



The bridge to possible

Zero-trust Network Access

SD-Access med Catalyst Center

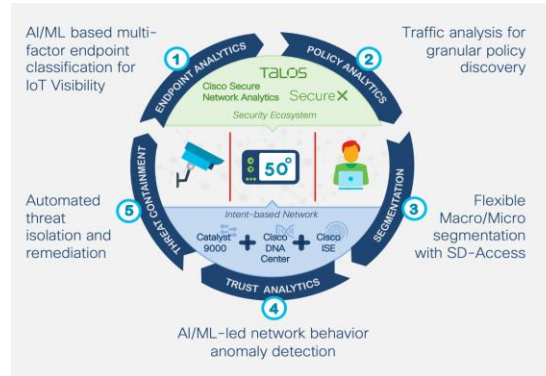
Per Jensen & Rene Andersen

Technical Solution Architects

October-2023

Agenda

1.



2.

Takeaways

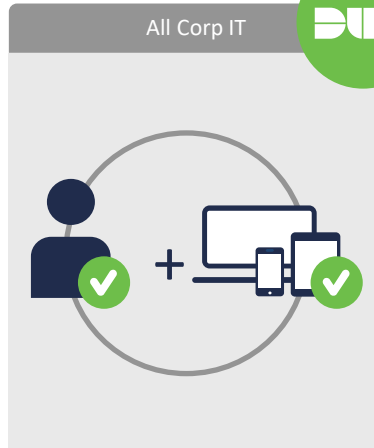
Shift in IT Landscape

Users, devices, and apps are everywhere



Cisco Zero Trust

Secure the Workforce
With Duo

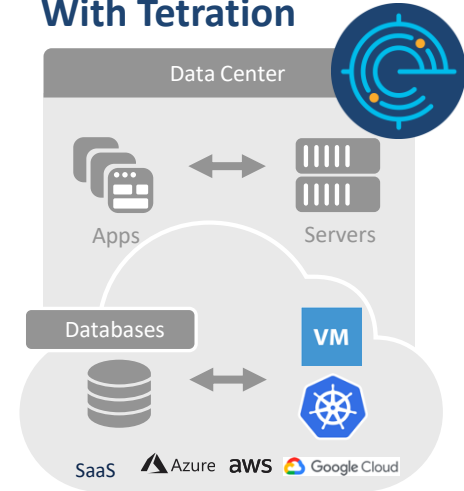


User-bound Device Access



Network Access

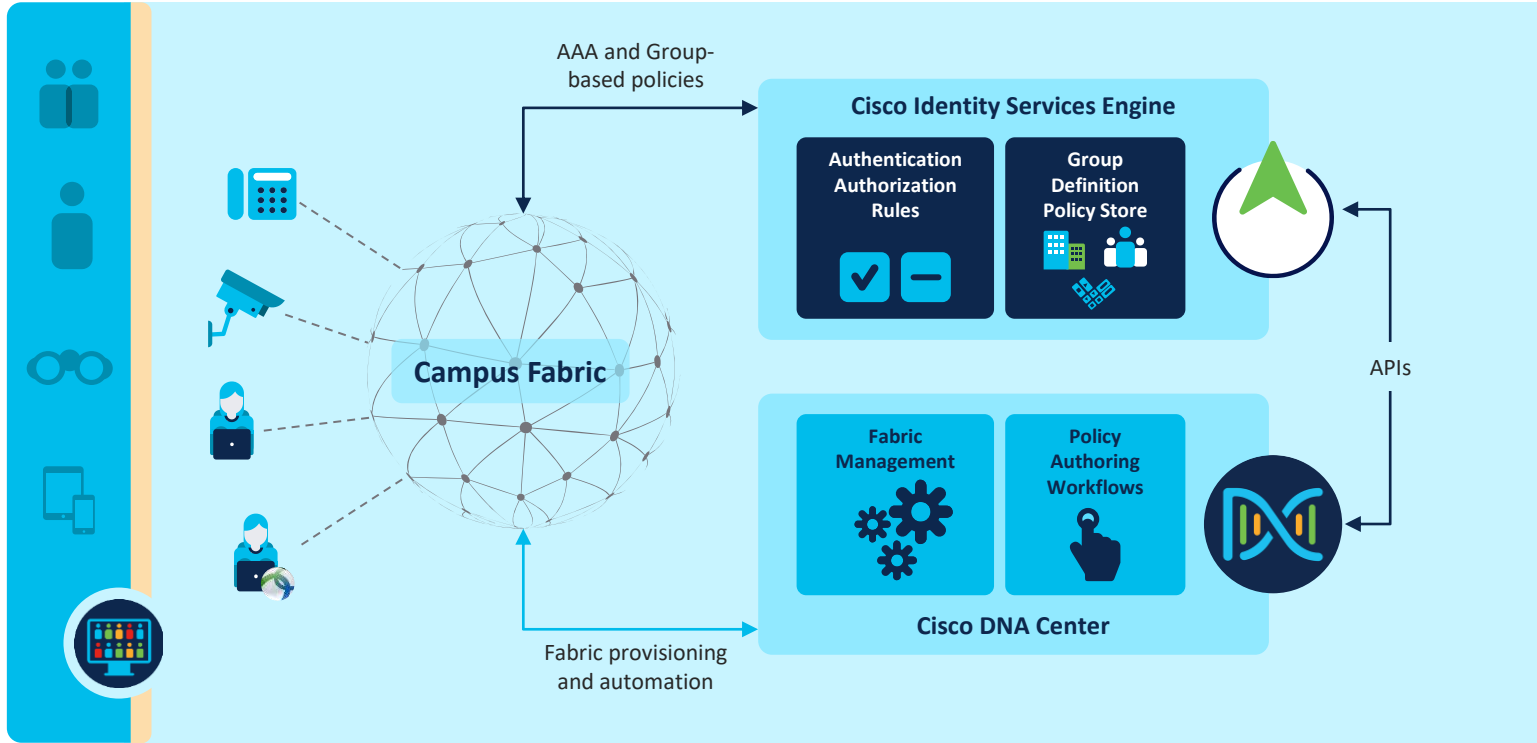
Secure Your Workloads
With Tetration



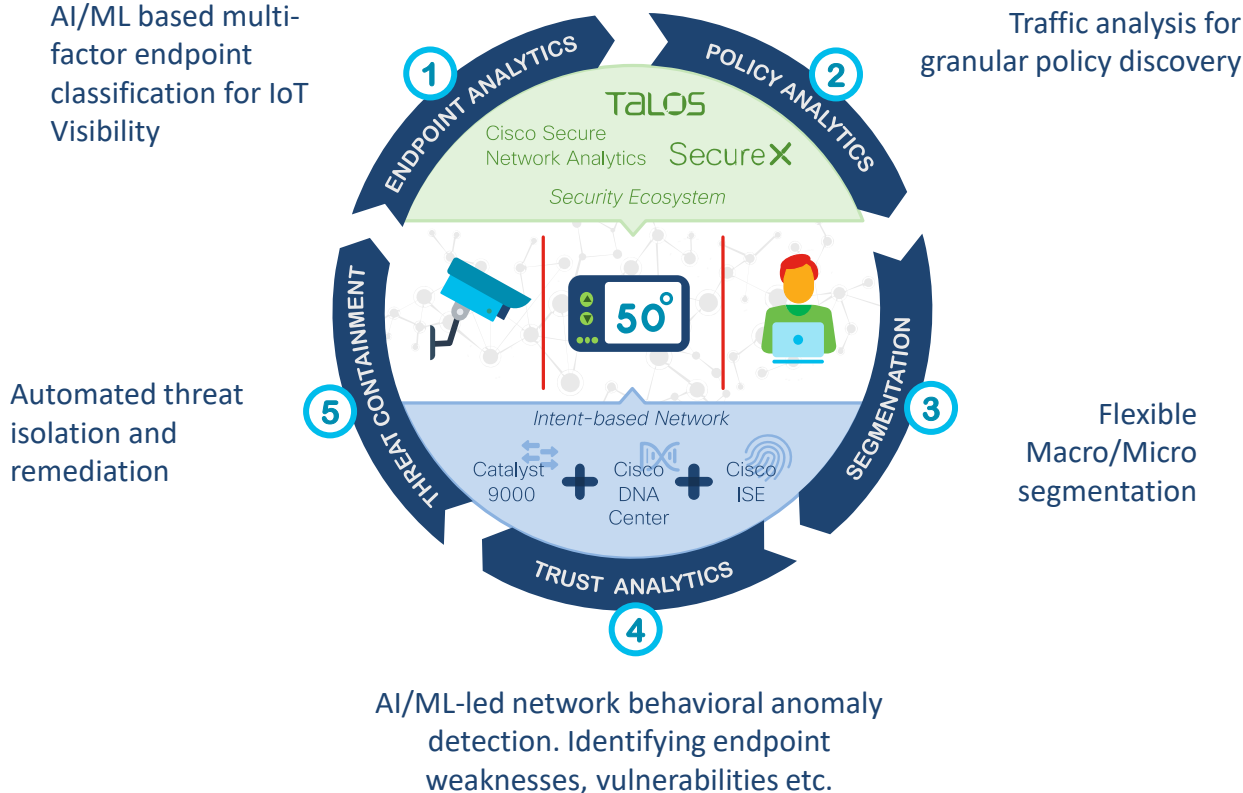
Workload Access

Network segmentation with policy

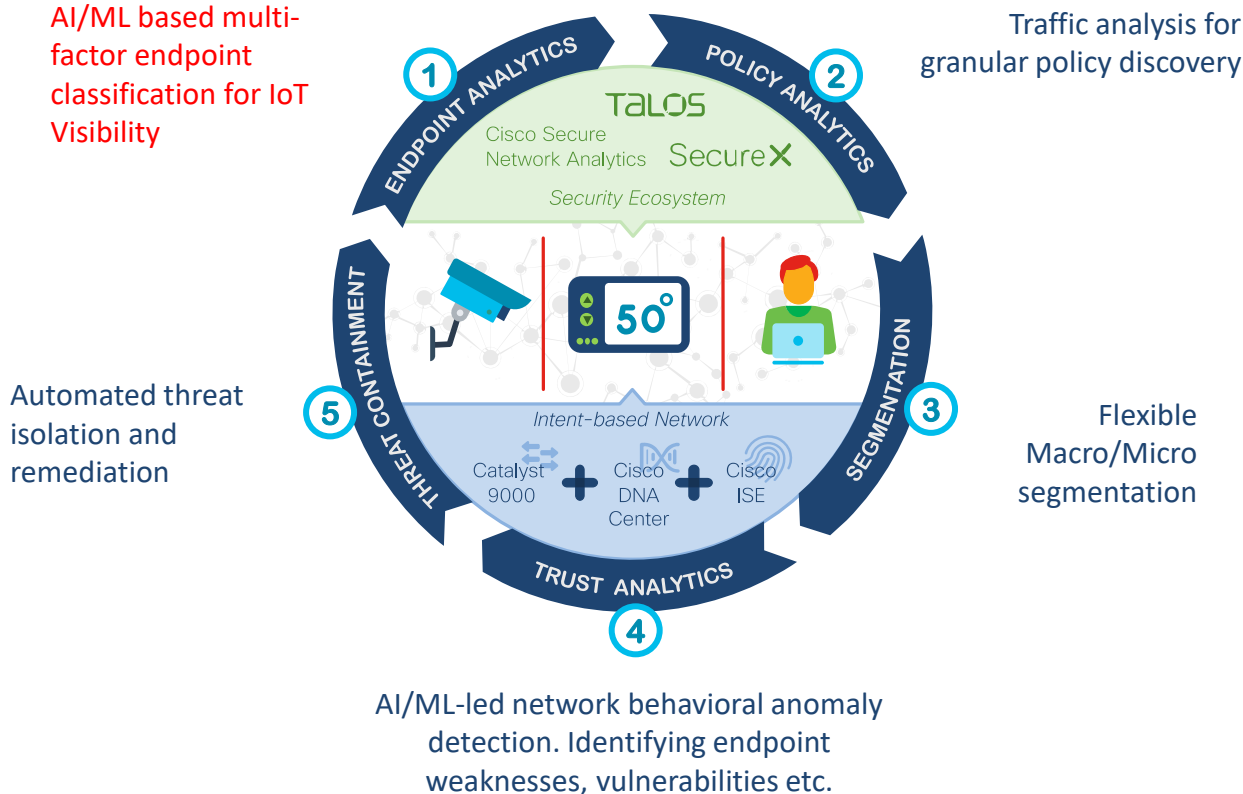
Segmenting with software defined access



SD Access solution for Zero Trust for Workplace



SD Access solution for Zero Trust for Workplace



Cisco ISE for intent-based access

Cisco Identity Services Engine (ISE)
is an industry leading, Network Access Control
and Policy Enforcement platform, that lets
you,

See

Users, endpoints
and applications



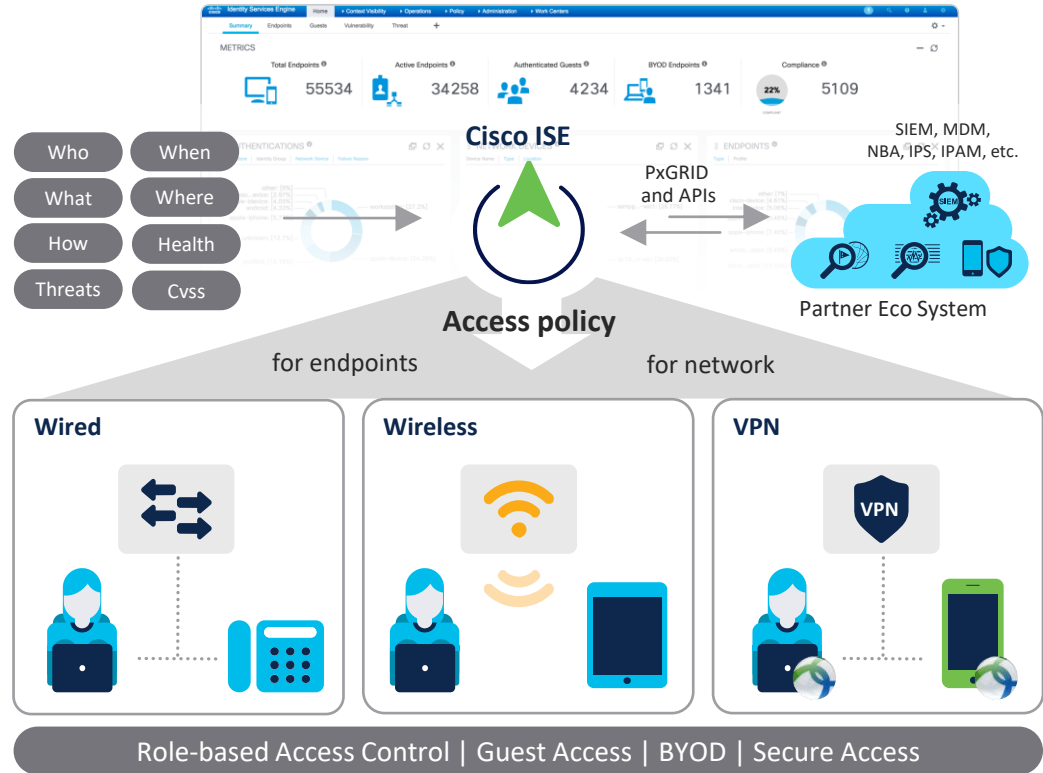
