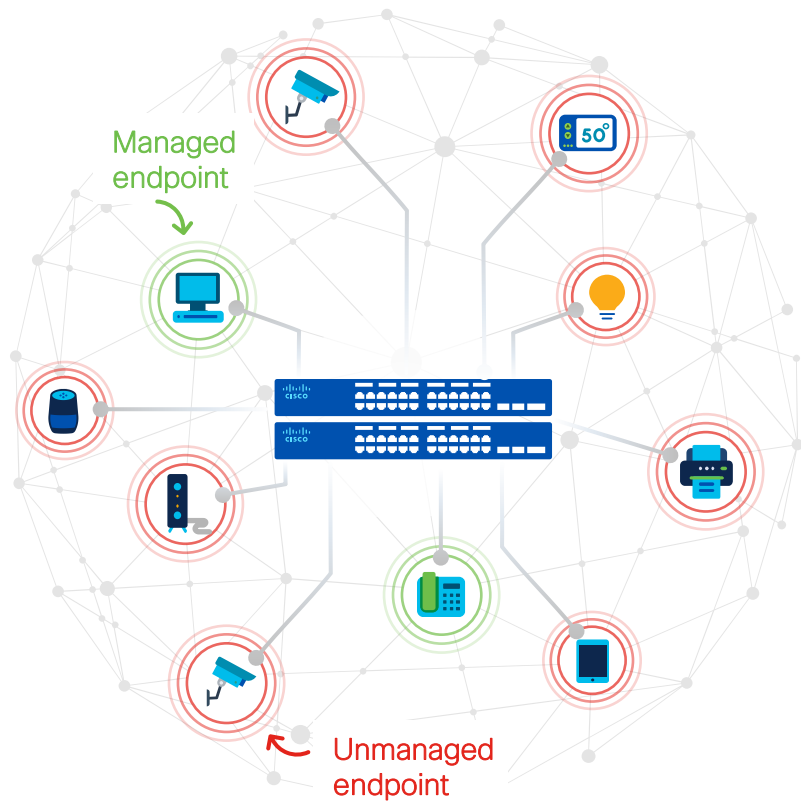
Expectation



Reality



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.

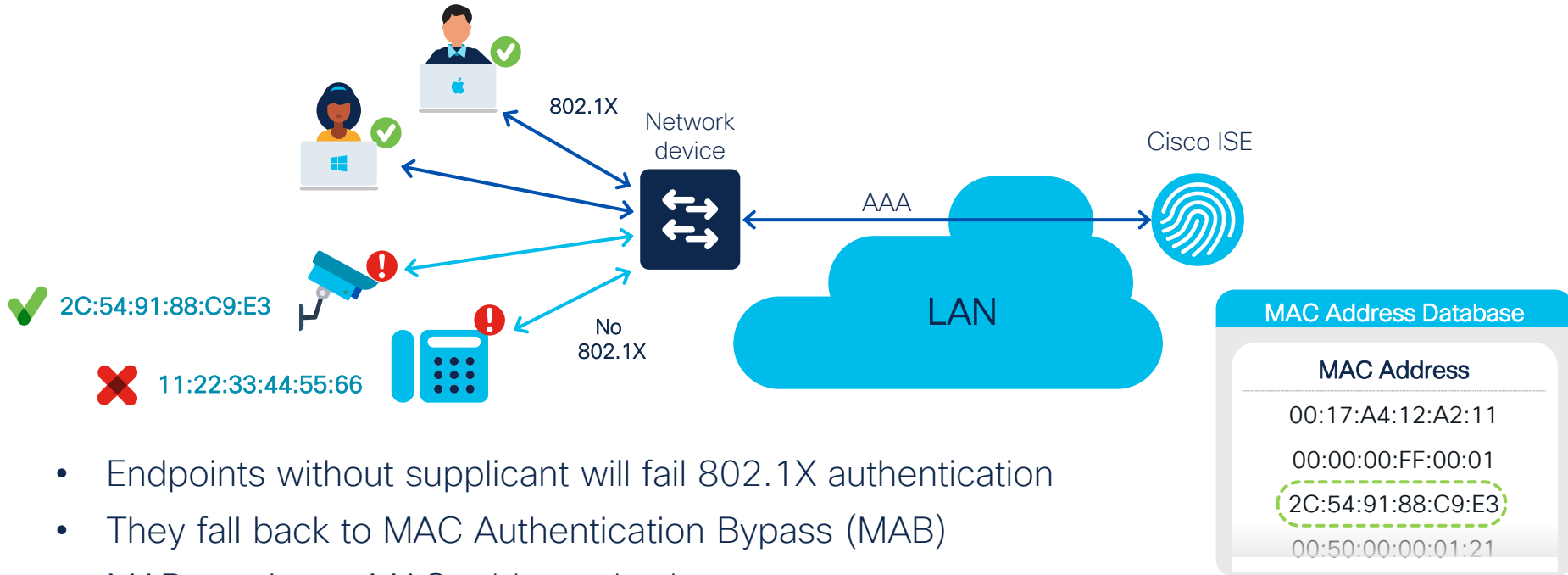


Secure authentication mechanisms
unusable on unmanaged endpoints



Open, unsegmented networks with IOT
devices put organizations at risk

Authentication of unmanaged assets is insecure

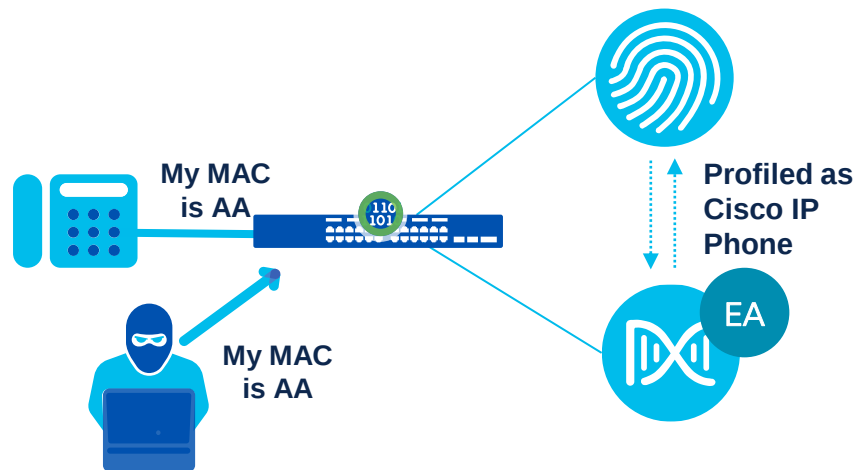


- Endpoints without supplicant will fail 802.1X authentication
- They fall back to MAC Authentication Bypass (MAB)
- MAB requires a MAC address database
- Unknown MACs use default authorization policy (catch-all)

Problem to solve: Impersonation Attacks

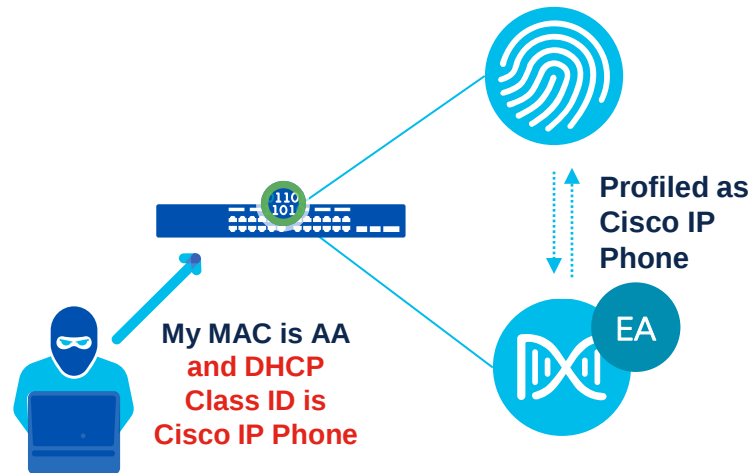
MAC address must not be the only source of truth

MAC Spoofing



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

Attribute Spoofing



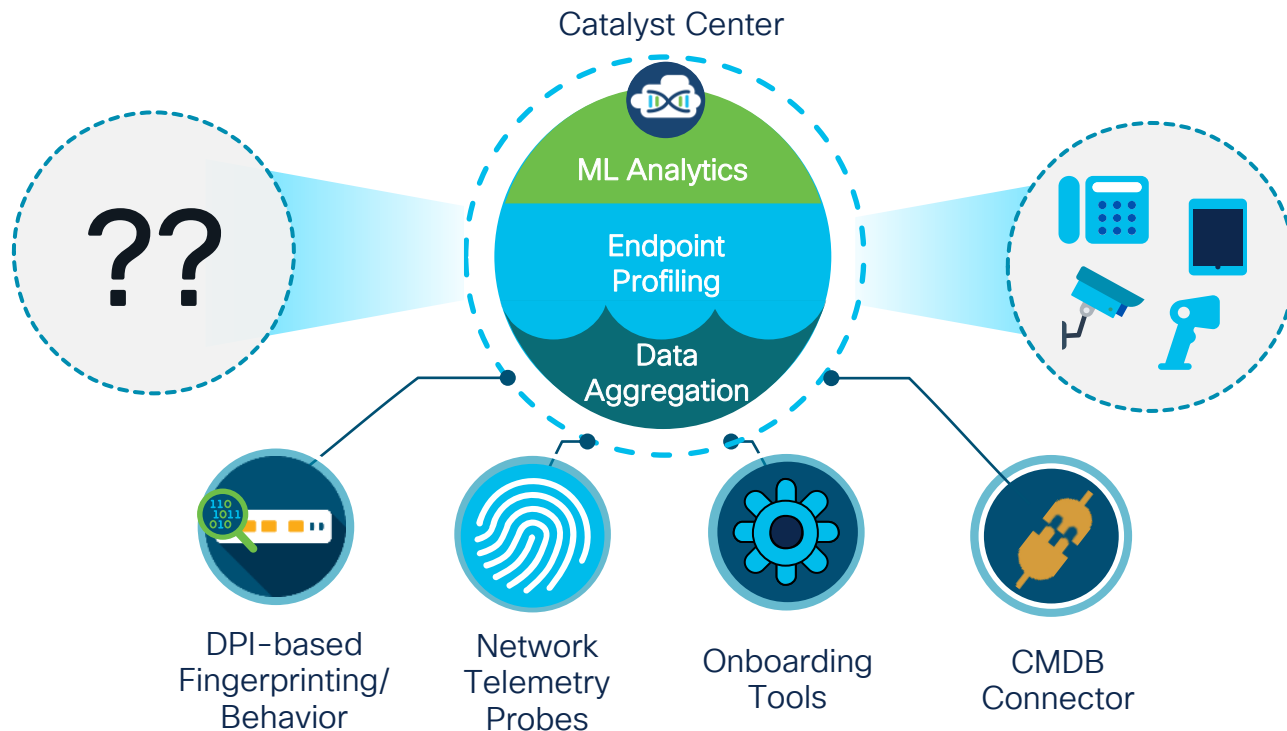
Impersonate class/type of the device in order to get privileged network access

AI Endpoint Analytics in Catalyst Center

Rapidly reducing the unknowns by aggregating data from different sources



Connected
Catalyst



Endpoint Analytics uses multifactor classification

EA classifies endpoints using four independent label categories



Device type

Laptop

CT scanner

Smartphone



Hardware manufacturer

Apple

GE

Globex Corp.



Hardware model

Ultima

Optima CT540

Galaxy S8



Operating system

MacOS 10.14.6

CTT OS 6.3.x Linux

Windows 7

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

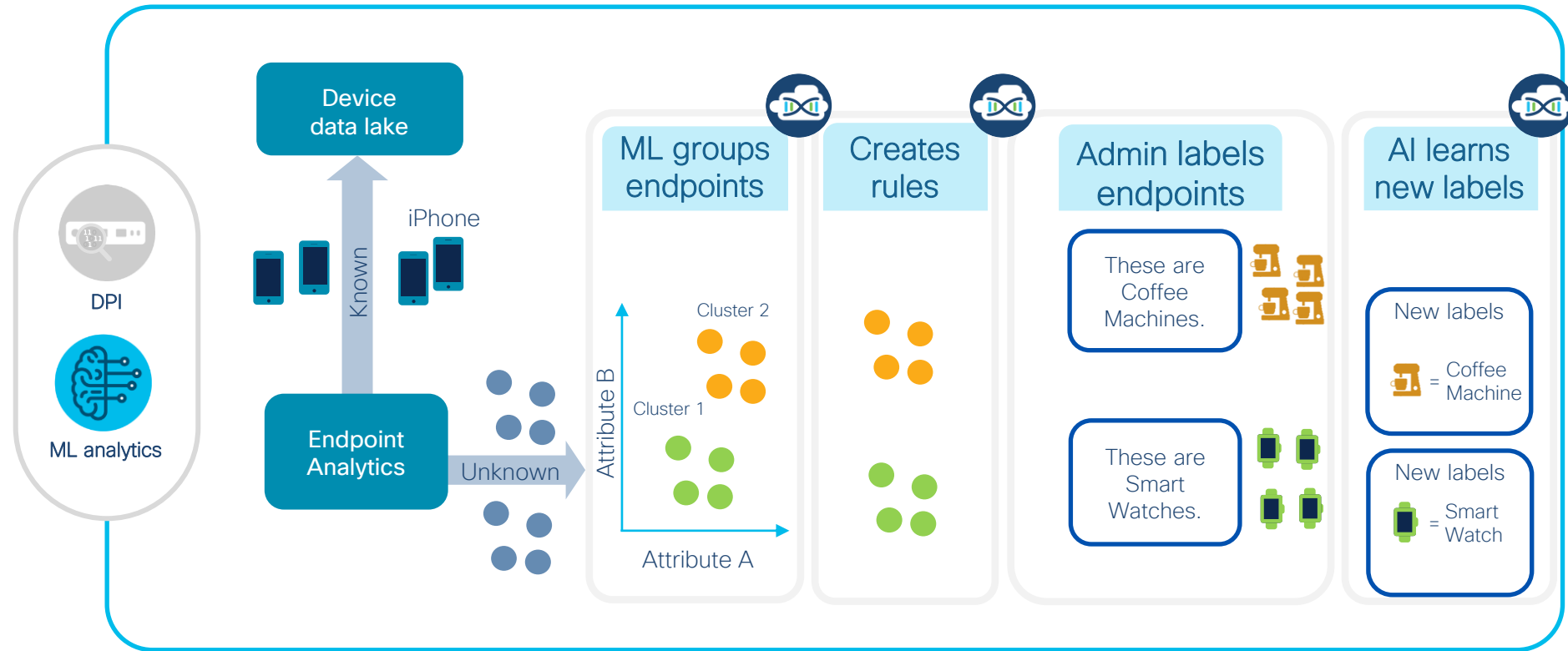
Connecte
Catalyst



Reduce Unknowns with Machine Learning (ML)

