cisco Live!

#CiscoLive

The bridge to possible

Securing the Hybrid Campus and Branch

Jeff Meek
Product Marketing Manager, EN Switching/Smart Building

PSOENT-1002

Cisco Webex App

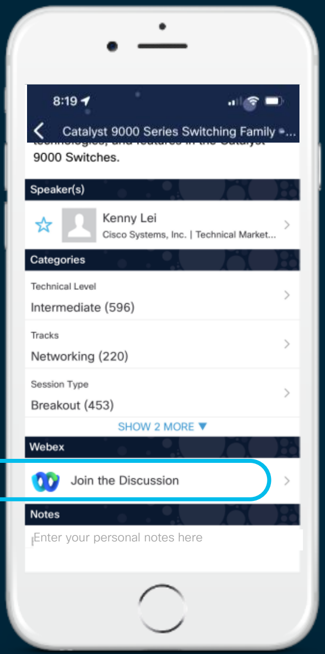
Questions?

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

How

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

Webex spaces will be moderated
by the speaker until June 17, 2022.



8:19

Catalyst 9000 Series Switching Family ...

9000 Switches.

Speaker(s)

Kenny Lei
Cisco Systems, Inc. | Technical Market...

Categories

Technical Level
Intermediate (596)

Tracks
Networking (220)

Session Type
Breakout (453)