Secure

By controlling network
access and segmentation

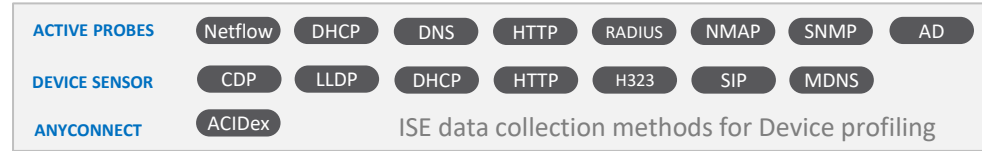


Share

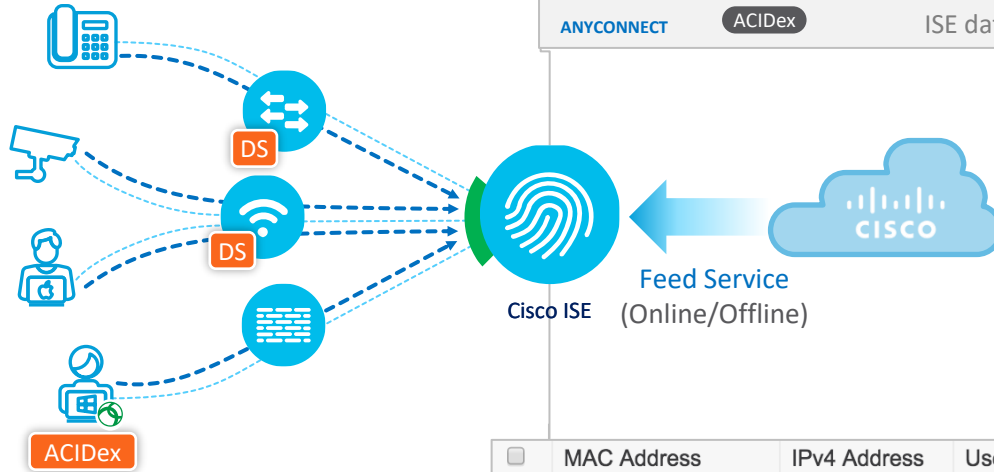
Context with partners for
enhanced operations



Profiling and probes



Endpoints send interesting data, that reveal their device identity



☒ Enable Online Subscription Update

Automatically check for updates every day at hh mm UTC [?](#)

Test result:

☒ Notify administrator when download occurs

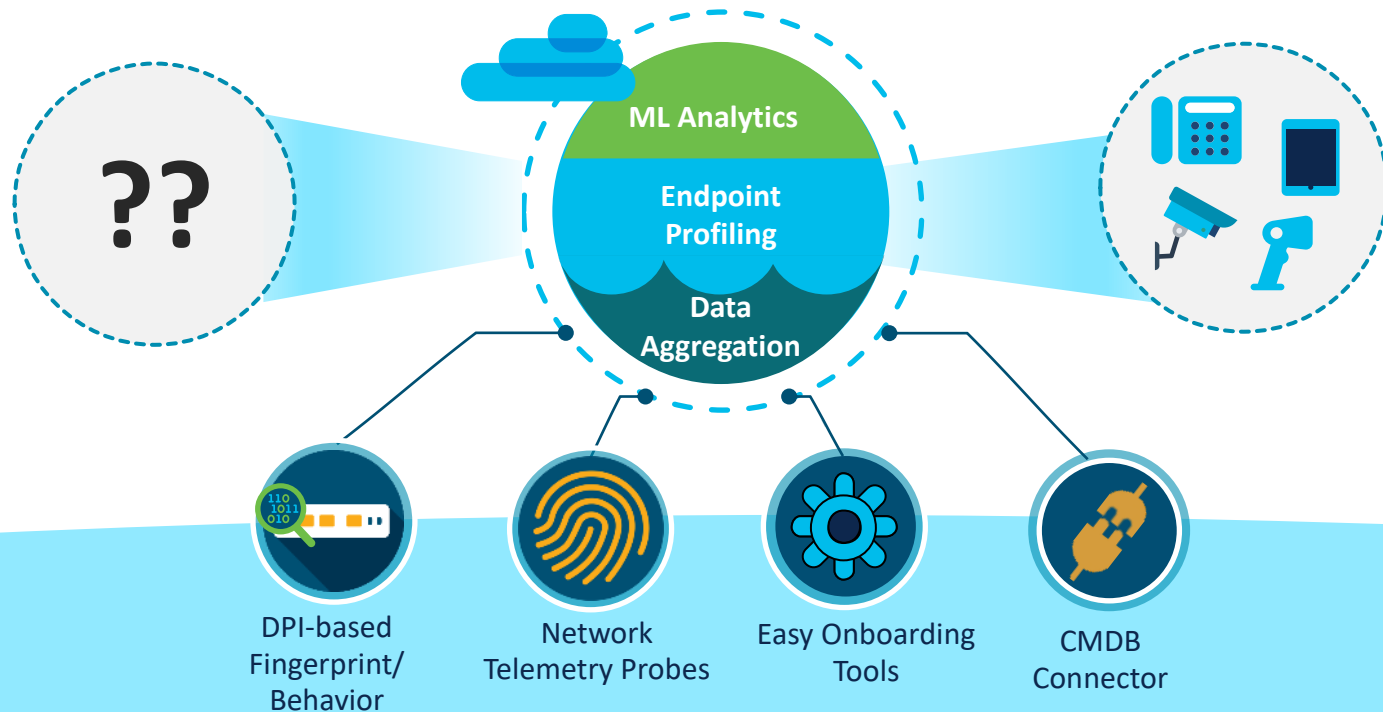
Administrator email address

Profiling helps with differentiated access also for authenticated devices

<input type="checkbox"/>	MAC Address	IPv4 Address	Username	Hostname	Endpoint Profile
×	MAC Address	IPv4 Address	Username	Hostname	Endpoint Profile
<input type="checkbox"/>	00:22:BD:D3:5B:2F	10.34.75.13			Cisco-IP-Camera
<input type="checkbox"/>	00:02:4B:CC:D6:63	10.35.68.203			Cisco-IP-Phone
<input type="checkbox"/>	5C:F9:38:AA:1F:90	10.32.2.127	jim	Jim-Air	Apple-MacBook
<input type="checkbox"/>	30:46:9A:2E:C3:F0	10.86.98.138	host/ALICE	win7pc	Microsoft-Workstation