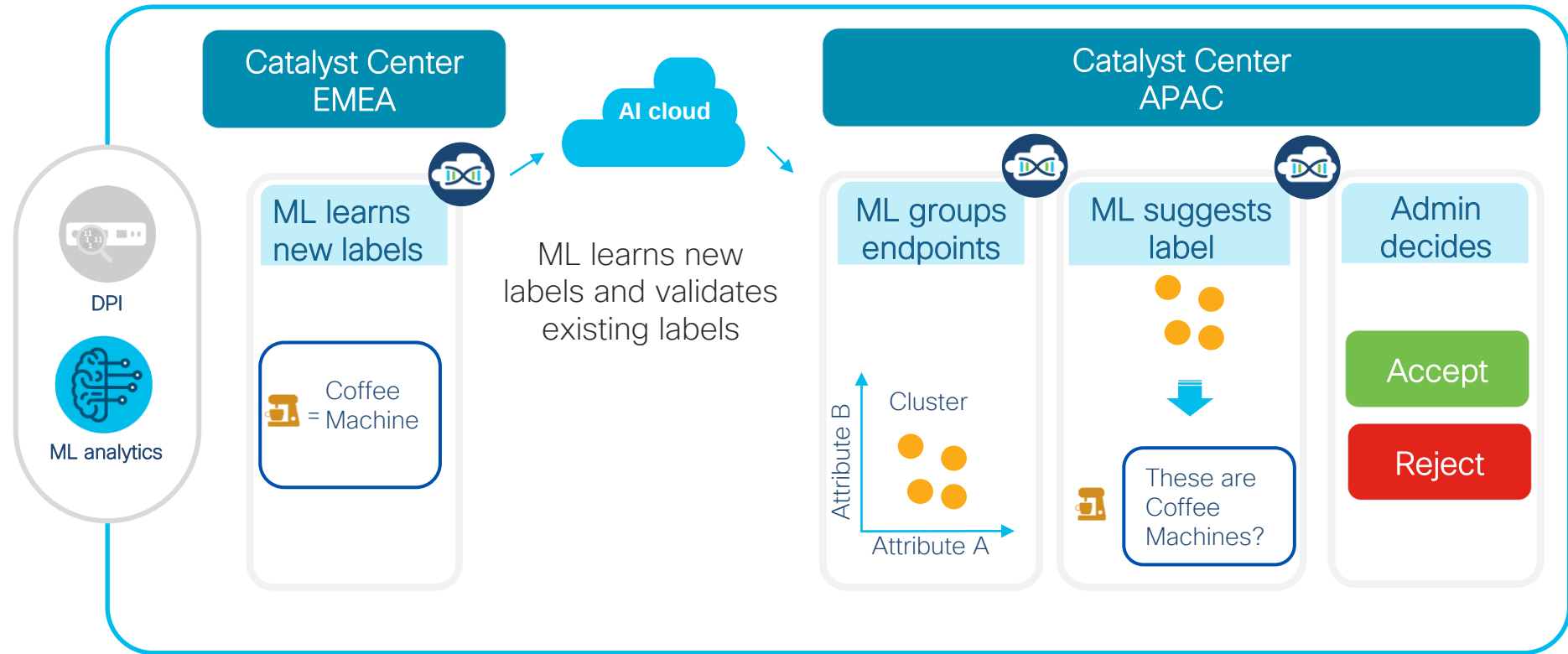


Connected
Catalyst



Crowdsourcing improves Machine Learning

Keep your global Catalyst Center deployments synchronized



Cisco Connected Catalyst

Optional cloud service that enhances Catalyst Center AI/ML functionality



Connected
Catalyst

Doc type
Cisco public

Privacy Data Sheet



Cisco Catalyst Center (formerly DNA Center)

Privacy Data Sheet



Addendum 1

Cisco AI Network Analytics

Privacy Data Sheet



Addendum 2

Cisco AI Endpoint Analytics

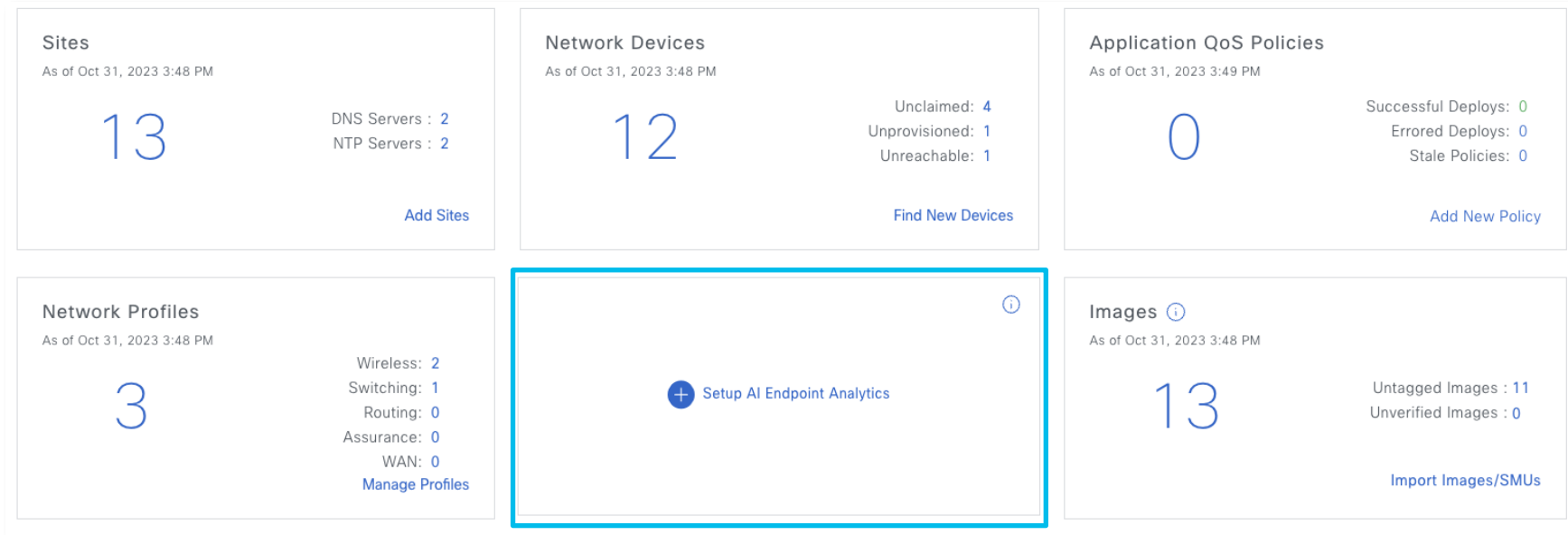
Choose your preferred cloud:

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

Status			
All		Enabled	Disabled
Configuration Name	Status		Details
1 DPI Enablement (CBAR)	🌙 Disabled		0 of 3 items are completed
2 ISE Configuration	🌙 Disabled		0 of 2 items are completed
3 AI Analytics Integration 	🌙 Disabled		0 of 1 items are completed

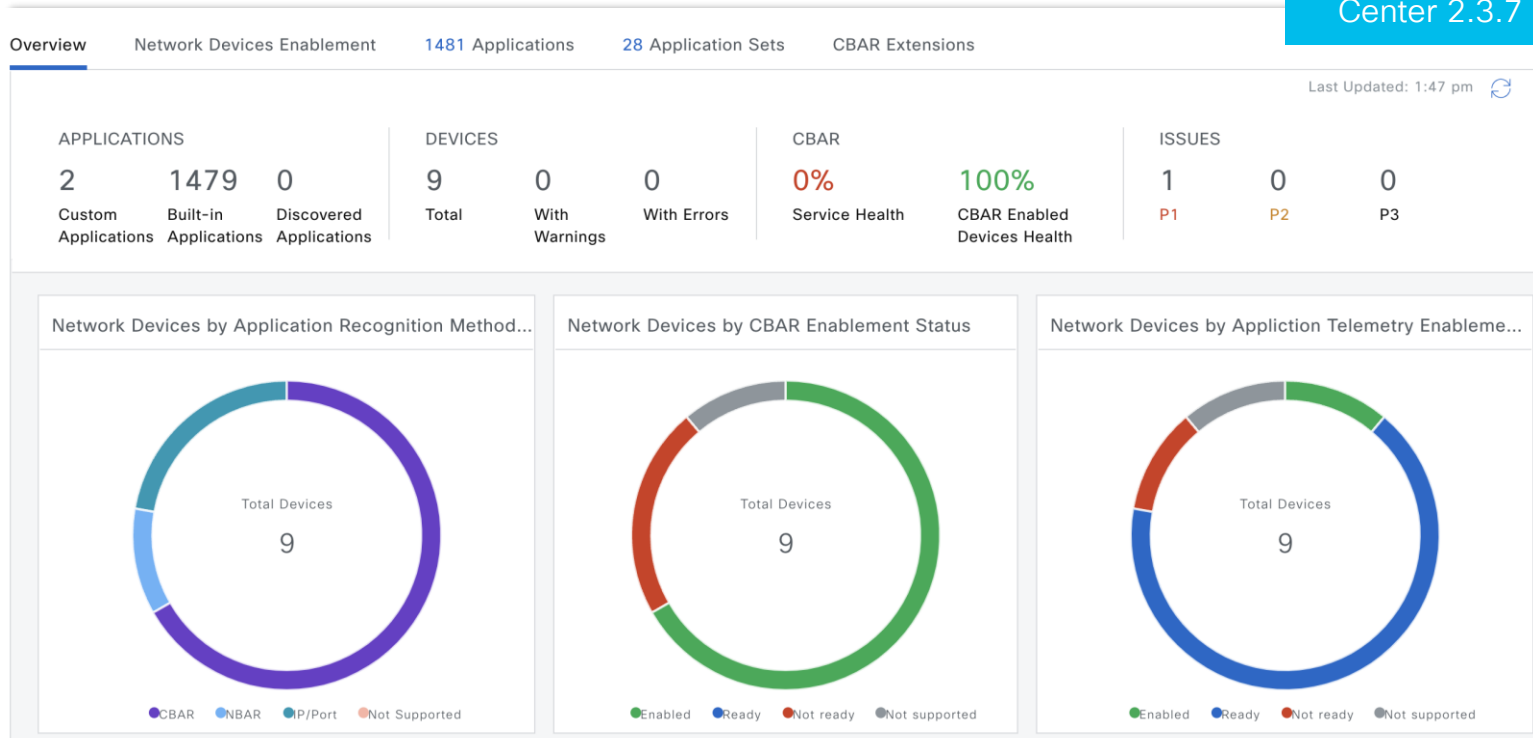
- Check the status of required configurations for EA
- Use links to follow steps to enable all three required configurations

Enable CBAR on C9K Devices

Provision > Services > Application Visibility Setup > Overview

1

*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

ISE Configuration

Endpoint attributes forwarding from Cisco ISE

Enable endpoint attribute forwarding from Cisco ISE to Cisco AI Endpoint Analytics for increased visibility using Cisco ISE probes.



Endpoint profile publishing to ISE

Allows publishing Cisco AI Endpoint Analytics profile data to Cisco ISE for authorizing endpoint access to network to and for endpoint control.



ISE Configuration



Settings have been updated.



Endpoint attributes forwarding from Cisco ISE

Enable endpoint attribute forwarding from Cisco ISE to Cisco AI Endpoint Analytics for increased visibility using Cisco ISE probes.



Endpoint profile publishing to ISE

Allows publishing Cisco AI Endpoint Analytics profile data to Cisco ISE for authorizing endpoint access to network to and for endpoint control.



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

Enable Catalyst Center AI Analytics

3

System > Settings > Cisco AI Analytics

Cisco AI Analytics

AI Network Analytics

AI Network Analytics harnesses machine learning to drive intelligence in the network, empowering administrators to effectively improve network performance and accelerate issue resolution. AI Network Analytics eliminates noise and false positives significantly learning the network behavior and adapting to your network environment.

☒ Enable AI Network Analytics

Enable AI Network Analytics

Enable AI Endpoint Analytics settings

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

AI Endpoint Analytics

Provides fine-grained endpoint identification and assigns labels to a variety of Endpoints.

ENDPOINT SMART GROUPING

Using AI and Machine Learning, Endpoint Smart Grouping reduces the number of unknown endpoints in the network by providing AI based endpoint groupings, automated custom profiling rules and crowdsourced endpoint labels.

☒ Enable Endpoint Smart Grouping

AI SPOOFING DETECTION *PREVIEW*

AI Spoofing Detection will detect endpoints being spoofed based on behavioral models. Models are currently being built using collected flow information from devices.