SHOW 2 MORE ▼

Webex

Join the Discussion

Notes

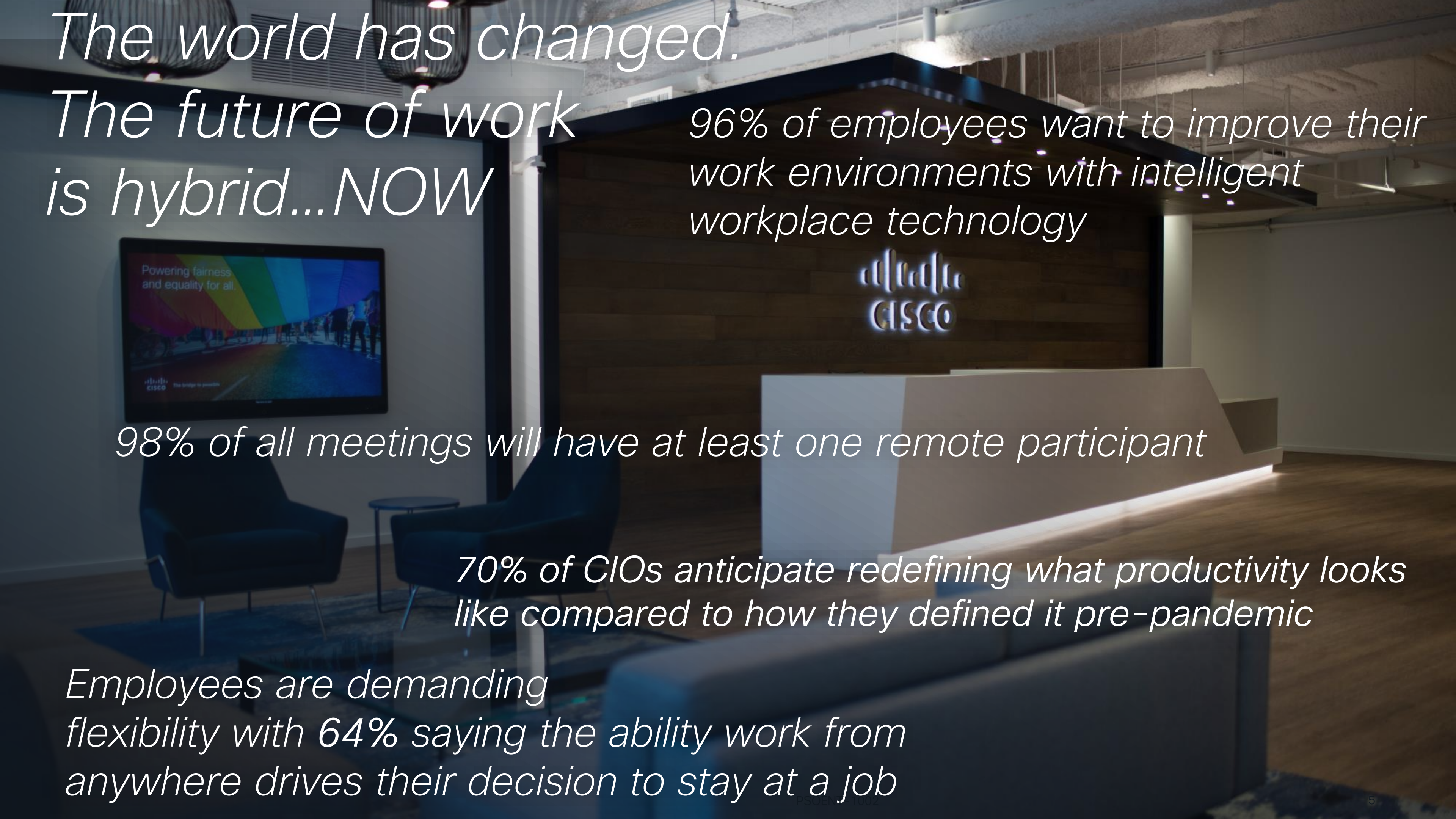
Enter your personal notes here

https://ciscolive.ciscoevents.com/ciscolivebot/#BPSOENT-1002

Agenda

- Zero Trust
  - Endpoint analytics
  - Traffic Analytics
  - Segmentation

- Catalyst 9000 Secure Connectivity
- Securing Cisco PENN1



The world has changed. The future of work is hybrid…NOW

96% of employees want to improve their work environments with intelligent workplace technology

98% of all meetings will have at least one remote participant

70% of CIOs anticipate redefining what productivity looks like compared to how they defined it pre-pandemic

Employees are demanding flexibility with ***64%*** *saying the ability work from anywhere drives their decision to stay at a job*

Top priorities for businesses as they return to buildings

Sustainable

Energy efficient, carbon reducing designs that create an agile environment, with 90W PoE technology built in as the 4th utility.

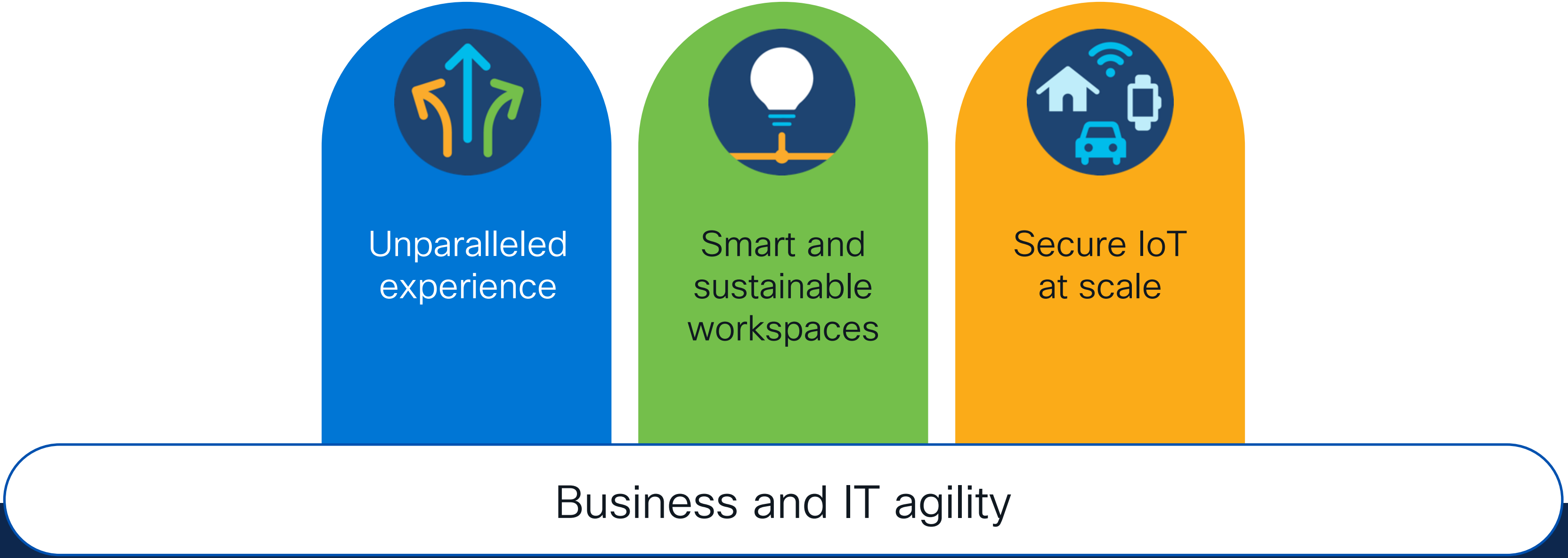
Convergence

Eliminating siloed networks; powering, connecting and securing the building and simplifying design and operations