AI Endpoint Analytics on Cisco DNA Center

Rapidly reducing the unknowns by aggregating data from different sources



CMDB: Configuration Management Database

AI Endpoint Analytics: Multifactor classification

Classifying endpoints using four independent label categories for more flexible profiling



Device type

Laptop

CT scanner

Smartphone



Hardware model

MacBook Pro

Optima CT540

Galaxy S8



Hardware manufacturer

Apple

GE

Samsung



Operating system

MacOS 10.14.6

CTT OS 6.3.x Linux

Android 9.0

Cisco ISE probes and data sources



Unique Cisco ISE probes used in EA

ISE and Third party

RADIUS

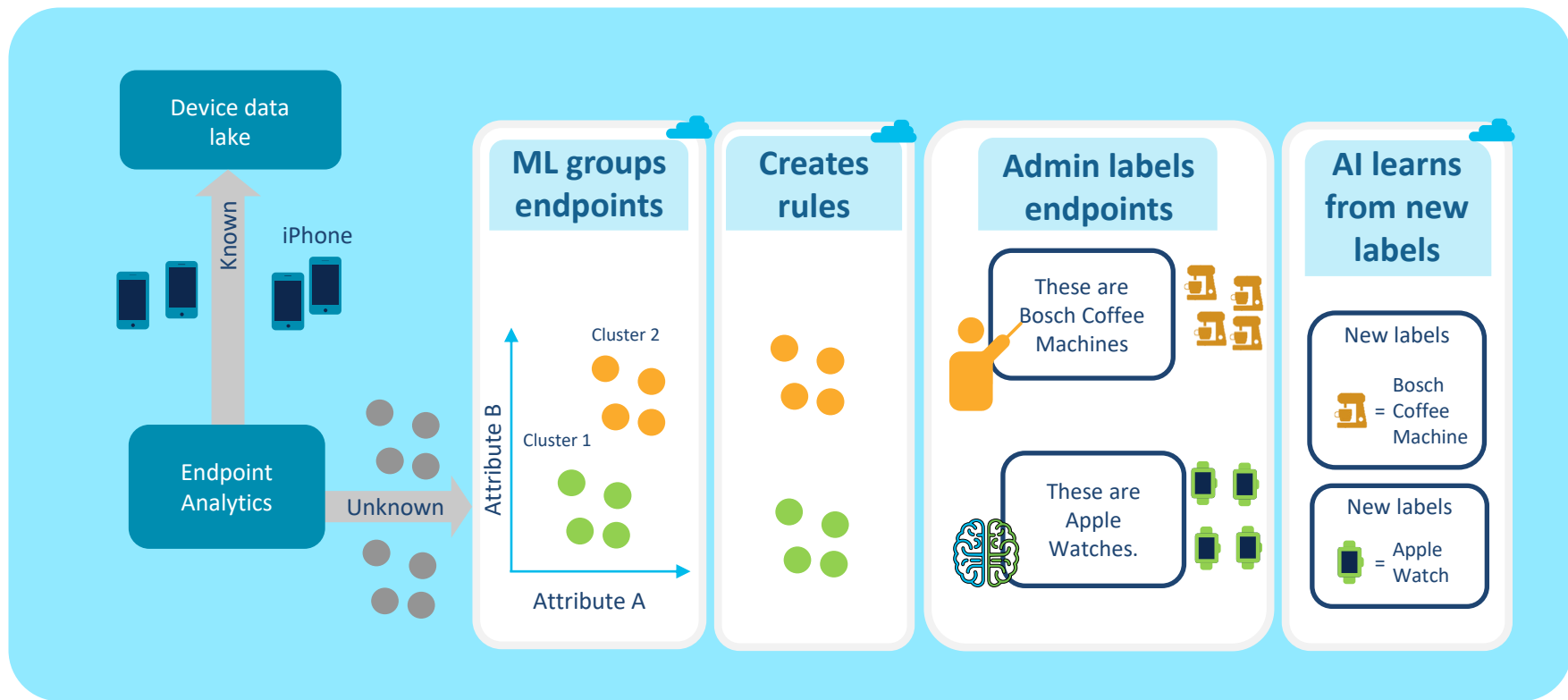
AD

MDM

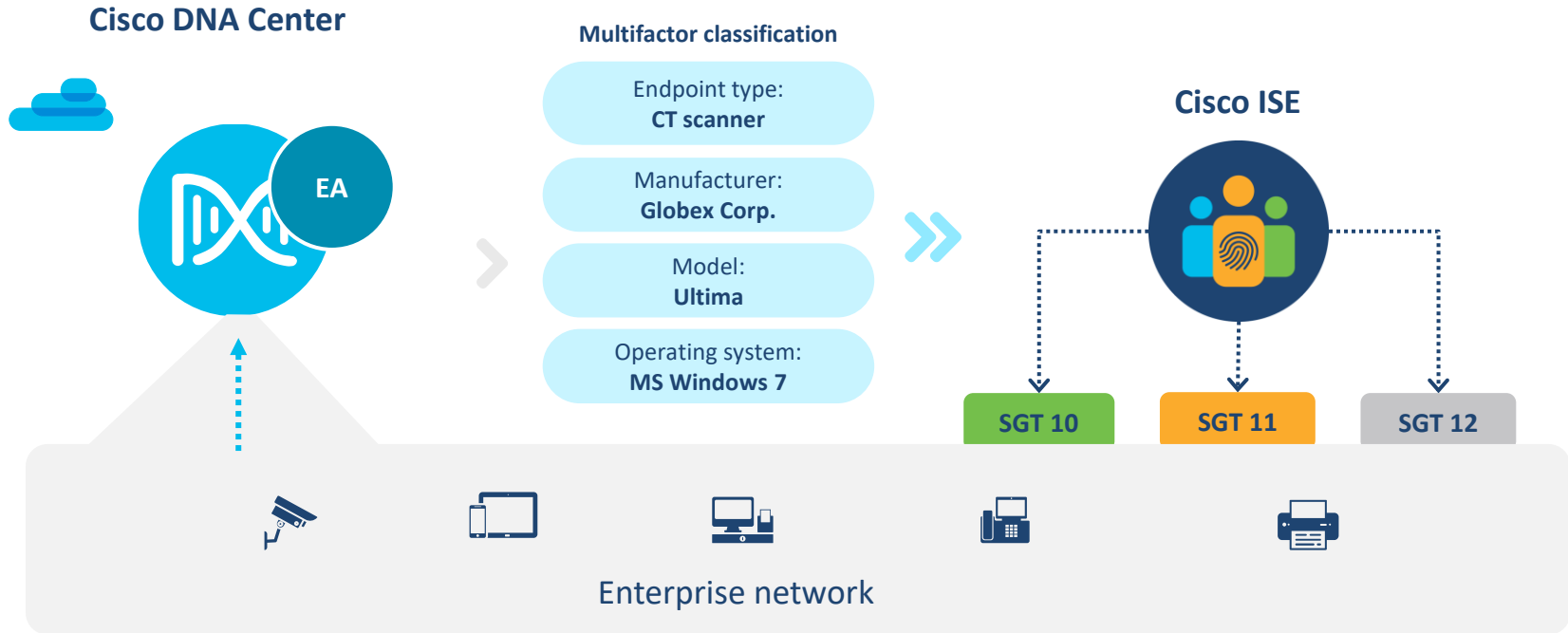
AnyConnect

ACIDex

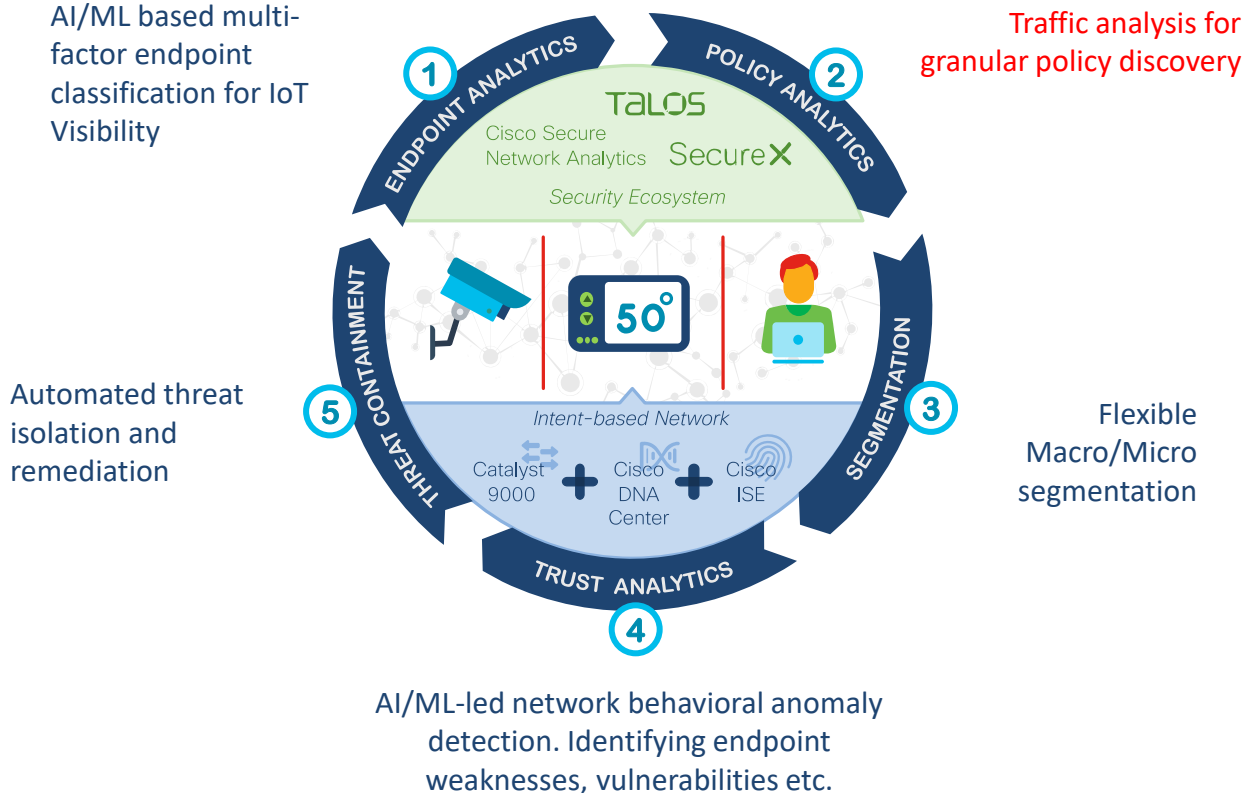
Reducing Unknowns with Machine Learning