☒ Enable AI Spoofing Detection

Update

Cloud Data Storage ⓘ
Europe (Germany)



Connected
Catalyst Center

Required Configuration Steps to enable EA

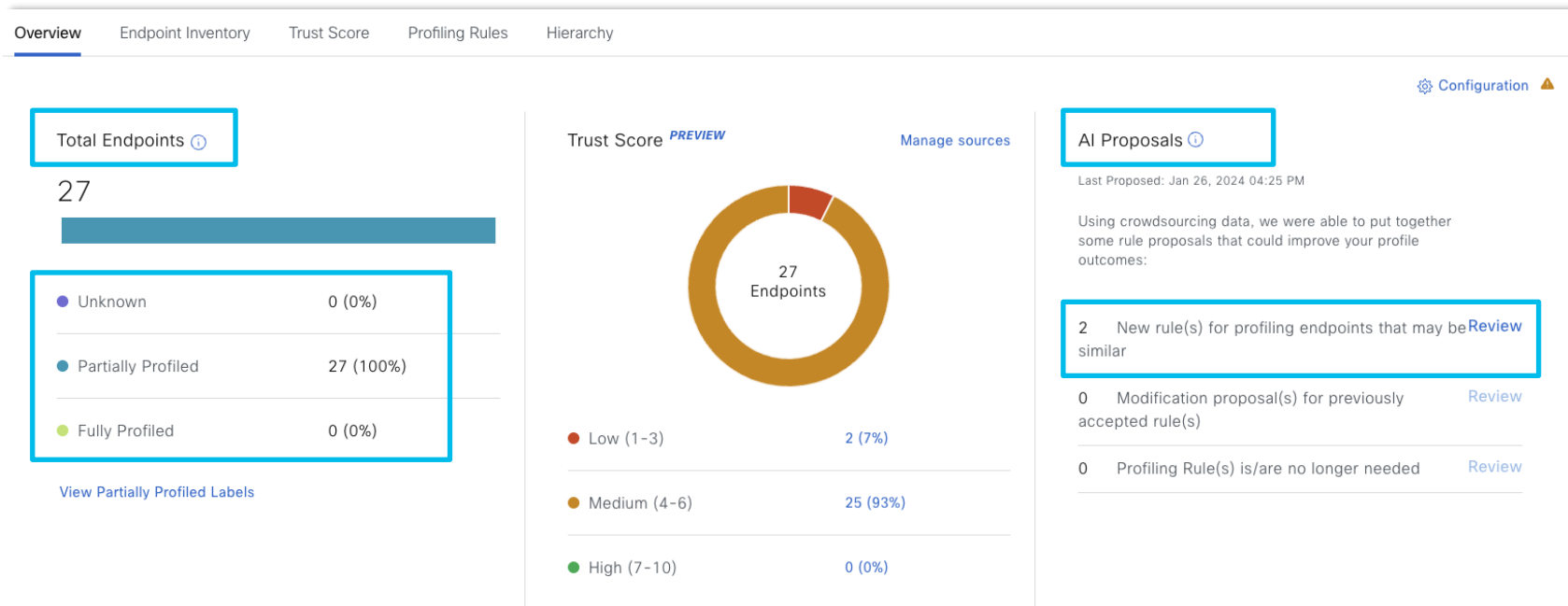
Policy > Endpoint Analytics – Manage Sources – Manage Configurations

Status			
All		Enabled	Disabled
Configuration Name		Status	Details
1	DPI Enablement (CBAR)	✓ Enabled	0 of 3 items are completed
2	ISE Configuration	✓ Enabled	0 of 2 items are completed
3	AI Analytics Integration 	✓ Enabled	0 of 1 items are completed

- 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



Overview **Endpoint Inventory** Trust Score Profiling Rules Hierarchy

Endpoint Inventory (12) Focus: [Select](#) ▾

🔍 Filter for endpoints by selecting values

0 Selected

MAC Address ⓘ	IP Address ▾	Hostname ⓘ	Endpoint Type	OS Type
00:91:9E:F1:3F:AB	10.14.70.87	Jennie-Laptop	Workstation	Windows
6C:7E:67:D7:68:E9	10.14.70.83	Wireless-MBP	Workstation	macOS C
8C:F8:C5:B5:08:60	10.14.70.76	DESKTOP-G6NQ1KH	Workstation	Windows
58:CE:2A:13:9B:97	10.14.70.61	wireless-tme	Workstation	Windows
DC:FB:48:A3:94:A9	10.14.70.56	DESKTOP-54LIALB	Workstation	Windows
42:7A:4D:B0:83:CF	10.14.70.50	-	Mobile Device	iOS 16 (1

58:CE:2A:13:9B:97

Hostname **wireless-tme** Trust Score ● 9

User Details

User Name **hitesh.malhan** User Group ID **-**

Endpoint details

Endpoint Type	Workstation ⓘ
Hardware Manufacturer	Dell Inc. ⓘ
Hardware Model	Dell-Device Inspiron 16 5620 ⓘ
OS Type	Windows 10 ⓘ
Connected Location	San Jose/Building 14/Floor1
UUID	-

Authentication Status	STARTED
Authorization Profile	PermitAccess
Scalable Group Tag	-
Last Seen	Jan 24, 2024 09:07

Endpoint Inventory shows all known endpoint MAC addresses and classification

EA Attributes are integrated into Assurance

Assurance > Dashboards > Health > Client



status

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
☐	📶 <a>anna	Intel-Device	10	9	●	●	Intel Corporation	Windows	Workstation
☐	📶 <a>greg	Intel-Device	10	9	●	●	Intel Corporation	Windows	Workstation
☐	📶 <a>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

AI Endpoint Analytics

Method	Name	Description	URL	Actions
GET	Fetch the count of endpoints	Fetch the total count of endpoints that match the given filter criteria.	/endpoint-analytics/endpoints/count	 
GET	Get task details	Fetches the details of backend task. Task is typically created by making call to some other API that takes longer time to execute.	/endpoint-analytics/tasks/\${taskId}	
PUT	Apply ANC Policy	Applies given ANC policy to the endpoint.	/endpoint-analytics/endpoints/\${epId}/anc-policy	

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

cmdbSerialNumber	cmdbSerialNumber
concurrentMacAddr...	concurrentMacAd...
deviceType	deviceType
groupHierarchy	groupHierarchy
hardwareManufacturer	hardwareManufac...
hardwareModel	hardwareModel
mfcAnomalyResult	mfcAnomalyResult
natAnomalyResult	natAnomalyResult
openPortList	openPortList
operatingSystem	operatingSystem
portScanningResult	portScanningResult
spuriousAccessResult	spuriousAccessR...
trustScore	trustScore

Endpoint type

Manufacturer

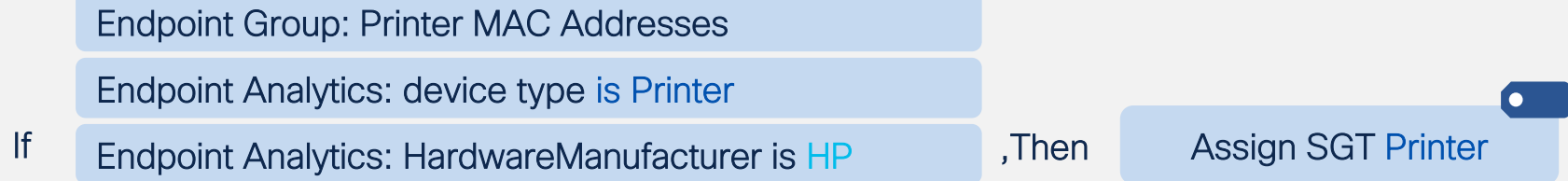
Model

Operating system

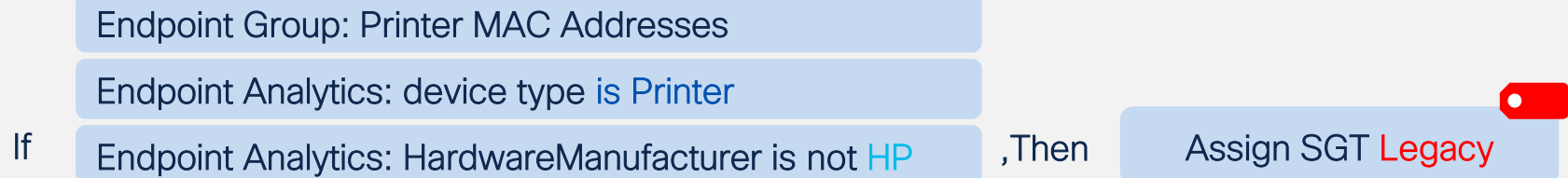
Several new endpoint attributes available for identification in authorization policies

Use Endpoint Analytics attributes in ISE policy

Authorization policy for HP Printers:



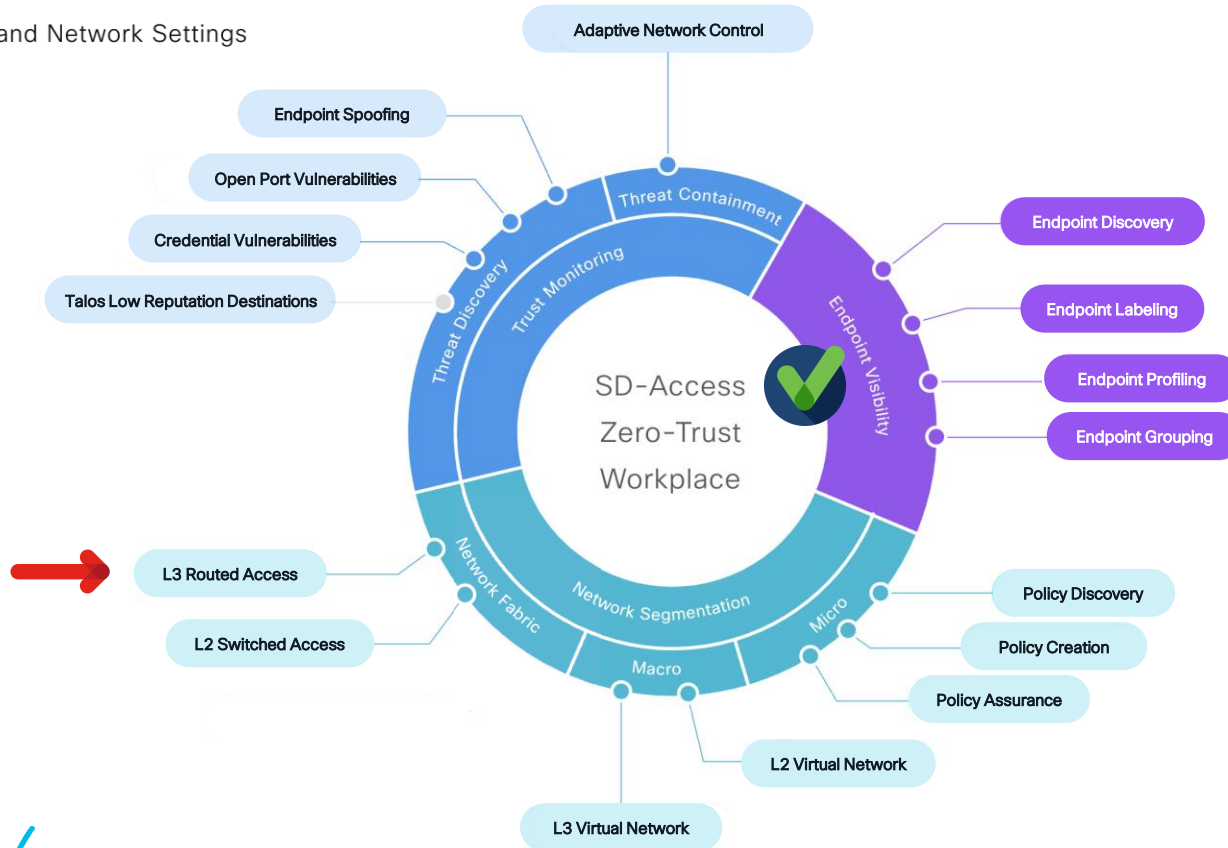
Authorization policy for legacy printers



We gained deep visibility of our endpoints

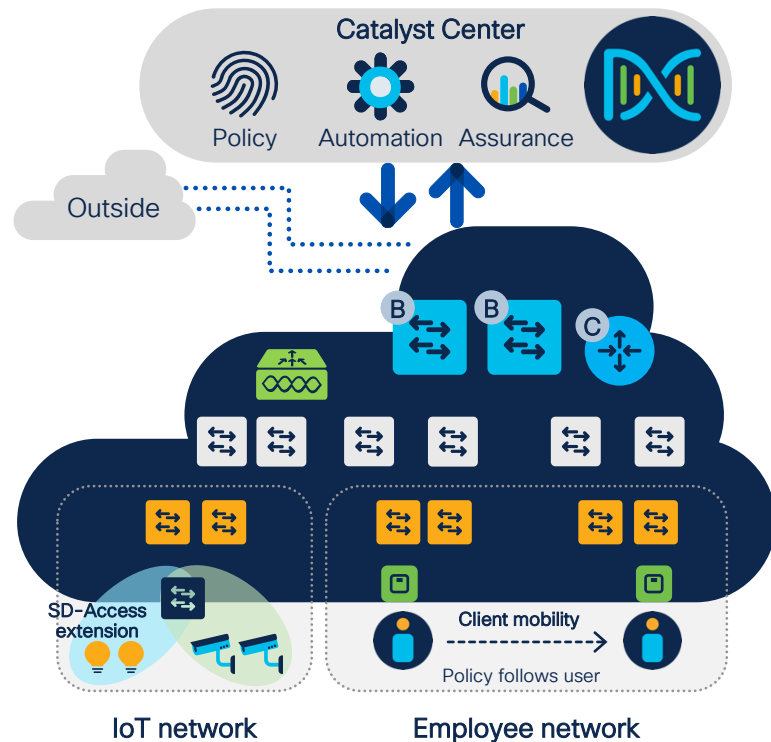
✓ Your Services and Network Settings

- ✓ CAT9K
- ✓ ISE
- ☾ Talos
- ✓ CBAR



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

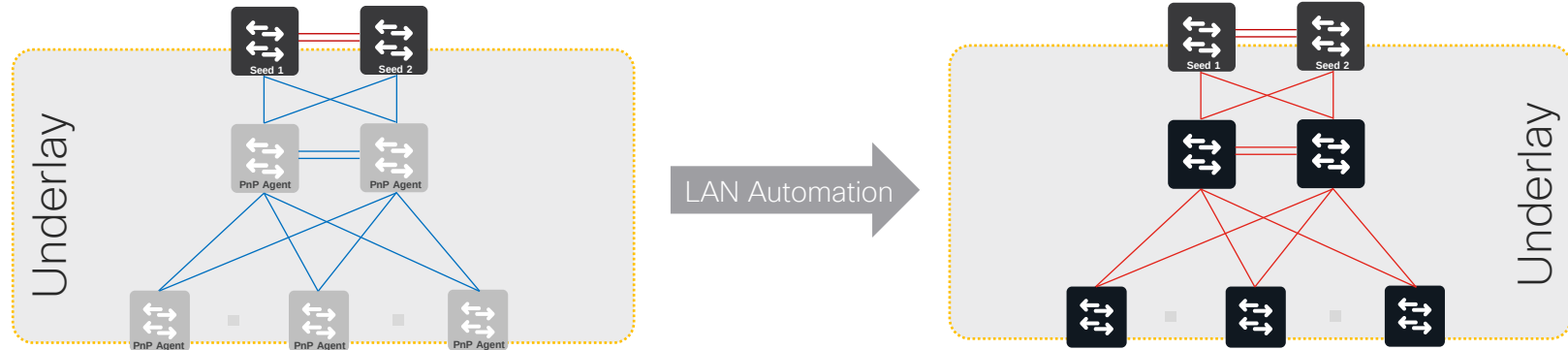
Why should we use LAN Automation?