Hybrid Work

Enable flexible workspaces, hoteling and hot desking with space utilization and insights to enable employees to use as desired

Catalyst 9000 empowers IT to accelerate hybrid work



Unparalleled experience

Smart and sustainable workspaces

Secure IoT at scale

Business and IT agility

Pushing the boundaries of technology to create freedom of choice

Trusted Workplace is critical to your business

Retail chain leverages IoT and A.I

Doctor performs remote robotic surgery

Student logs into a microscope in a lab

31 BILLION TOTAL IoT DEVICES BY 2025

⚠ Default access policy is set as ‘permit’ due to inability to properly identify the influx of newly connected devices in the stores

⚠ A flat, unsegmented network allowed cyber-criminals to propagate malware placed in HVAC to the robotic surgery equipment

⚠ Despite good segmentation, a hacker gains access by spoofing the microscope’s identity and brings down the network with a DDoS attack

$10.5 trillion annual cybercrime impact by 2025

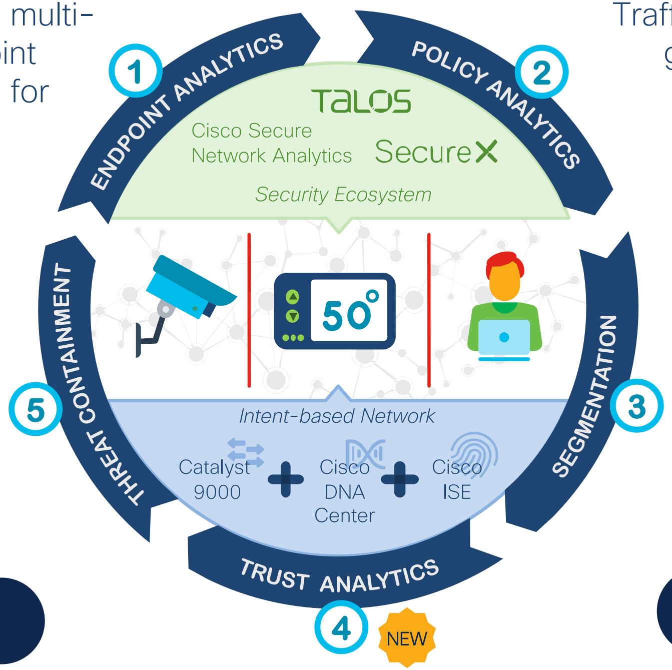
Cisco SD-Access delivers workplace zero trust