Better classification reduces unauthorized access

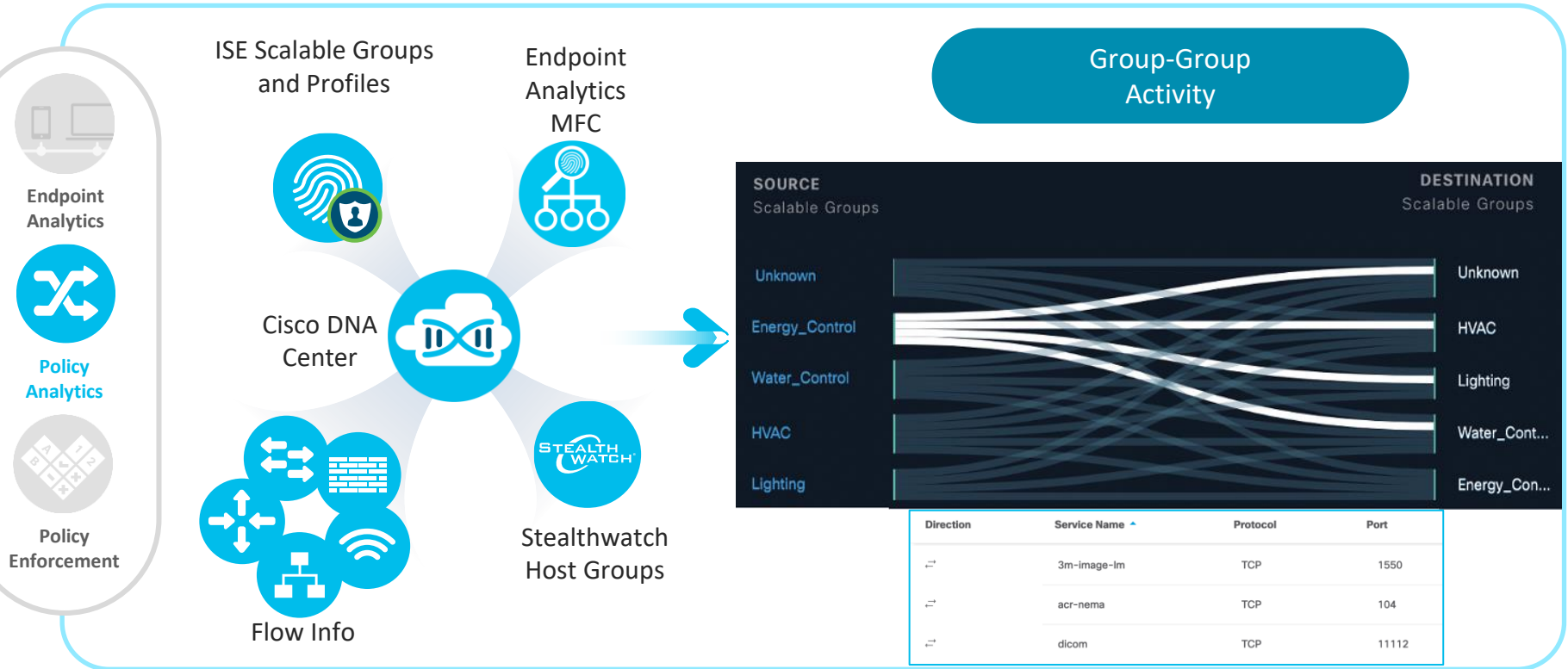


SD Access solution for Zero Trust for Workplace



Group-Based Policy Analytics

...maps traffic between groups



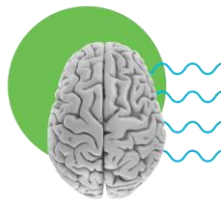
Cisco Secure Network Analytics

Gain confidence in your security effectiveness



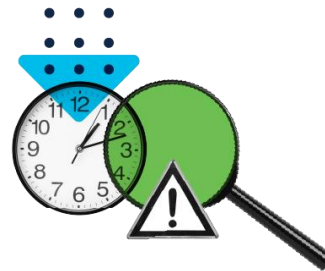
Contextual network-wide visibility

Agentless, using existing
network and cloud infrastructure,
even in encrypted traffic



Predictive threat analytics

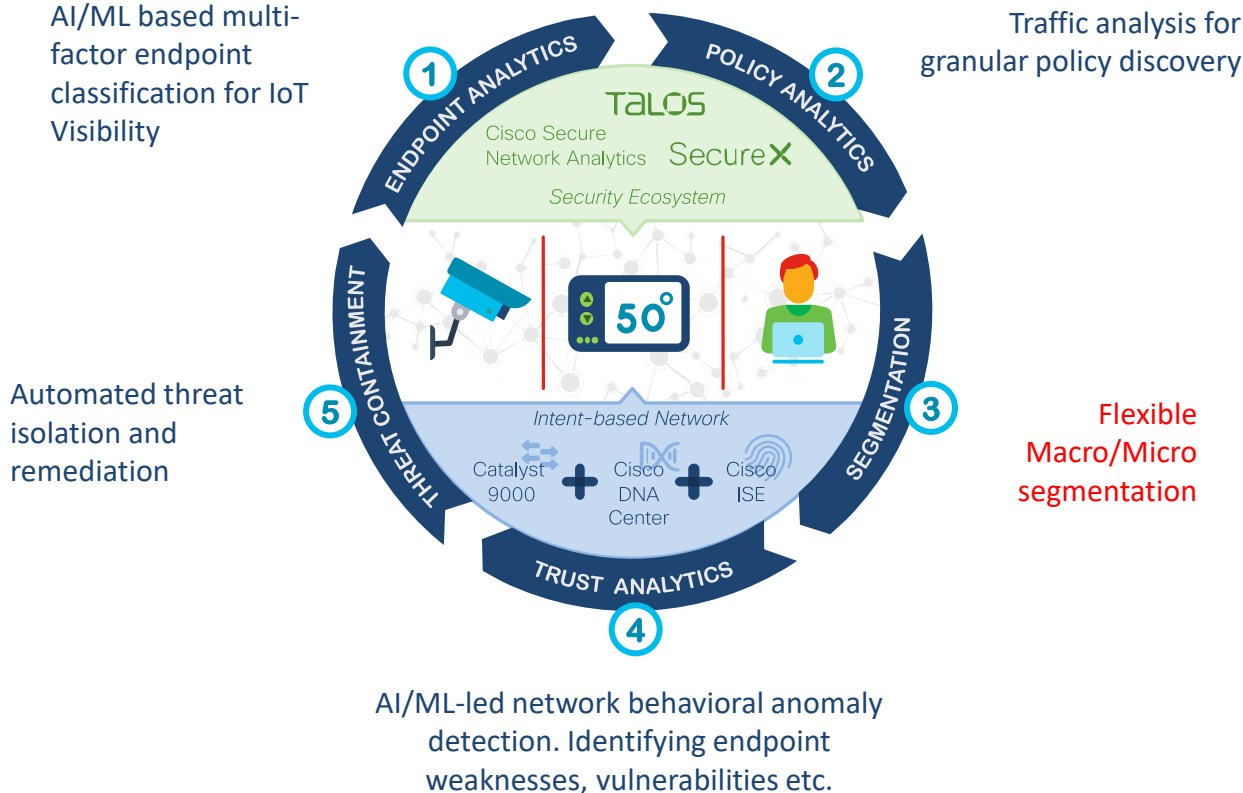
Combination of behavioral modeling,
machine learning and global threat
intelligence



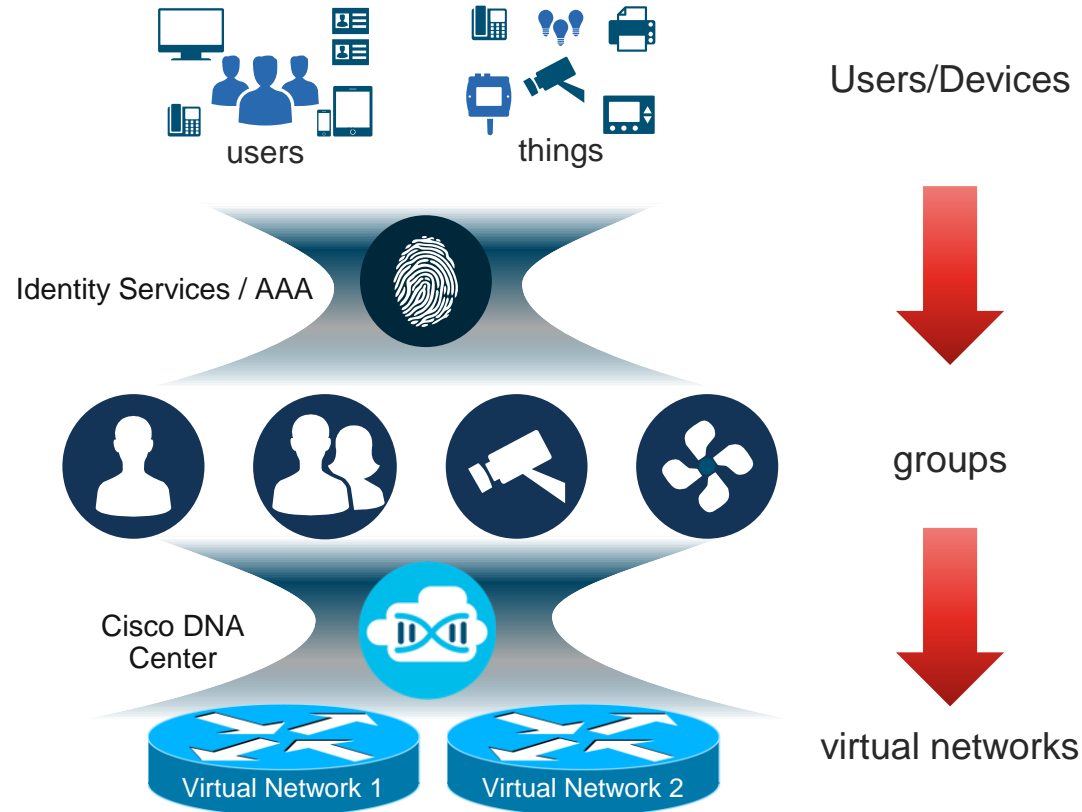
Automated detection and response

High-fidelity alerts prioritized by
threat severity with ability to conduct
forensic analysis