Explaining the LAN Automation

LAN automation leverages PnP and configures for you:

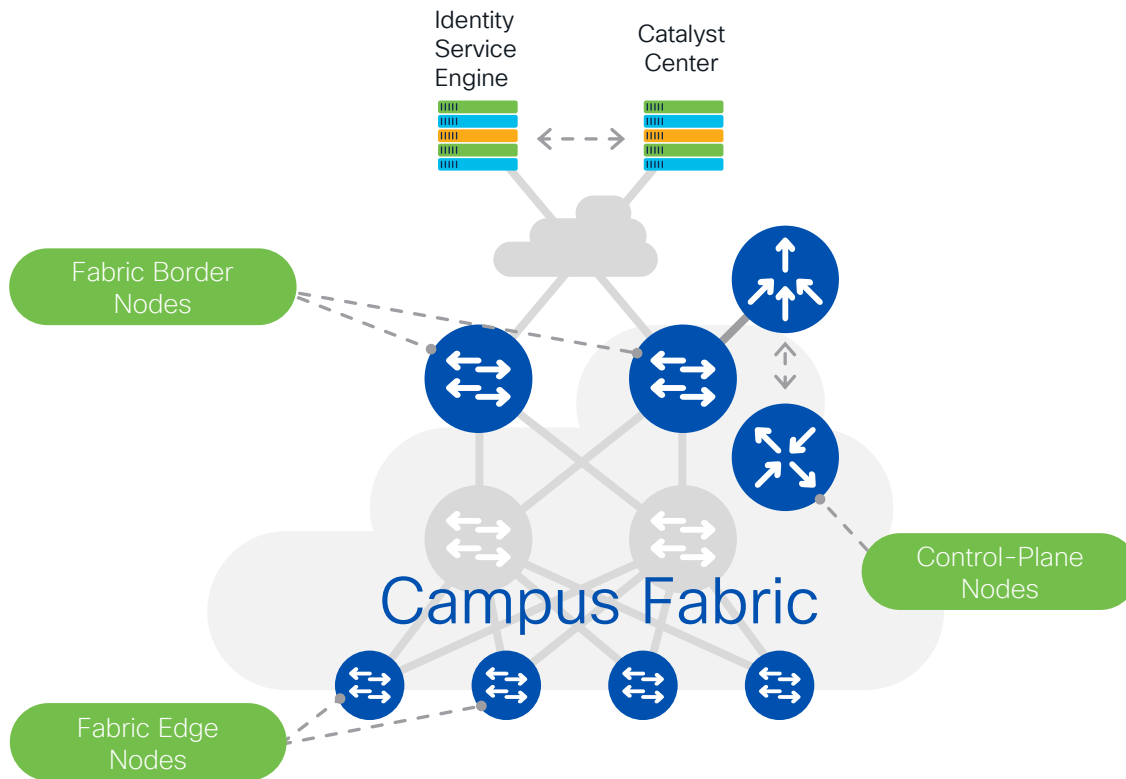
- Routed interconnections
- Loopback0
- IS-IS routing protocol
- Host names

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

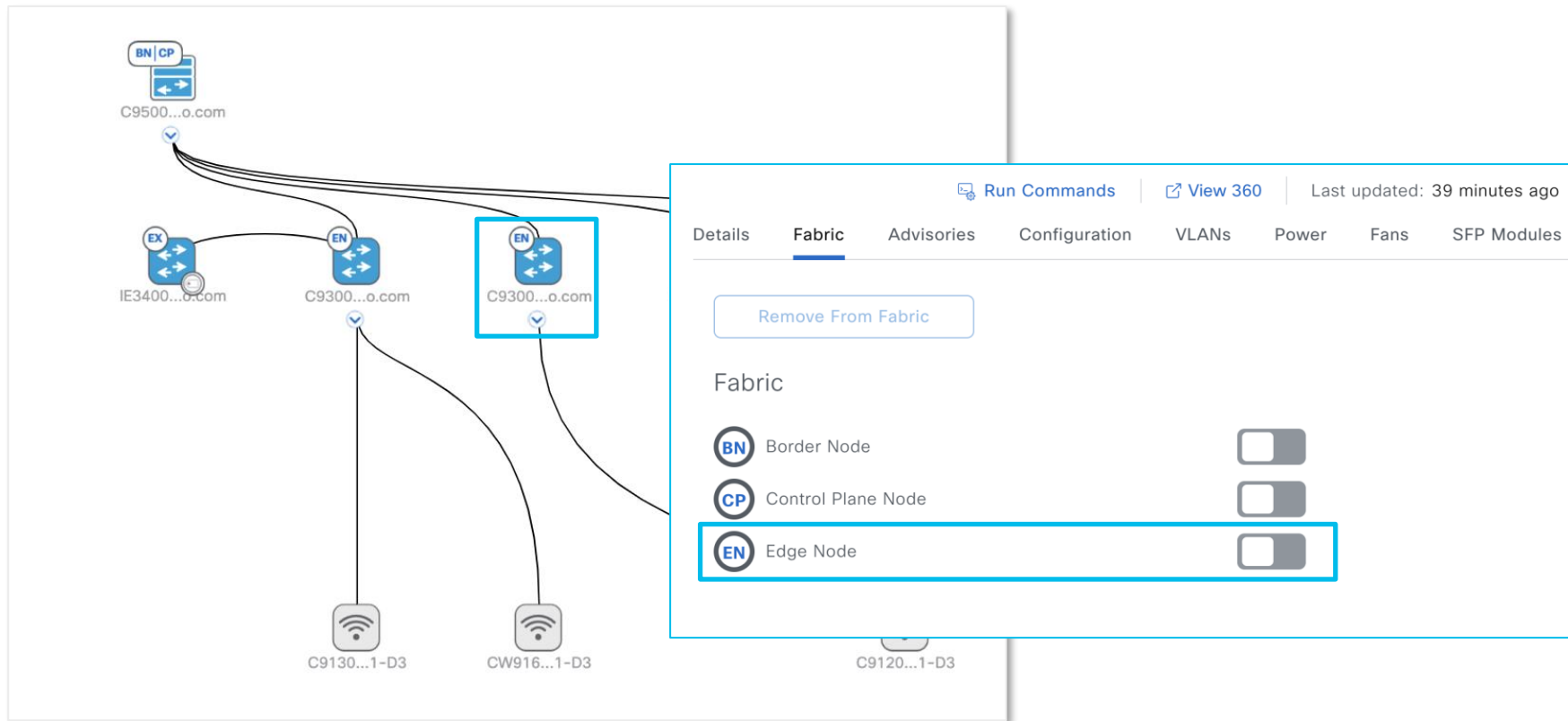
A fabric device (e.g. Core) that connects External L3 network(s) to the SD-Access fabric