Leverage network and ML to scale workplace zero trust

Continuous visibility

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

Traffic analysis for granular policy discovery



Automated threat isolation and remediation

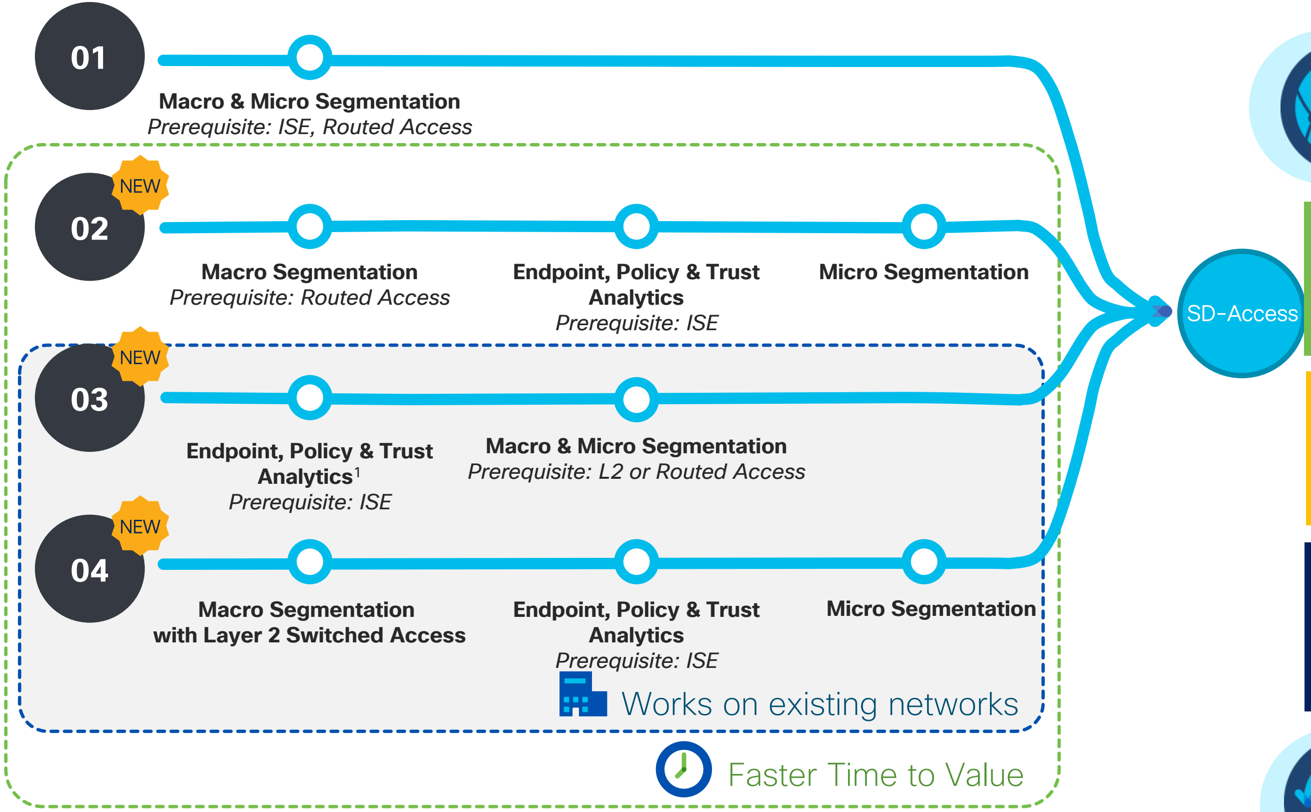
Flexible Macro/Micro segmentation

AI/ML-led network behavior anomaly detection

Constant protection

Zero-trust access

New journeys deliver results faster!


01
Macro & Micro Segmentation
Prerequisite: ISE, Routed Access
NEW
02
Macro Segmentation
Prerequisite: Routed Access
Endpoint, Policy & Trust Analytics
Prerequisite: ISE
Micro Segmentation
NEW
03
Endpoint, Policy & Trust Analytics[1]
Prerequisite: ISE
Macro & Micro Segmentation
Prerequisite: L2 or Routed Access
NEW
04
Macro Segmentation with Layer 2 Switched Access
Endpoint, Policy & Trust Analytics
Prerequisite: ISE
Micro Segmentation
Works on existing networks
Faster Time to Value
SD-Access