SD Access solution for Zero Trust for Workplace

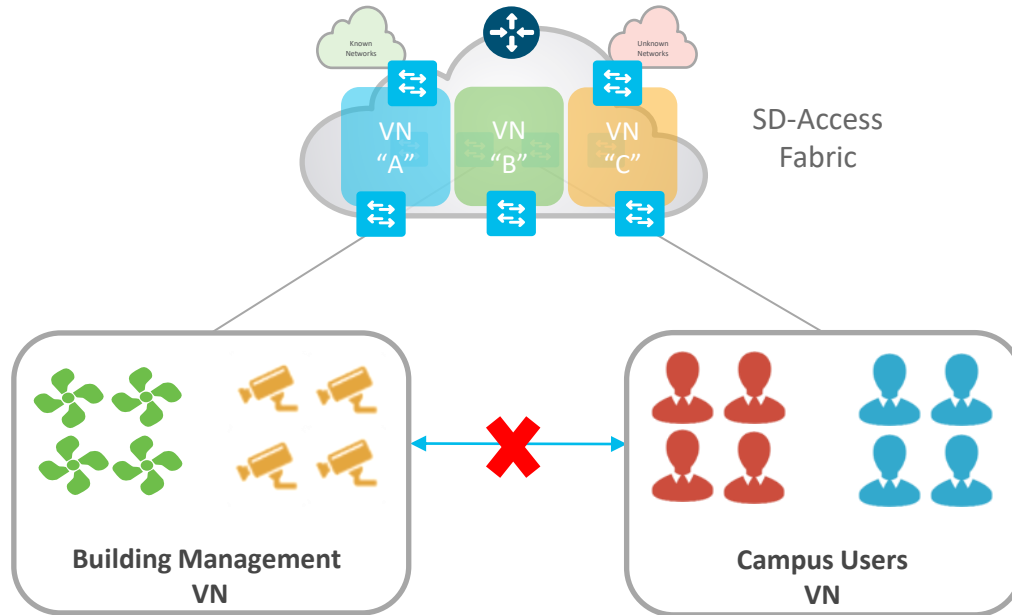


User/Device Groups & Virtual Networks



SD-Access Policy

Two Level Hierarchy - Macro Segmentation

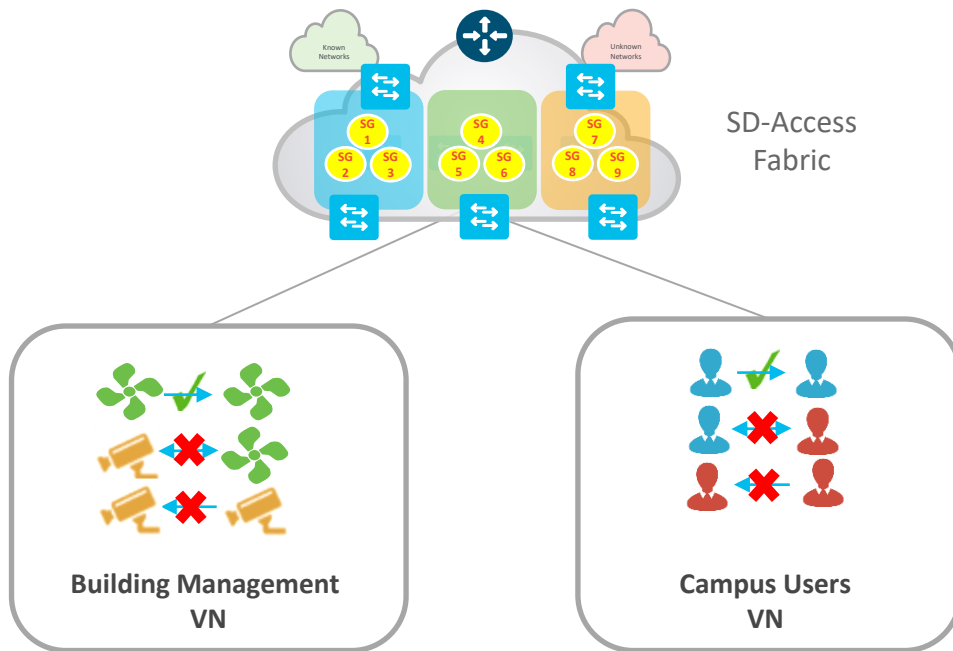


Virtual Network (VN)

First level Segmentation ensures **zero communication** between forwarding domains. Ability to consolidate multiple networks into one management plane.

SD-Access Policy

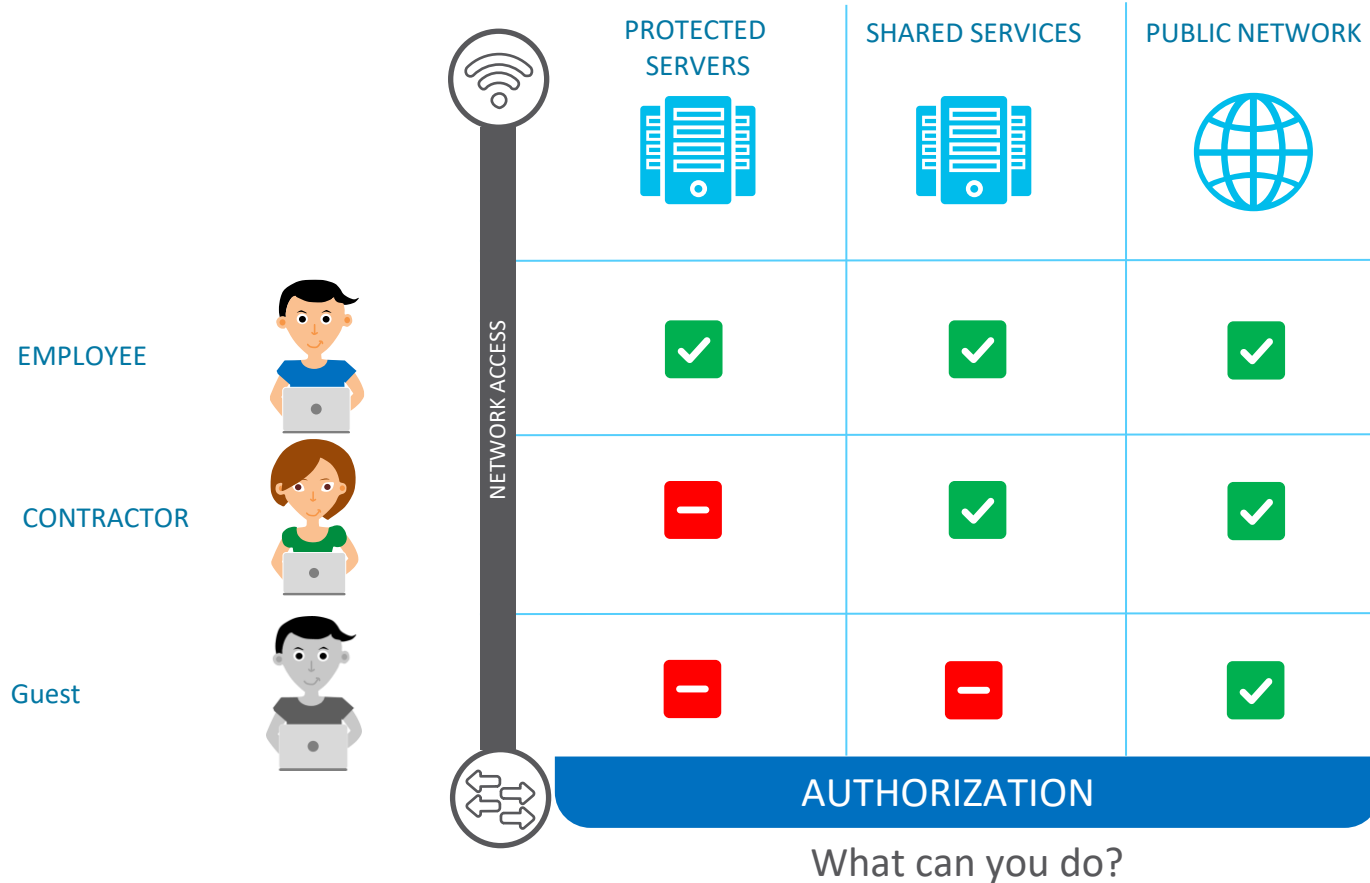
Two Level Hierarchy - Micro Segmentation



Scalable Group (SG)

Second level Segmentation ensures **role based access control** between two groups within a Virtual Network. Provides the ability to segment the network into either line of businesses or functional blocks.

Design your Security Access Policy



SDA design Segmentation

Macro segmentation

VN Name /Function	Description
enterprise	Corporate owned managed and unmanaged Devices. Non-Factory equipment
internet	The Guest VN is intended for all non-employee connection requirements and devices only require Internet access
partner	Corporate owned device, but managed by external Partners
factory	Corporate owned manage / unmanaged End-points Used in the Factories
Unknown / Future	Not yet specified

Micro segmentation

VN Name / Function	SGT Name	Description
enterprise	Enterprise-Devices	PC / MAC, Corporate owned managed End-points
	IP-Phones	Corporate owned managed End-points
	Video	Corporate owned managed End-points
	Printers	Office area print services, Corporate owned unmanaged End-points
	Mdev	Corporate owned unmanaged End-points
internet	Guest	The Guest VN is intended for all non-employee connection requirements
	Internet-Only	Devices only require Internet access
	Mobile-Phones	Only require Internet access
partner	Alarm-Systems	Corporate owned unmanaged End-points
	Access-Control	Corporate owned unmanaged End-points
	Camera	Corporate owned unmanaged End-points
	UPS	Corporate owned unmanaged End-points
	Time-Terminals	Corporate owned unmanaged End-points
	Building-Mngt	Corporate owned unmanaged End-points
factory		
	Handheld-Terminals	Corporate owned unmanaged End-points
	PLC	Corporate owned unmanaged End-points
	CNC	Corporate owned unmanaged End-points
	NAT-Router	Corporate owned managed device
Unknown / Future		

Why SD-Access?