Fabric Edge Nodes

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

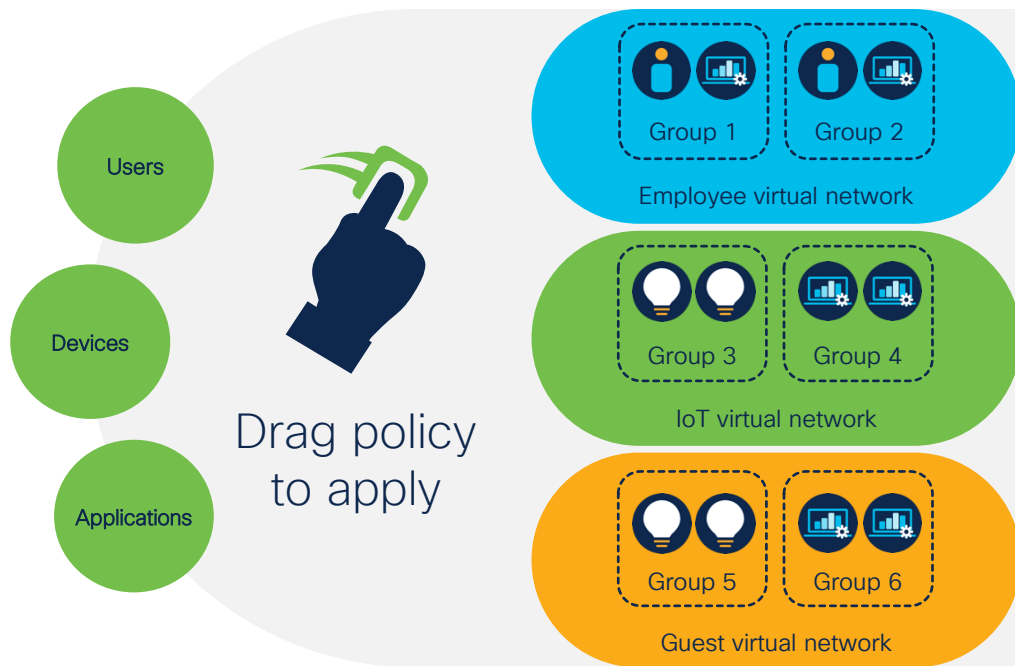
Assign Fabric Roles to Fabric Devices

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

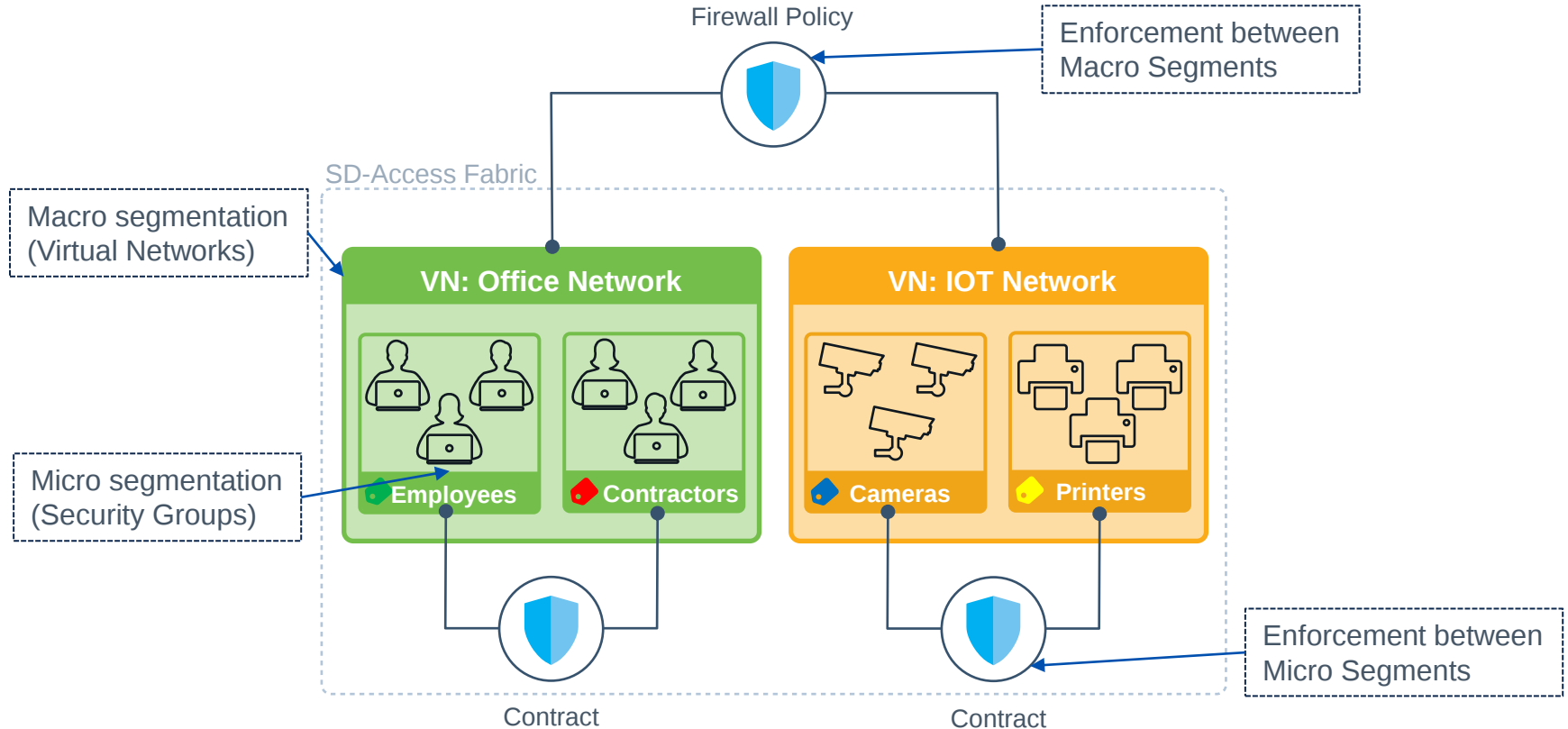
Security

- 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



Fabric Site: Global

- Layer 3

Layer 2

Anycast Gateways

Extranet Policies

🔍

Search Layer 3 Virtual Networks

🔽

0 selected

ⓘ

⊕ Create Layer 3 Virtual Networks

More Actions ▼

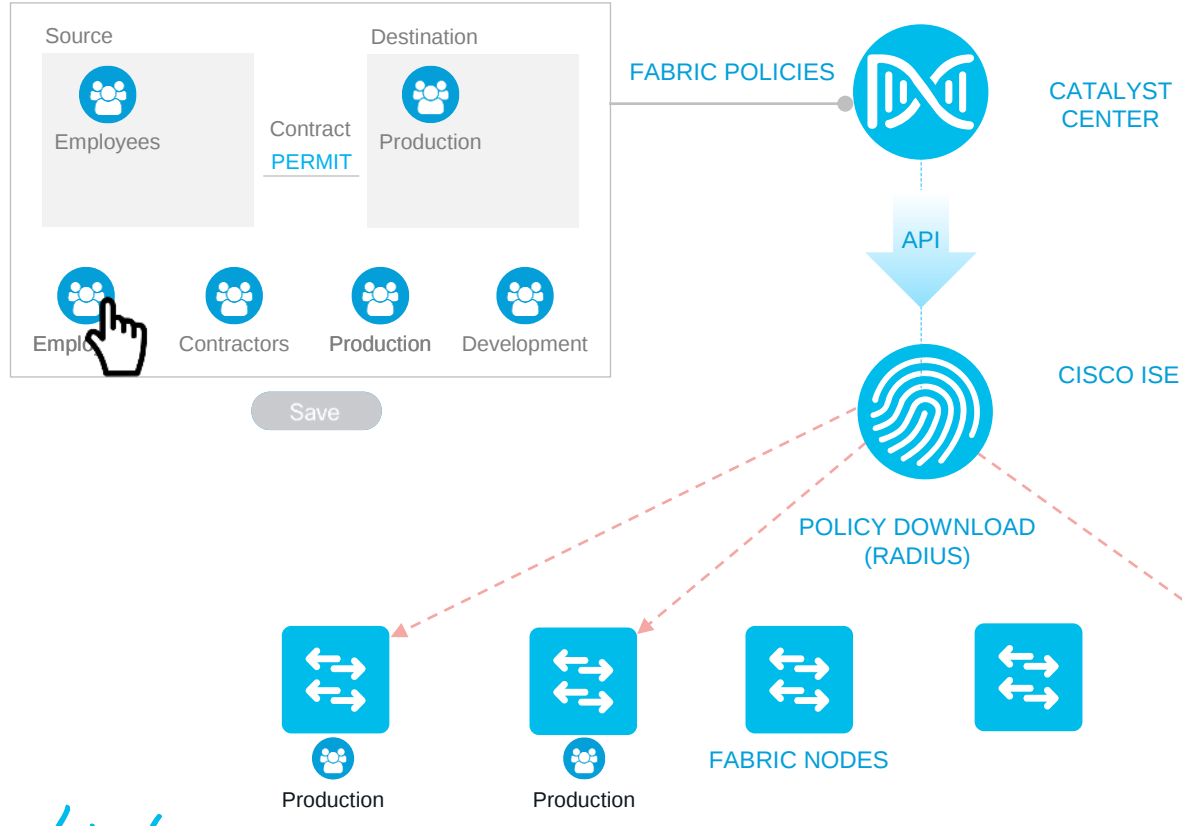
As of: Feb 2, 2024 6:37 PM

🔄

☐	Layer 3 Virtual Network ▲	Layer 3 VNID	Health Score ⓘ	Anycast Gateways	Associated Fabric Sites	Associated Fabric Zones	Multicast-Enabled Fabric Sites
☐	Campus_Network	4119	--	0	1	0	--
☐	D3_4114	4114	--	0	1	0	--
☐	D3_4115	4115	--	0	1	0	--
☐	D3_CAMPUS	4111	100%	1	1	0	--
☐	D3_GUEST	4112	100%	1	1	0	--

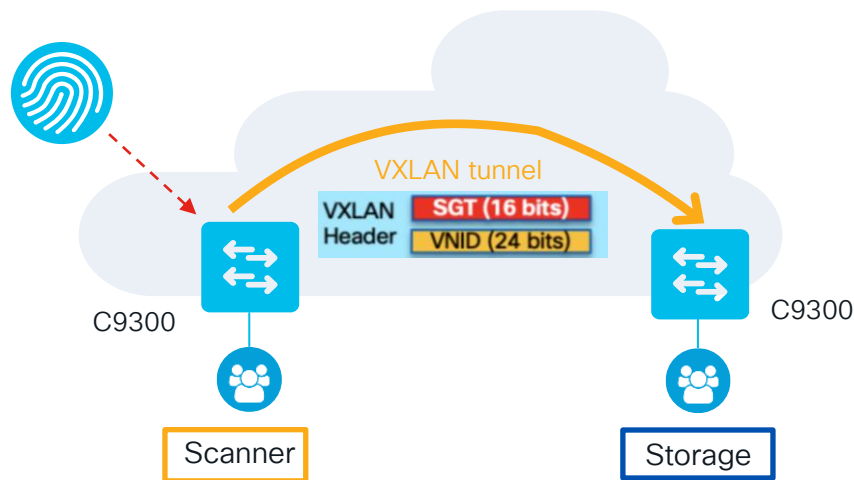
SD-Access Policy

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

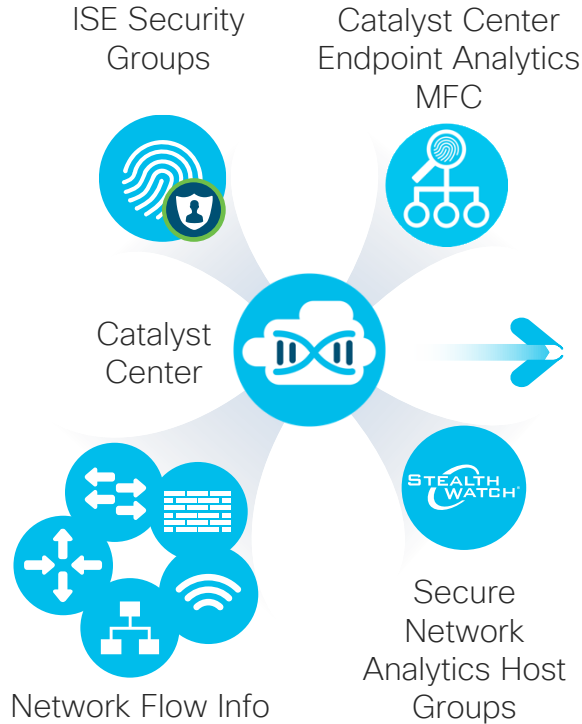
IPv4 Role-based permissions from group 36 Scanners to group 27 Storage_PACS:

Permit_IP_Log-01

		■ Permit	■ Deny	■ Custom	□ Default					
Source	Destination	Employees	Scanners	Contractors	Water_Control	Unknown	Doctors	Storage	Development_...	Auditors
	Employees	■	□	□	□	□	□	□	■	□
Scanners	□	■	□	□	■	□	■	□	□	□
Contractors	□	□	□	□	□	□	□	□	■	□

Group Based Policy Analytics shows real flows

Displays traffic between groups



CISCO *Live!*



Default permit



Default deny

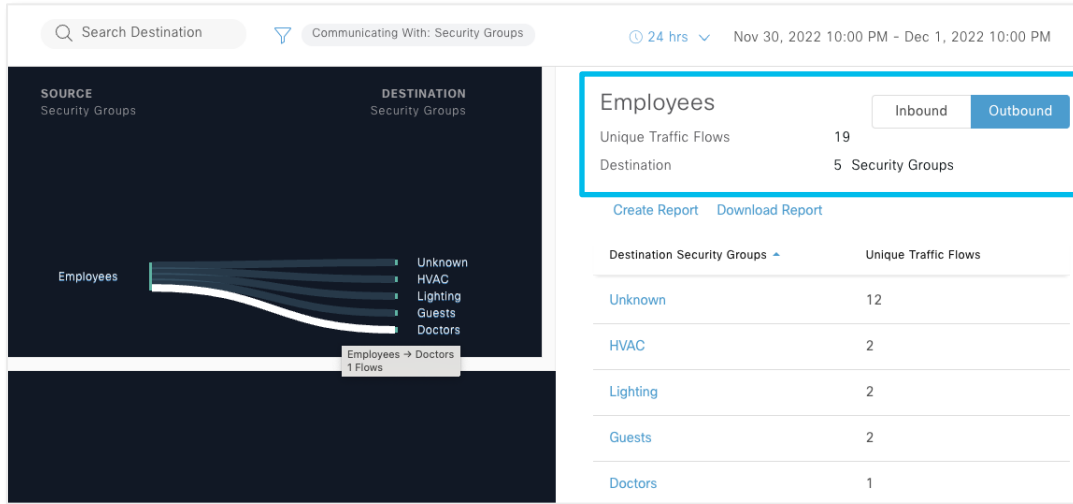


Cisco ISE TrustSec Allow-List Model (Default Deny IP) With SDA

<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

The interface shows a detailed traffic flow table for the connection from 'Employees' to 'Doctors'. It includes a 'View Contract' button and a 'View Policy Enforcement Stats' link. The table lists the direction, service name, protocol, port, and flow count for each flow.

Direction	Service Name	Protocol	Port	Flow Count ①
↔	bootps	UDP	67	
↔	domain	UDP	53	
→	http	TCP	80	
→	https	TCP	443	
→	ftp	TCP	21	
→	llmnr	UDP	5355	

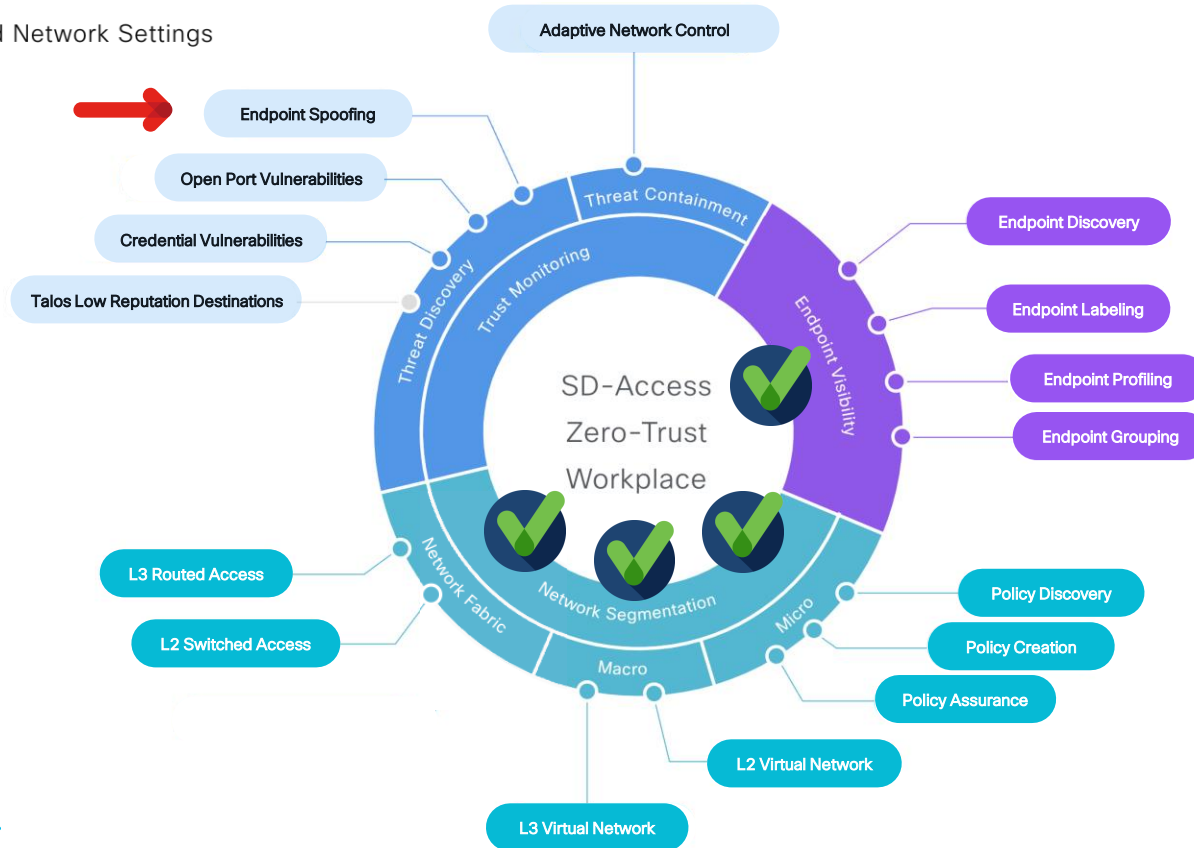
View Contract

Ports detected from group Employees to group Doctors

We segmented our network on multiple levels

✓ Your Services and Network Settings

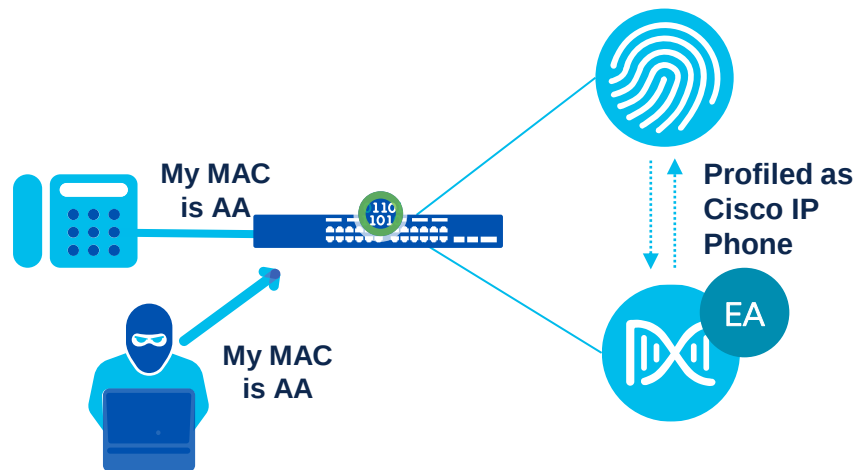
- ✓ CAT9K
- ✓ ISE
- ☒ Talos
- ✓ CBAR



Problem to solve: Impersonation Attacks

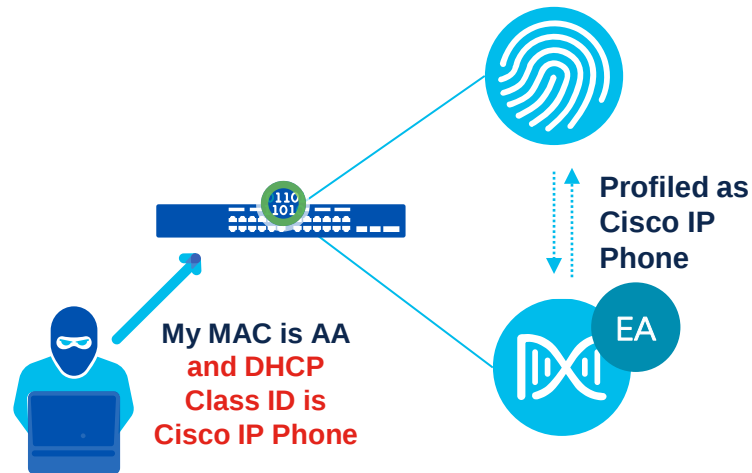
MAC address must not be the only source of truth