Lower Barrier to Start

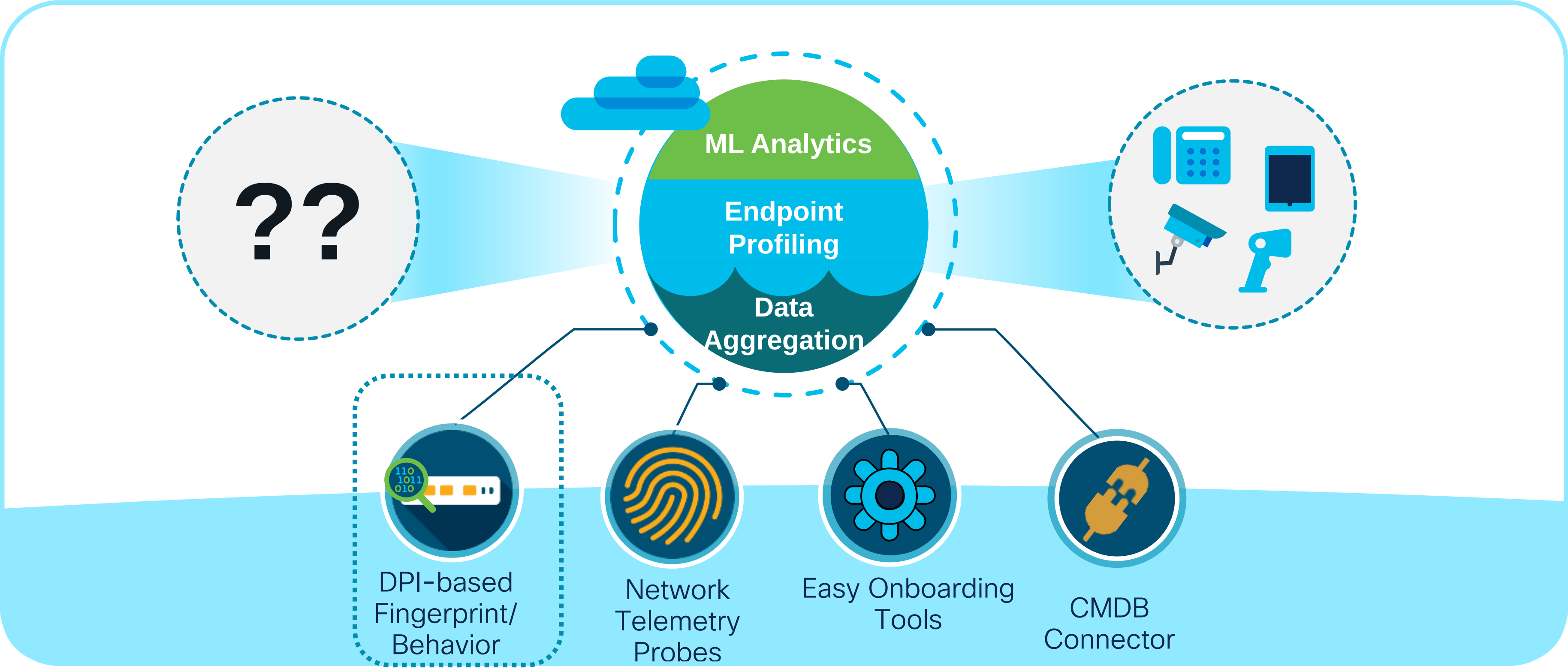
New Segmentation Capabilities	Overlapping IP space, L2 Network Segments
New Deployment Flexibility	Retain Layer 2 Access
Incremental Migration	Macro segmentation without ISE

Faster Time To Value

[1] Fabric is optional to deploy Endpoint, Policy & Trust Analytics

Endpoint profiling, data sources and ML analytics

Rapidly reducing the unknowns by aggregating data from different sources



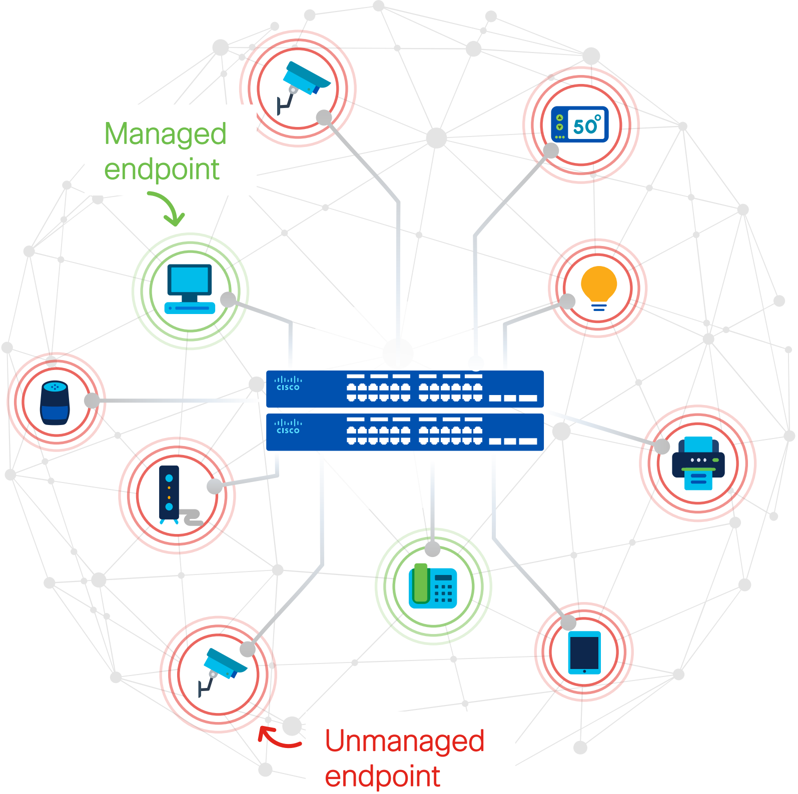
CMDB: Configuration Management Database

Cisco AI Endpoint Analytics

Know what is connecting to your network

Next generation endpoint visibility with **AI-driven analytics** and network driven **deep packet inspection**

What's happening in the workplace?