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



Automated threat isolation and remediation

Traffic analysis for granular policy discovery

AI/ML-led network behavior anomaly detection

Flexible Macro/Micro segmentation with SD-Access

1

Simplified Migration

- Preserve existing network blueprints when migrating to Fabric from traditional designs

2

Simplified Operations

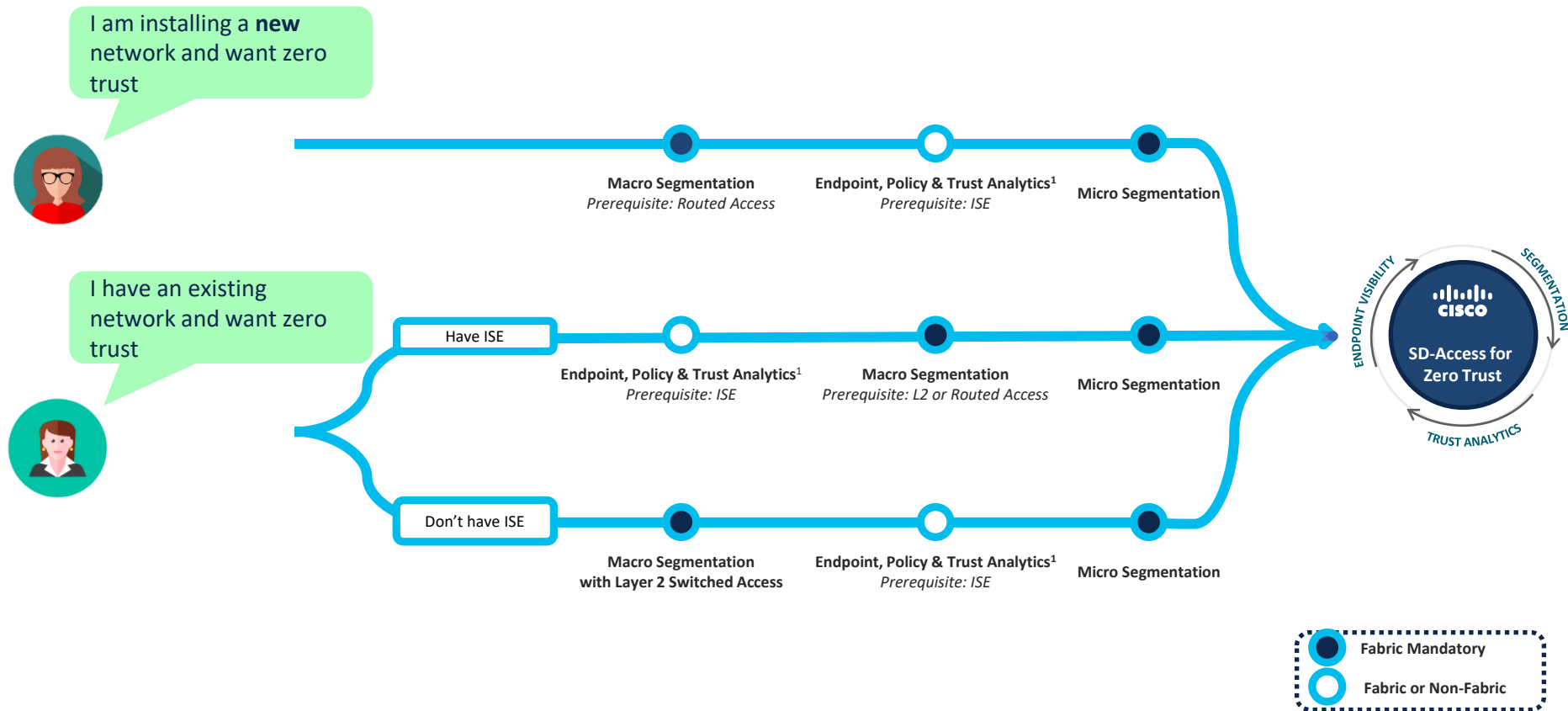
- Intent-based
- Advanced workflows

3

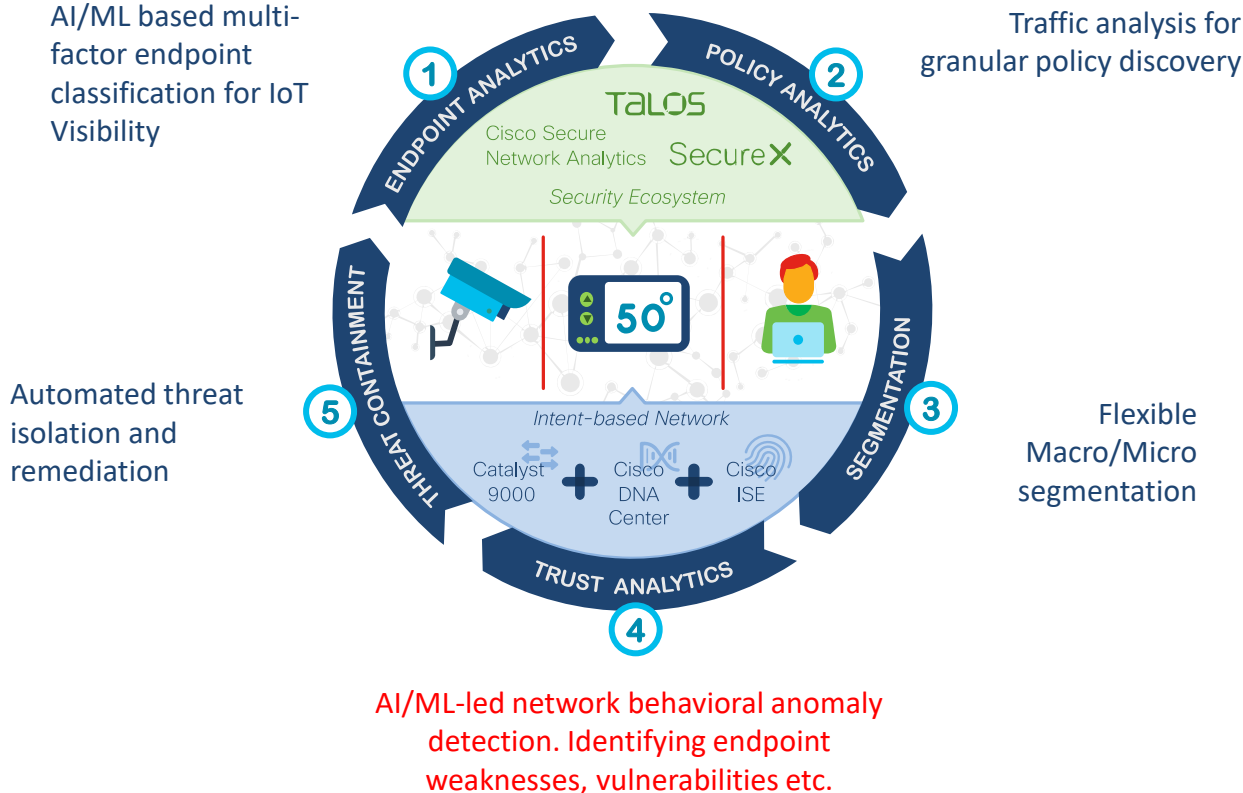
Assurance

- SDA

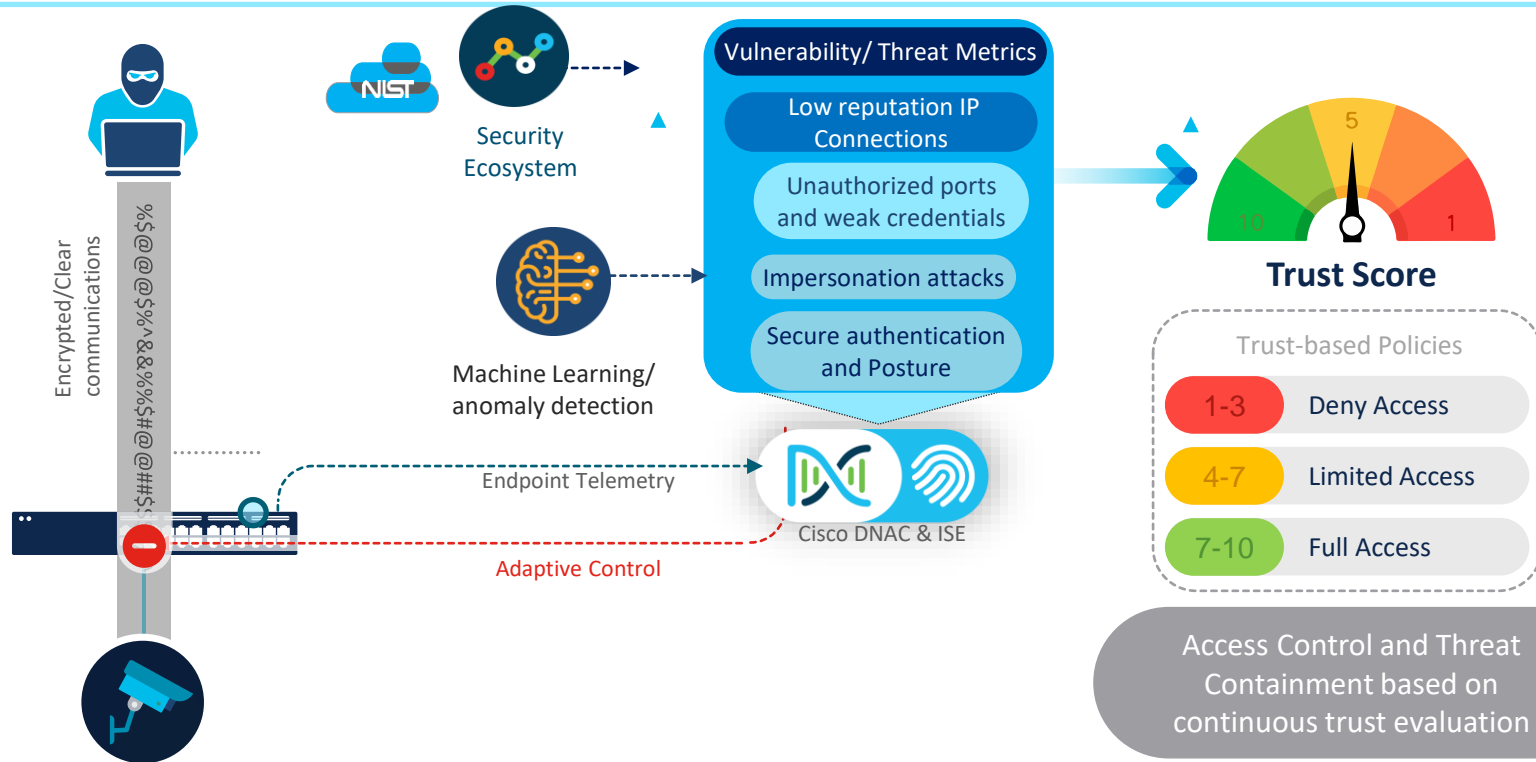
Flexible Start Options removes barriers to Quick Value