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



Negative Influence

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

Trust-based ISE Policies

1-3 Deny access

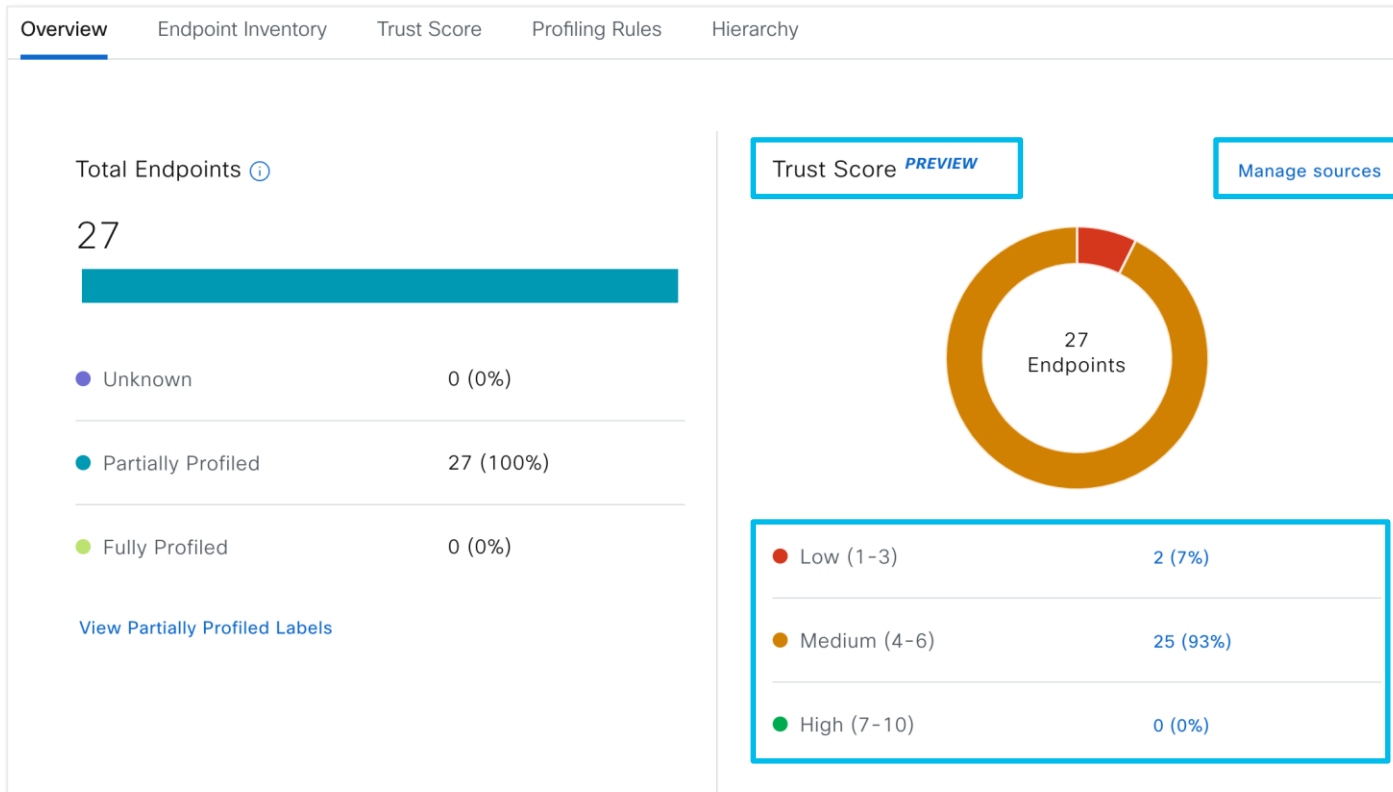
4-7 Limited access

7-10 Full access

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

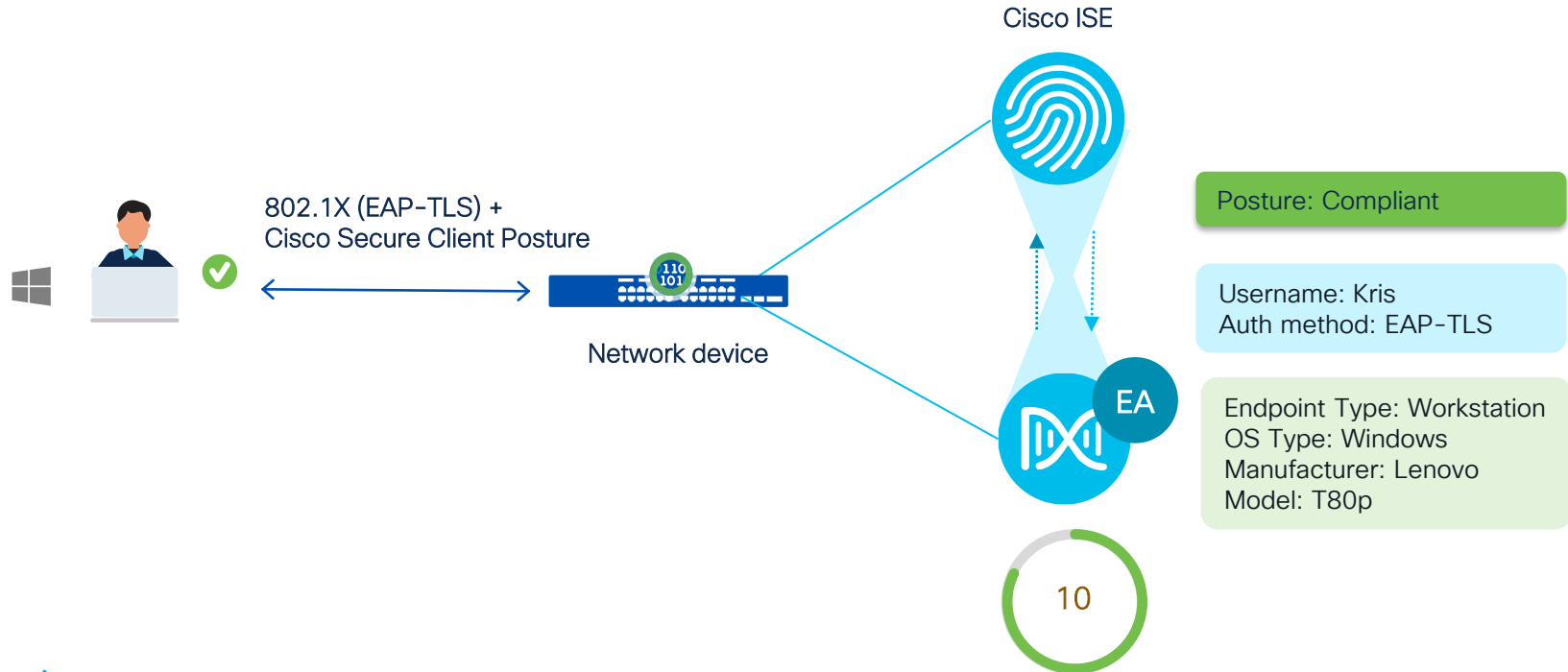
Policy > Endpoint Analytics – Manage Sources – Manage Configurations

Status			
AllEnabledDisabled			
	Configuration Name	Status	Details
1	Security Sensor	✓ Enabled	3 of 3 items are completed
2	ServiceNow	⌚ Disabled	0 of 1 items are completed
3	Talos IP Reputation	✓ Enabled	5 of 5 items are completed
4	AI Spoofing detection	✓ Enabled	3 of 3 items are completed

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

The screenshot displays the Cisco Trust Score interface. On the left, the 'Trust Score' tab is selected, showing a list of endpoints. The first endpoint, with MAC address 00:50:56:AE:C0:5E and a Trust Score of 10, is highlighted. A blue line connects this endpoint to the detailed view on the right. The detailed view shows the endpoint's Hostname (wx-emp1) and Trust Score (10). It also displays the 'Authentication Method' (Wired802_1x (PEAP (EAP-MSCHAPv2))) and 'Posture' (Compliant) status, both of which are highlighted with blue boxes. A blue box also highlights the 'Endpoints' link in the left sidebar. The 'Endpoint Context' section provides additional information about the authentication method and posture assessment.

Overview Endpoint Inventory **Trust Score** Profiling Rules Hierarchy

Trust Score

Trust Score assesses the trustworthiness of a given endpoint on the network to help achieve zero trust out. Values range from 1 (low trust) to 10 (high trust) and are calculated using several sources that provide context about the endpoint (e.g. posture, authentication), its vulnerability [View More...](#)

Alerts **Endpoints**

Endpoints (18) Focus: Trust Score - Default view

Search

0 Selected [Reset Trust Score](#) [More Actions](#)

MAC Address	Endpoint Trust Score	IP Address	Authentication Method
00:50:56:AE:C0:5E	10	172.16.1.202	Wired802_1x (PEAP (EAP-MSCHAPv2))
00:50:56:AE:18:87	8	172.16.1.201	Wired802_1x (PEAP (EAP-MSCHAPv2))
00:50:56:8F:57:E2	10	172.16.1.202	Wired802_1x (PEAP (EAP-MSCHAPv2))

00:50:56:AE:C0:5E

Hostname wx-emp1 Trust Score 10

Details **Trust Score** Attributes

Trust Score Total: 10

Endpoint Context

Authentication Method Wired802_1x (PEAP (EAP-MSCHAPv2))

Authentication Method identifies how an endpoint authenticates itself to the network and acts as a positive input to the endpoint trust score.
Status: Wired802_1x (PEAP (EAP-MSCHAPv2))

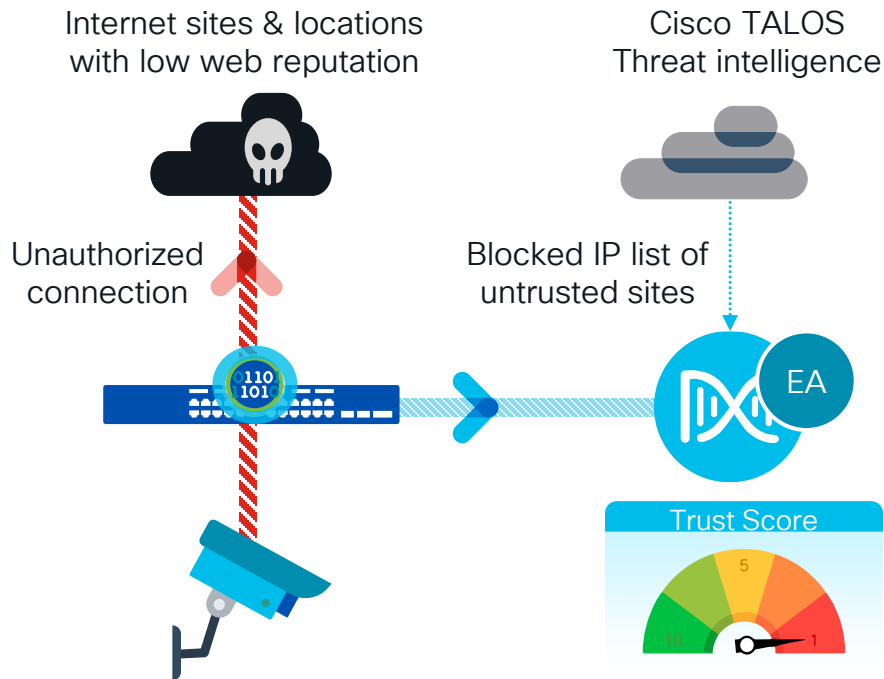
Posture Compliant

Endpoint posture assessment gathers information on the device such as OS, antimalware and patch level status in order to determine if endpoint is compliant. Posture assessment collects posture information from ISE to be used to calculate Trust Score.

Enabled

Low reputation IP connections

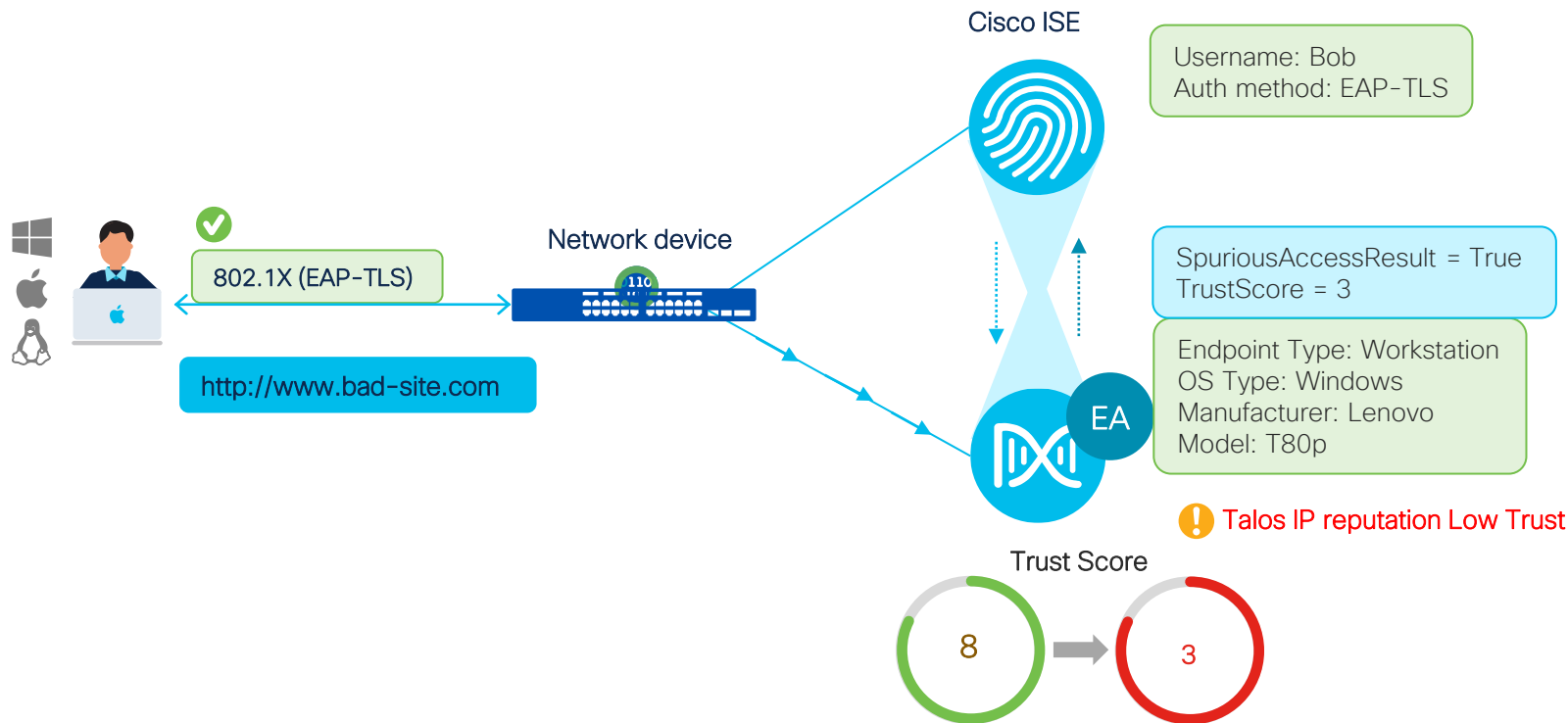
Detecting endpoint connections to low reputation sites.