SD Access solution for Zero Trust for Workplace



Continuously monitor endpoint trust



Trust Sources and impact on Trust score

Positive Influence

- Secure Authentication
- Posture Compliance

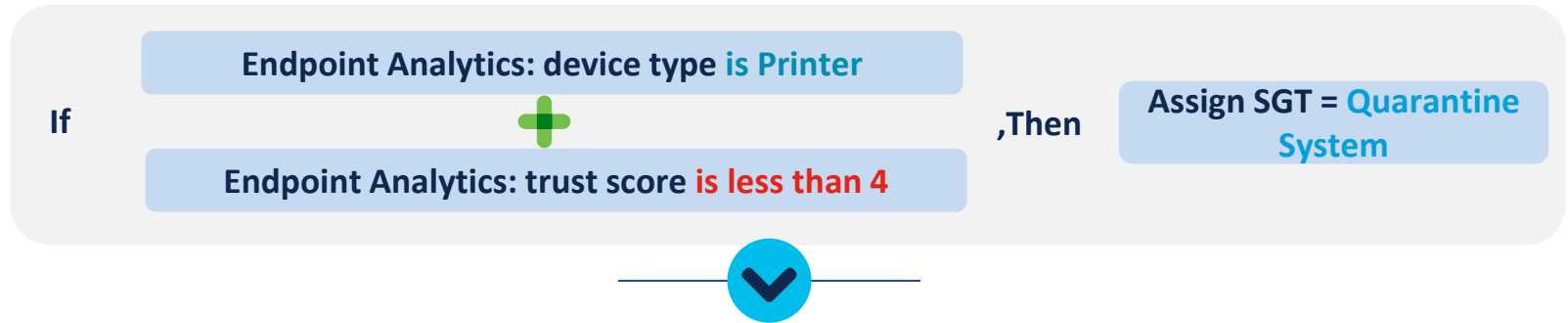


Negative Influence

- MAC spoofing/
Attribute spoofing
- Unauthorized open
TCP/UDP ports
- Weak Credentials
- Behind NAT device
- Contacting destinations
marked by TALOS

Using Endpoint Analytics attributes in authorization policy

For example, authorization policy for **Low Trust - Printers**:



<div><div></div></div> +	Status	Rule Name	Conditions		Security Groups
<div><div></div> Search</div>					
	<div><div></div></div>	Low Trust - Printers	AND	<div><div></div> Endpoint-Analytics-trustScore LESS 4</div> <div><div></div> Endpoint-Analytics-deviceType EQUALS Printers</div>	<div>Quarantined_Systems<div><div></div></div></div>



AI Endpoint Analytics works for endpoints coming to Cisco DNA Center from ISE running one of (2.4.0.357 Patch 11+ or 2.6.0.156 Patch 4+ or 2.7.0.356 Patch 1+ or 3.0 onwards) OR Cisco Catalyst 9000 series access devices, Cisco Traffic Telemetry Appliance running IOS-XE 17.3.1 or later.

[Overview](#)[Endpoint Inventory](#)[Profiling Rules](#)[Hierarchy](#)

Trust Score (12)

Focus: [Trust Score](#) [Take a Tour](#)

Search



















0 Selected

[More Actions](#) 

As of: May 23, 2022 11:50 AM



<input type="checkbox"/>	MAC Address 	Endpoint Trust Score 	IP Address	Authentication Method	Posture	AI Spoofing Detection	Changed Profile Labels	NAT Mode Detection	Conc
<input type="checkbox"/>	B8:27:EB:8C:C8:26	 1	10.1.137.11	 WiredMAB (Lookup)	-	 10	-	-	-
<input type="checkbox"/>	B8:27:EB:A4:05:1F	 8	10.1.128.11	 WiredMAB (Lookup)	-	-	-	-	-
<input type="checkbox"/>	B8:27:EB:D9:9D:73	 5	10.1.136.23	 Wireless802_1x (PEAP (EAP-MSCHAPv2))	-	 4	-	-	-
<input type="checkbox"/>	B8:27:EB:F1:50:4A	 8	10.1.136.24	 Wireless802_1x (PEAP (EAP-MSCHAPv2))	-	-	-	-	-
<input type="checkbox"/>	DC:A6:32:71:33:43	 9	10.1.142.88	 Wireless802_1x (PEAP (EAP-MSCHAPv2))	-	-	-	-	-
<input type="checkbox"/>	DC:A6:32:71:35:DA	 8	10.1.137.28	 Wireless802_1x (PEAP (EAP-MSCHAPv2))	-	-	-	-	-

AI Endpoint Analytics works for endpoints coming to Cisco DNA Center from ISE running one of the following versions: Cisco ISE 3.10(1) or later, Cisco Traffic Telemetry Appliance running IOS-XE 17.3.1 or later.

Overview **Endpoint Inventory** Profiling Rules Hierarchy

Trust Score (12) Focus: **Trust Score**

Search

0 Selected

More Actions

<input type="checkbox"/>	MAC Address	Endpoint Trust Score	IP Address	Authentication Method
<input type="checkbox"/>	B8:27:EB:8C:C8:26	1	10.1.137.11	WiredMAB (Lookup)
<input type="checkbox"/>	B8:27:EB:A4:05:1F	8	10.1.128.11	WiredMAB (Lookup)
<input type="checkbox"/>	B8:27:EB:D9:9D:73	5	10.1.136.23	Wireless802_1x (Profile)
<input type="checkbox"/>	B8:27:EB:F1:50:4A	8	10.1.136.24	Wireless802_1x (Profile)
<input type="checkbox"/>	DC:A6:32:71:33:43	9	10.1.142.88	Wireless802_1x (Profile)
<input type="checkbox"/>	DC:A6:32:71:35:DA	8	10.1.137.28	Wireless802_1x (Profile)

B8:27:EB:8C:C8:26

Hostname raspi3-3-Eschborn Trust Score 1

This endpoint has a low trust score of 1 and needs immediate attention. [View Trust Score Details](#)

Details **Trust Score** Attributes

Trust Score Total: 1

Endpoint Authentication and Compliance

> Authentication Method WiredMAB (Lookup) Last Authenticated: May 06, 2022 09:33 AM

> Posture Not Detected

Endpoint Anomaly Detection

> AI Spoofing Detection 10 Last Scored: Apr 25, 2022 06:00 PM

> Changed Profile Labels Not Detected

> Concurrent MAC Address Not Detected

AI Endpoint Analytics works for endpoints coming to Cisco DNA Center from ISE running one of the following versions: ISE 3.10 or later, Cisco Traffic Telemetry Appliance running IOS-XE 17.3.1 or later.

Overview **Endpoint Inventory** Profiling Rules Hierarchy

Trust Score (12) Focus: **Trust Score** ▾

Q Search

0 Selected

More Actions ▾

<input type="checkbox"/>	MAC Address	Endpoint Trust Score	IP Address	Authentication Method
<input type="checkbox"/>	B8:27:EB:8C:C8:26	1	10.1.137.11	WiredMAB (Lookup)
<input type="checkbox"/>	B8:27:EB:A4:05:1F	8	10.1.128.11	WiredMAB (Lookup)
<input type="checkbox"/>	B8:27:EB:D9:9D:73	5	10.1.136.23	Wireless802_1x (Profile)
<input type="checkbox"/>	B8:27:EB:F1:50:4A	8	10.1.136.24	Wireless802_1x (Profile)
<input type="checkbox"/>	DC:A6:32:71:33:43	9	10.1.142.88	Wireless802_1x (Profile)
<input type="checkbox"/>	DC:A6:32:71:35:DA	8	10.1.137.28	Wireless802_1x (Profile)

Trust Score Total: 1

Endpoint Authentication and Compliance

> Authentication Method WiredMAB (Lookup) Last Authenticated: May 06, 2022 09:33 AM

> Posture Not Detected

Endpoint Anomaly Detection

AI Spoofing Detection 10 Last Scored: Apr 25, 2022 06:00 PM

AI Spoofing Detection detects when an endpoint is being spoofed by comparing endpoint behaviour to that of AI based behaviour models. AI Spoofing Detection runs on-premise on your Cisco DNA Center appliances and does not send any data to the cloud.

Severity 100 Confidence 100

Severity

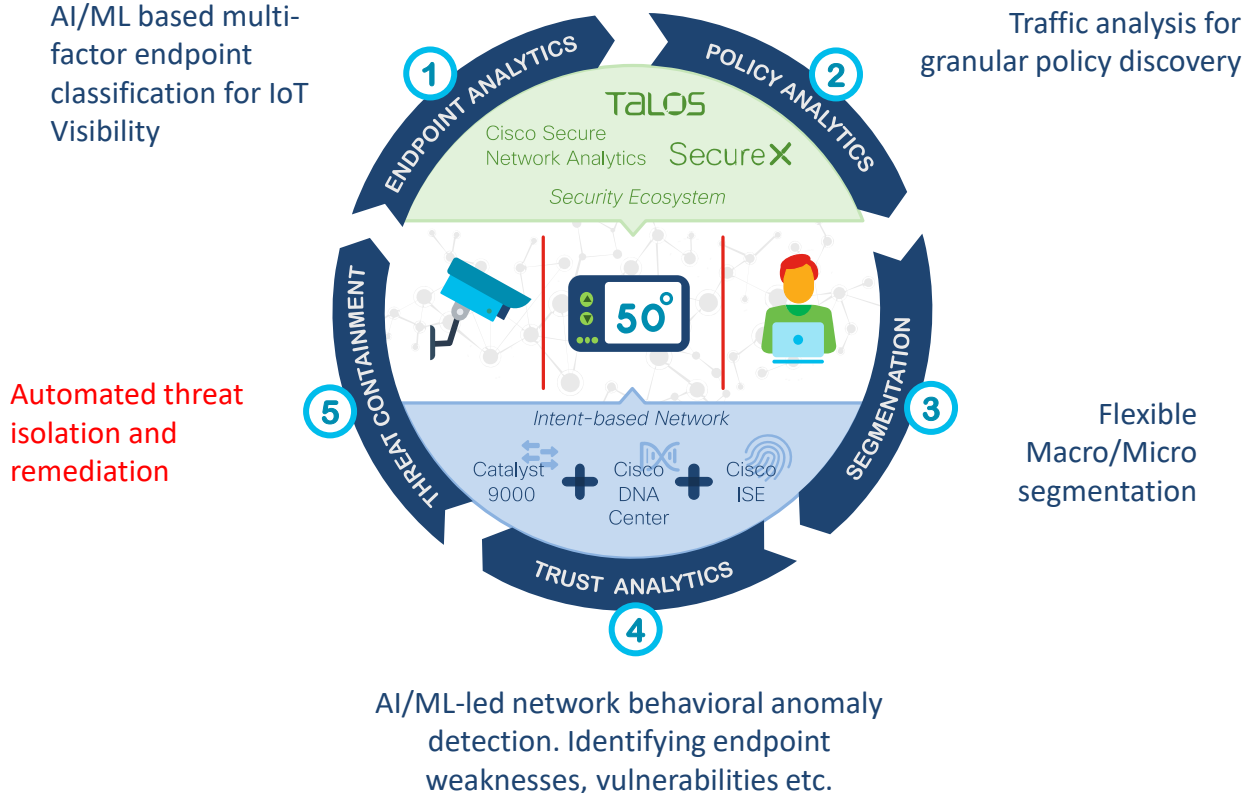
Expected Endpoint Type IP Phone

Anomalous Applications
client-https
server-ssh
client-youtube
client-spiegel-online




Enabled

SD Access solution for Zero Trust for Workplace




AI Endpoint Analytics works for endpoints coming to Cisco DNA Center from ISE running one of the following versions: ISE 2.6 or later, Cisco Access Router Controller running IOS-XE 17.3.1 or later.