- 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

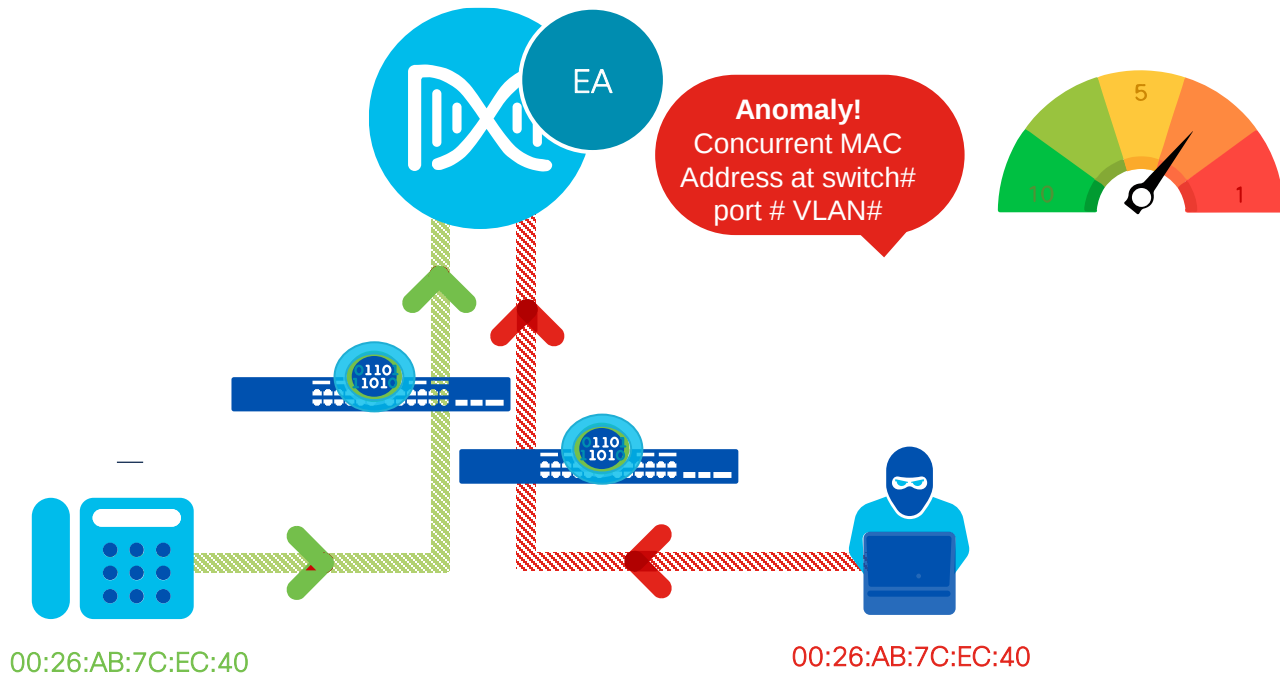
Trust Score changes after anomaly

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

B8:27:EB:2C:DC:08
Hostname - Trust Score 3

Details **Trust Score** Attributes

Trust Score Total: 3

Endpoint Context

> Authentication Method Not Detected

> Posture Not Detected

Threat and Vulnerability Context

> AI Spoofing Detection Not Detected

> Changed Profile Labels Not Detected

> Unauthorized Ports Not Detected

> Credential Vulnerability Not Detected

Network Context

> Concurrent MAC Address **Low Trust** Last Scored: Oct 27, 2022 10:23 AM

Network Context

✓ Concurrent MAC Address **Low Trust** Last Scored: Oct 27, 2022 10:23 AM

Concurrent MAC address detects when multiple endpoints are on the network (for example, on different switches or in different VLANs on the same switch) with the same MAC address

Severity 80 Confidence 100

VLAN ID	Network Device Name	Interface Name	Network Device IP
1	C9800-CL.hamlab.cisco.com	-	10.1.111.107
501	C9300-HH-1.hamlab.cisco.com	0	192.168.100.105

☒ Enabled

[Reset](#) [Was this accurate?](#)

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)

Manual
intervention

Tool to start temporary
remediation action

No permanent authorization policy
needed for port shut or quarantine

Re-auth and port
bounce actions require
authorization policy

Automated threat isolation and remediation
possible via ISE API

Demo

Welcome to Catalyst Center!

Explore

Cisco DNA Center is becoming Catalyst Center

As part of our vision to converge our products around an integrated platform, we are changing the name of Cisco DNA Center to Catalyst Center in the next release. The capability and functionality of Catalyst Center remains the same as Cisco DNA Center.

Assurance Summary

Health ⓘ

Healthy as of Feb 4, 2024 12:11 PM

85%

Network Devices

100%

Wireless Clients

100%

Wired Clients

View Details

Critical Issues

Last 24 Hours

4

P1

6

P2

View Details

Trends and Insights

Last 30 Days

4

AP Performance Advisories

5

Trend Deviations

View Details

Network Snapshot

Sites

As of Feb 4, 2024 12:11 PM

49

DNS Servers : 1

NTP Servers : 0

Network Devices

As of Feb 4, 2024 12:10 PM

66

Unclaimed: 1

Unprovisioned: 1

Application QoS Policies

As of Feb 4, 2024 12:14 PM

0

Successful Deploys: 0

Errored Deploys: 0

CISCO Live!

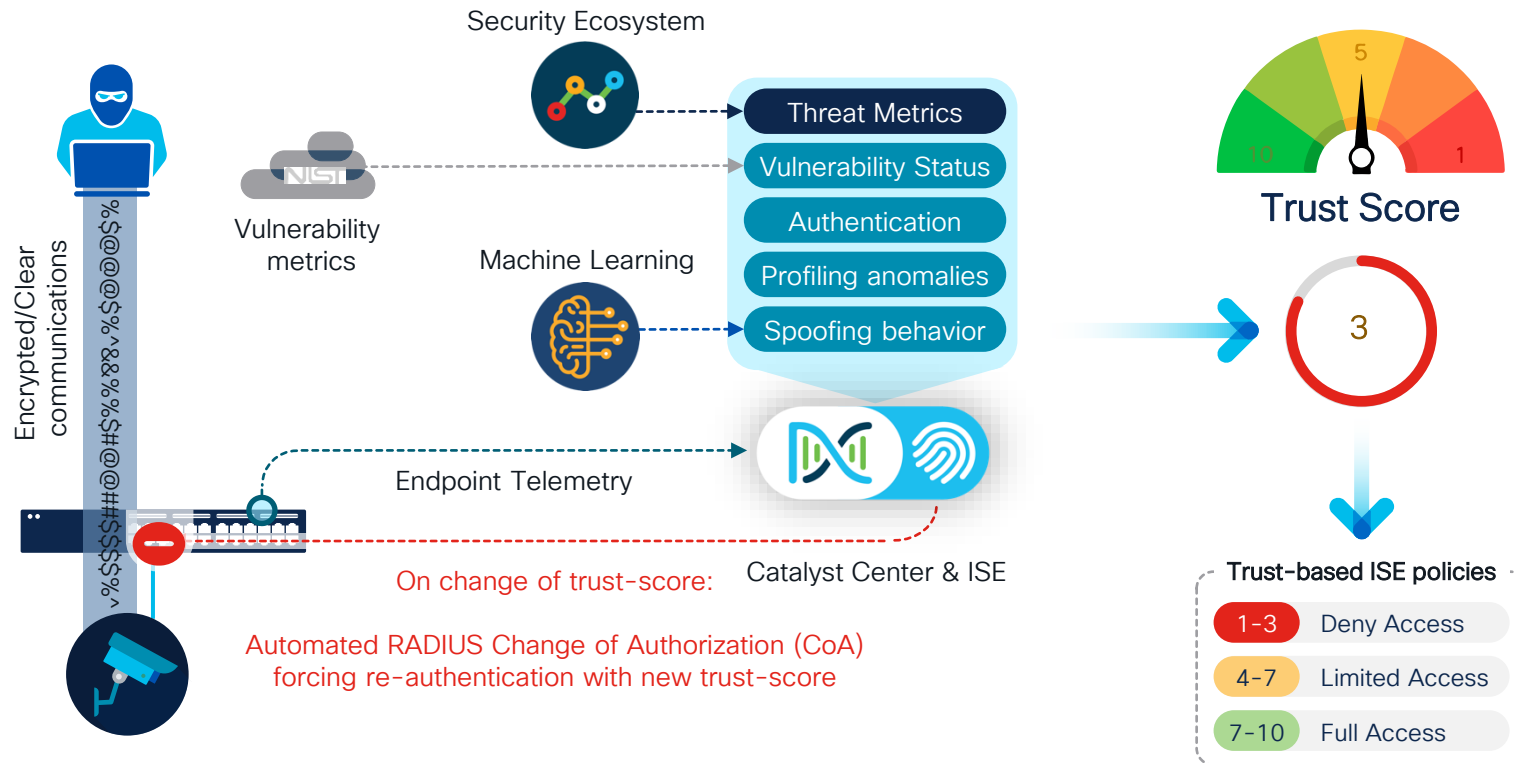
BRKOPS-2683

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

85

Trust based network access

Continuously monitor anomalies, endpoint trust and restrict access



Endpoint Analytics brings new dictionary to ISE

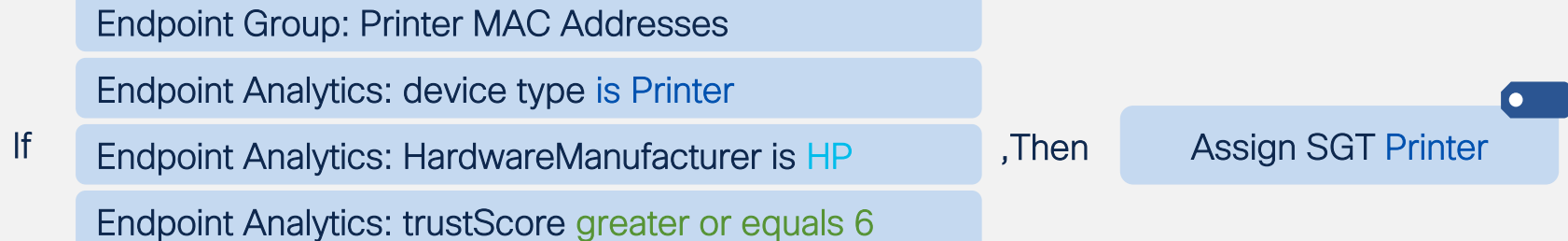
ISE: Policy > Policy Elements > Dictionaries > System > Endpoint-Analytics

cmdbSerialNumber	cmdbSerialNumber	
concurrentMacAddr...	concurrentMacAd...	
deviceType	deviceType	Endpoint type
groupHierarchy	groupHierarchy	
hardwareManufacturer	hardwareManufac...	Manufacturer
hardwareModel	hardwareModel	Model
mfcAnomalyResult	mfcAnomalyResult	
natAnomalyResult	natAnomalyResult	
openPortList	openPortList	
operatingSystem	operatingSystem	Operating system
portScanningResult	portScanningResult	
spuriousAccessResult	spuriousAccessR...	
trustScore	trustScore	Trust Score

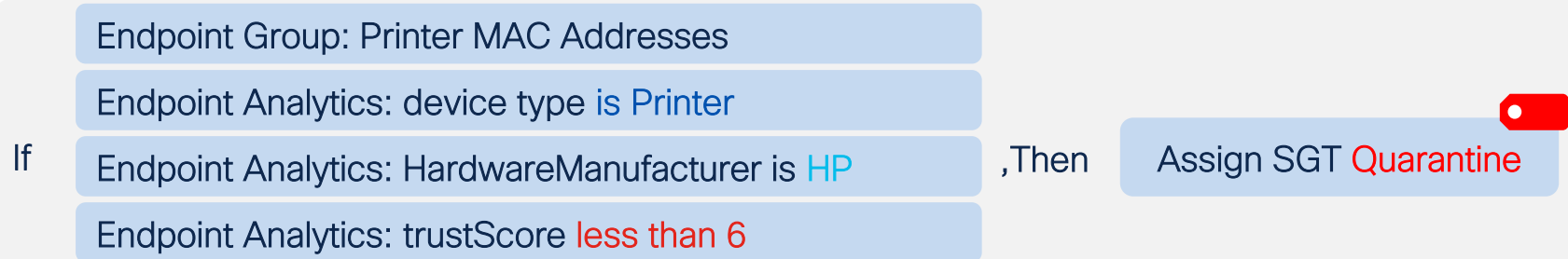
Trust Score available for use in authorization policies

Use Endpoint Analytics attributes in ISE policy

Authorization policy for HP Printers:



Authorization policy for untrusted HP printers



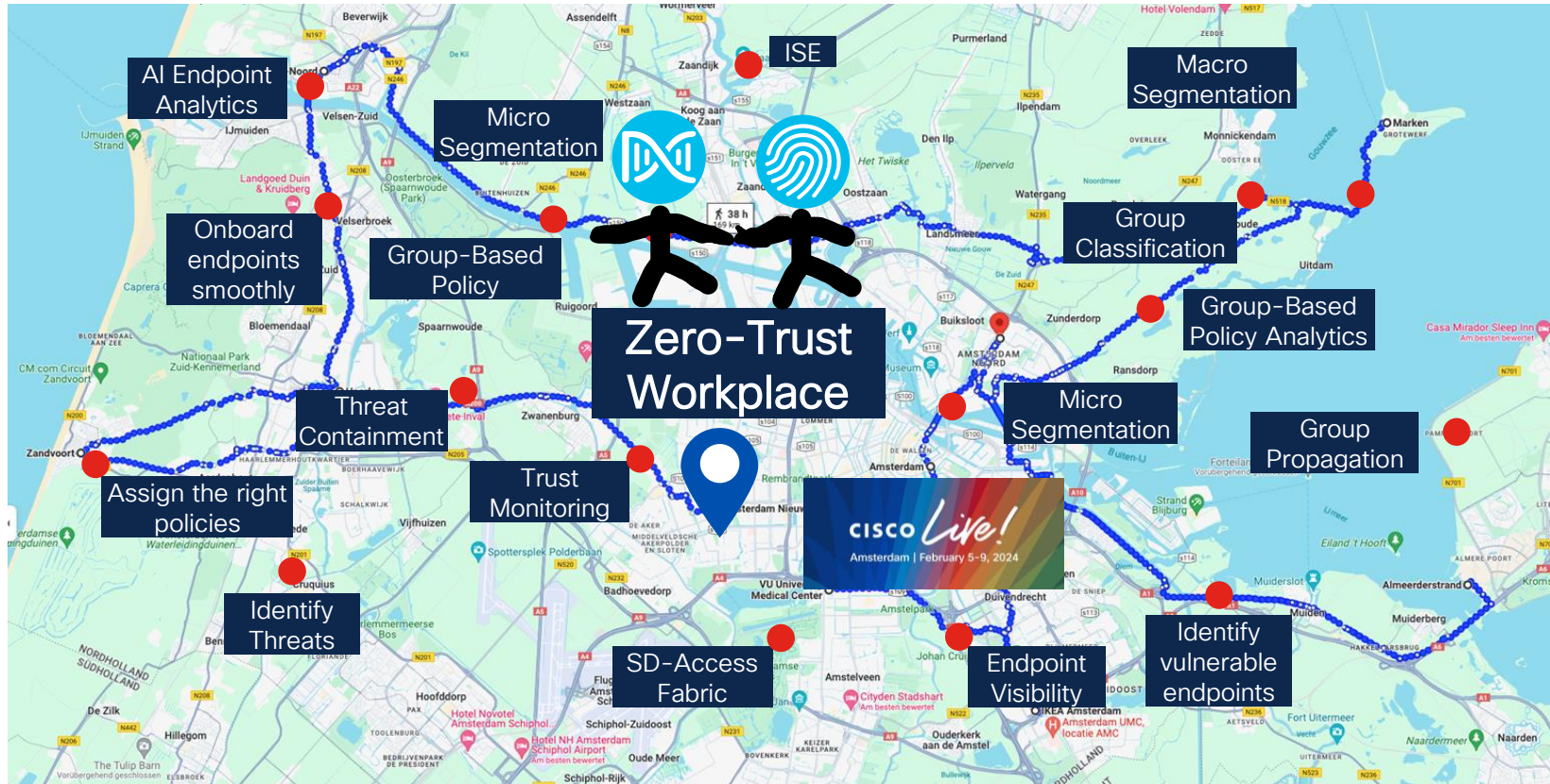
We finished to build a zero-trust campus network

✓ Your Services and Network Settings

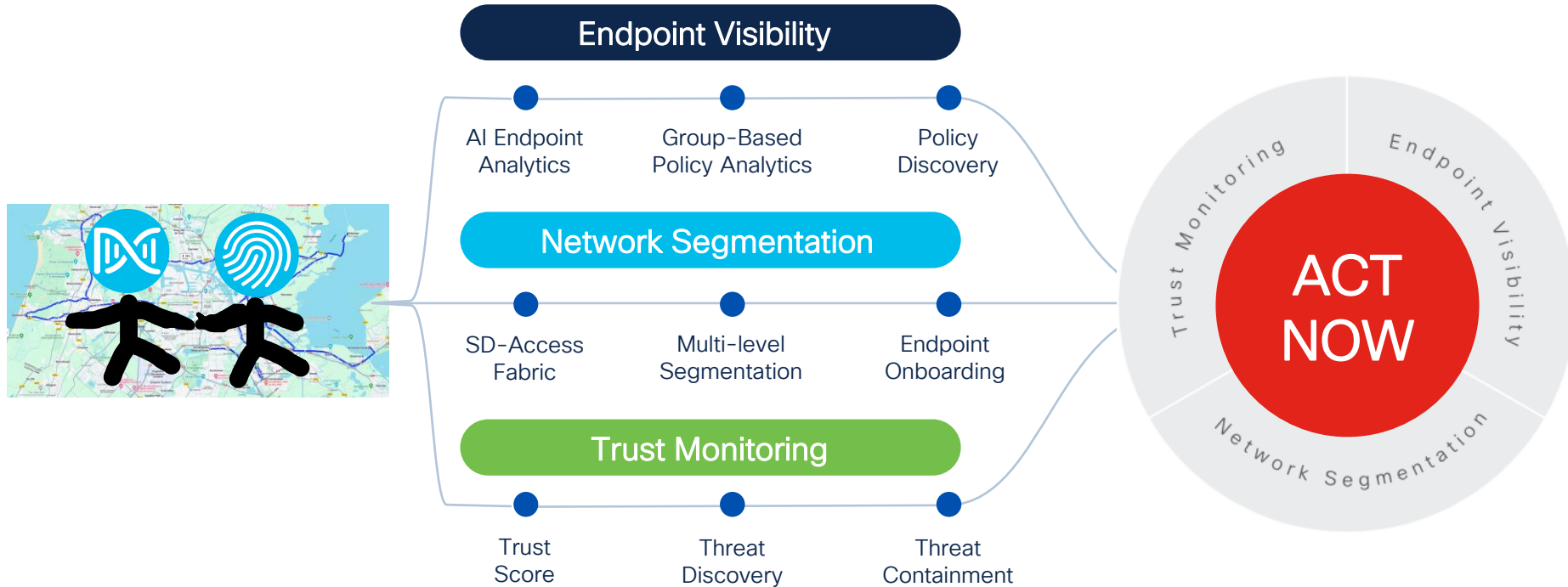
- ✓ CAT9K
- ✓ ISE
- ✓ Talos
- ✓ CBAR



We started our journey with multiple options



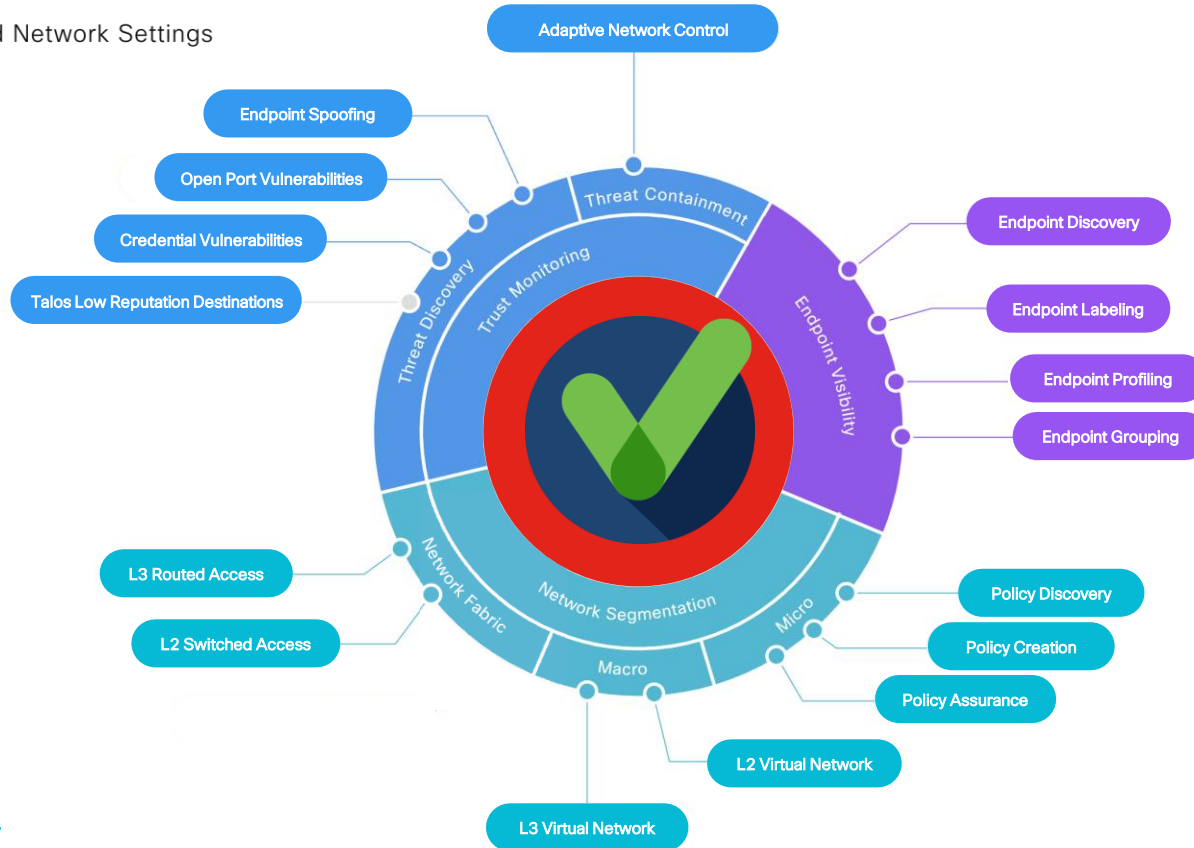
We showed you our recommended path today



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



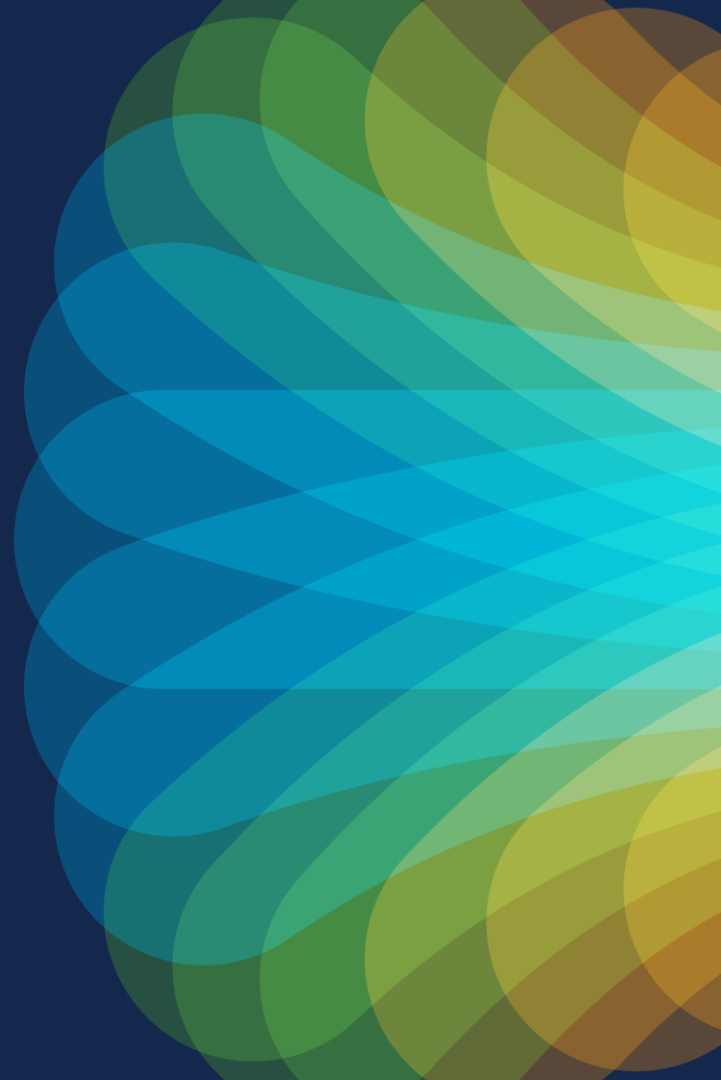
CISCO *Live!*

The background features a vibrant, multi-colored abstract design. On the left, there are horizontal, wavy bands of color in shades of red, orange, yellow, and green. On the right, a bright white light source emits a series of sharp, radiating lines in various colors, including blue, green, and yellow, creating a sunburst effect.

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](#)

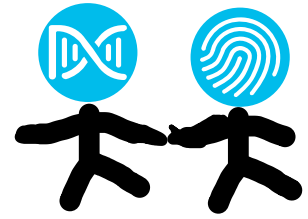
SD-Access

[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/tap/3648009>

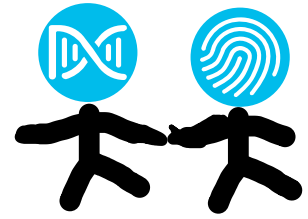
Catalyst Center Documentation Roadmaps

<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](#)

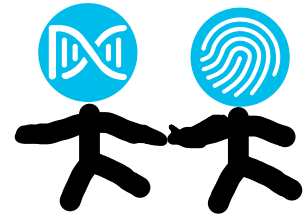
[Case Study: North Carolina DHHS](#)

[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>

The background features a vibrant, multi-colored abstract design. On the left, there are horizontal, wavy bands of color in shades of red, orange, yellow, and green. On the right, a bright white light source emits a series of sharp, radiating lines in various colors, including blue, green, and yellow, creating a sunburst effect.

cisco *Live!*

Let's go