Trust Score Total: ● 1 

Endpoint Authentication and Compliance

Overview **Endpoint Inventory** Profiling Rules Hierarchy

Trust Score (12) Focus: **Trust Score** 

 Search

0 Selected **More Actions** 

☐ MAC Address  Endpoint Trust

☐ B8:27:EB:8C:C8:26 ● 1

☐ B8:27:EB:A4:05:1F ● 8

☐ B8:27:EB:D9:9D:73 ● 5

☐ B8:27:EB:F1:50:4A ● 8

☐ DC:A6:32:71:33:43 ● 9

Apply ANC Policy

Choose an ANC Policy to apply to **B8:27:EB:8C:C8:26**. Doing so will affect the endpoints accessibility to your network based on the ANC Policy applied.

Apply ANC Policy 

 Don't see a policy you like?

 Search

ReAuthSystem

ShutdownSystem

PortBounce

Cancel

Apply

TAKEAWAY

Basic Tenant of Zero Trust

The effect of Zero Trust is

*Ubiquitous
Least-Privilege
Access*

(i.e., grant access,
but make it specific!)

CPH University 5th Best Uni in Europe, running SDA why?

C9K

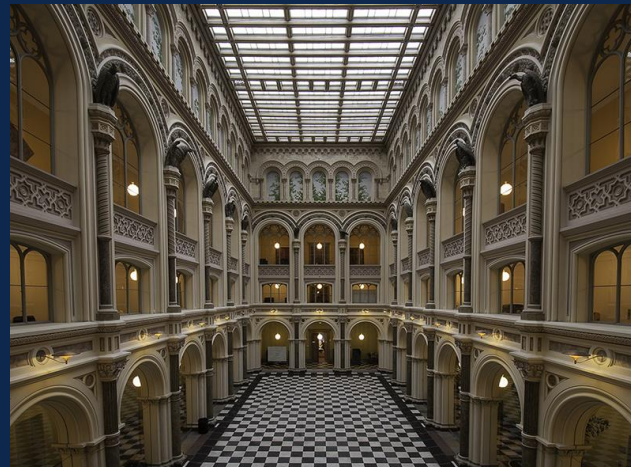
SDA (Catalyst Center)

ISE

Cisco Secure Analytics (Stealthwatch)

Common policy and the ability to Isolate threats in real-time

Focus on Automation, Segmentation and ZeroTrust





Sasa Dervovic

Head of Network and Data Center
at University of Copenhagen

in

t

f

LINK

A Modern University Raises the Bar: A Network Infrastructure That's Secure, Agile, and Invisible Based on Cisco DNA

[Change cookie settings](#)

<https://upshotstories.com/stories/a-modern-university-raises-the-bar-a-network-infrastructure-that-s-secure-agile-and-invisible-based-on-cisco->

KU SDA HDtools Automation

Christian Vesth
Network Specialist

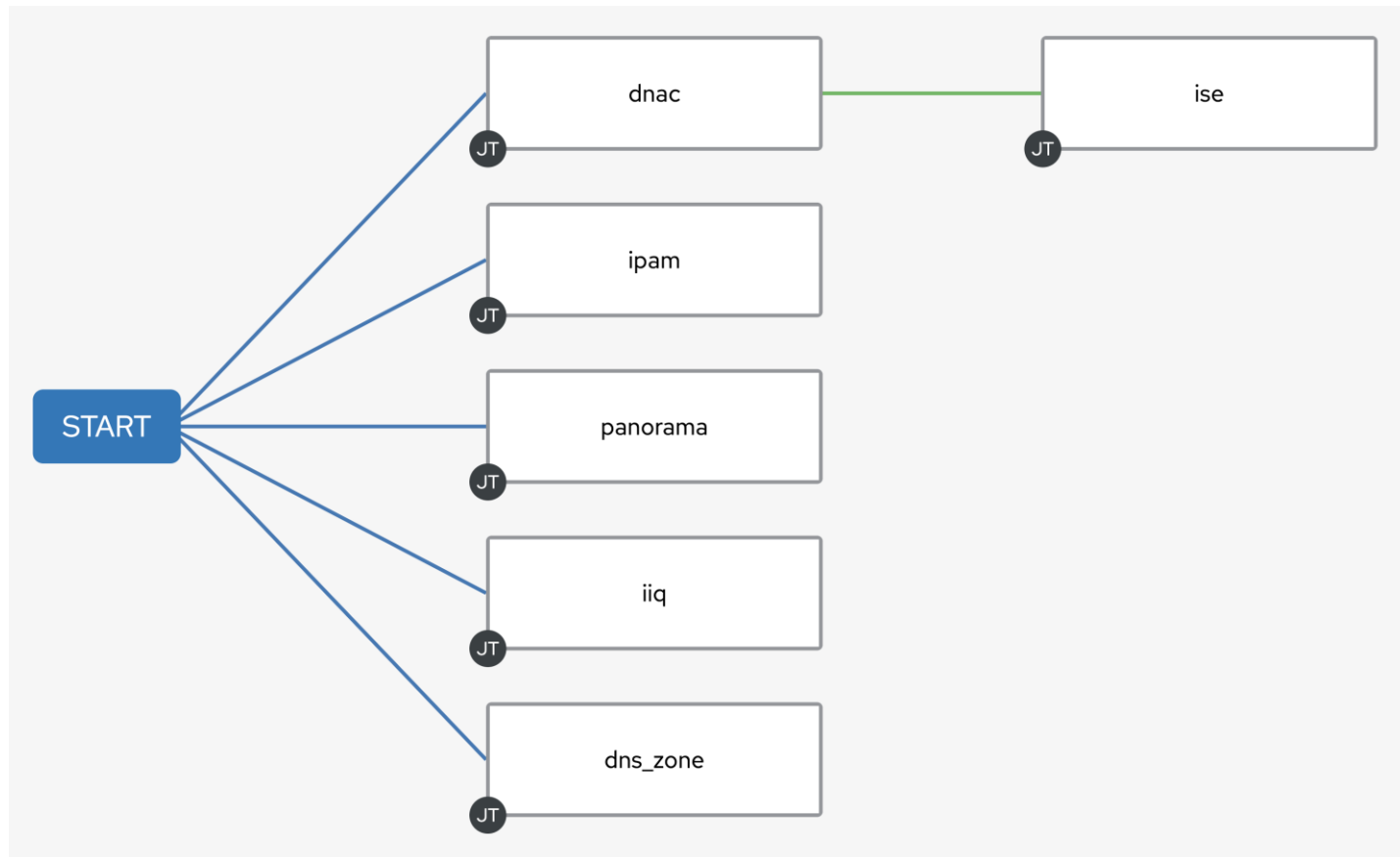
UNIVERSITY OF COPENHAGEN



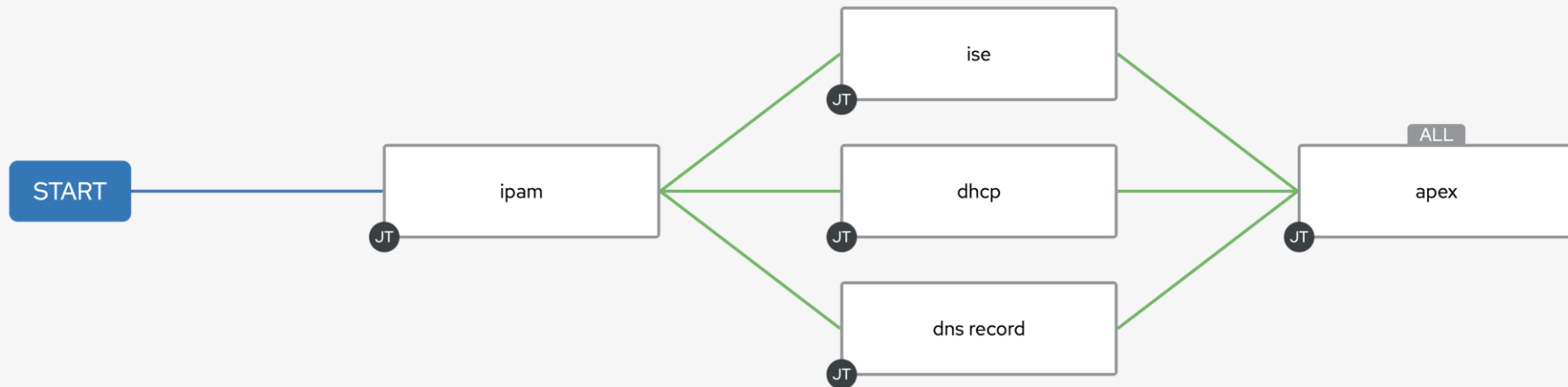
Indledning

- Oktober 2022 begynder vi at tage Forskning ind i netværket.
- Resulterede i omkring 85 forskellige LABnet (Netværkssegmenter/SGT'ere).
- Behov for automatisering og selvbetjening.
- Udvikling af HDTools
 - Fejlsøgningsværktøj i vores support sektion
 - Se status og fejl på en bruger eller udstyr
 - Selvbetjeningsværktøj til brugere af netværkssegmenter (Forskere, bygningsdrift)
 - Selv administrere sit segment, hvilket udstyr er registreret.
- Hdtools v1.0 klar i marts 2023
- Bygget på Oracle APEX platformen, med brug af Ansible bagved, samt direkte API kald mod DNAC.

Oprettelse af et Netværkssegment – Ansible Template



Oprettelse af et Endpoint – Ansible Template



Q&A