1:5

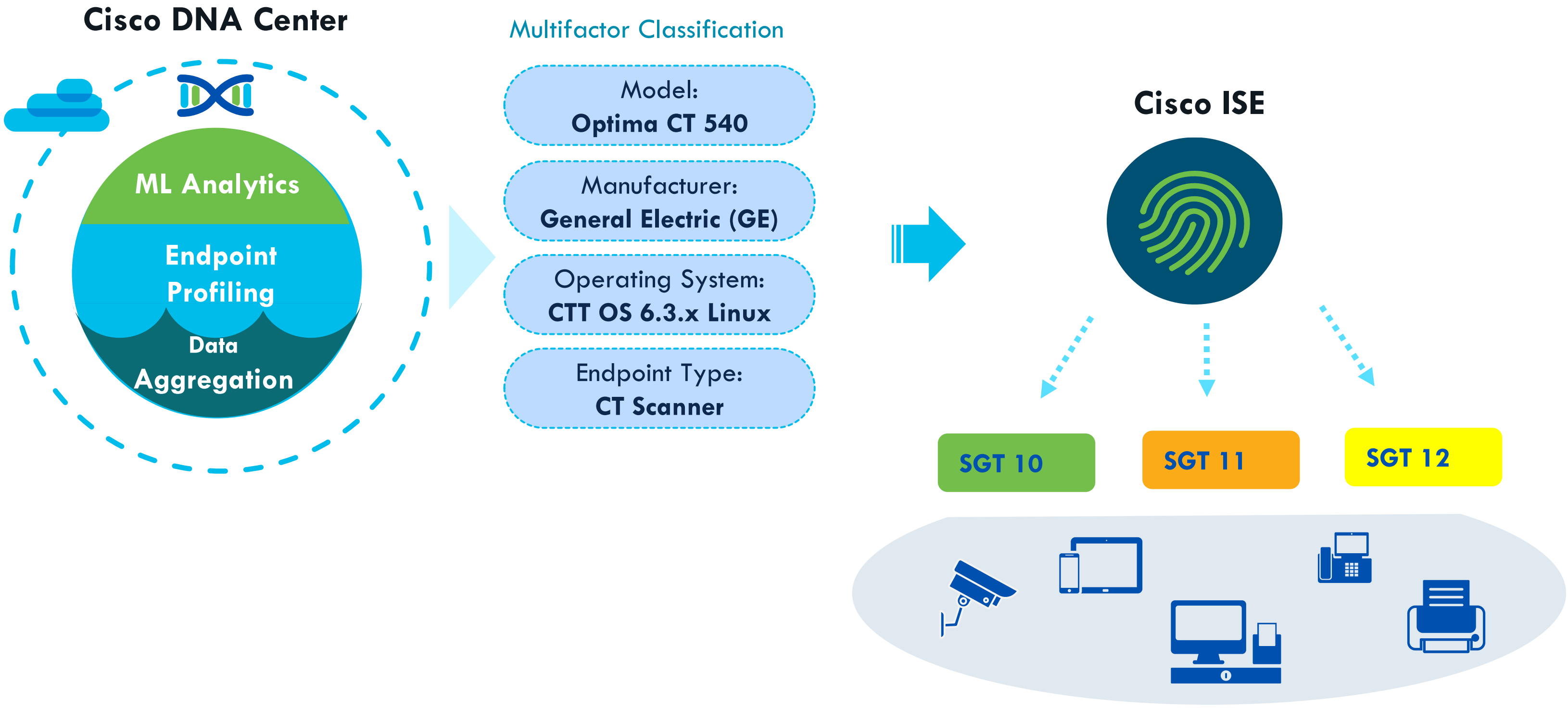
Unmanaged device proliferation.
1:5 managed to **unmanaged endpoint ratio**

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

Better classification reduces unauthorized access



Cisco DNA Center

ML Analytics

Endpoint Profiling

Data Aggregation

Multifactor Classification

Model: **Optima CT 540**

Manufacturer: **General Electric (GE)**

Operating System: **CTT OS 6.3.x Linux**

Endpoint Type: **CT Scanner**

Cisco ISE

SGT 10

SGT 11

SGT 12

Enterprise Network

Multifactor classification

Classifying endpoints using four independent label categories for more flexible profiling

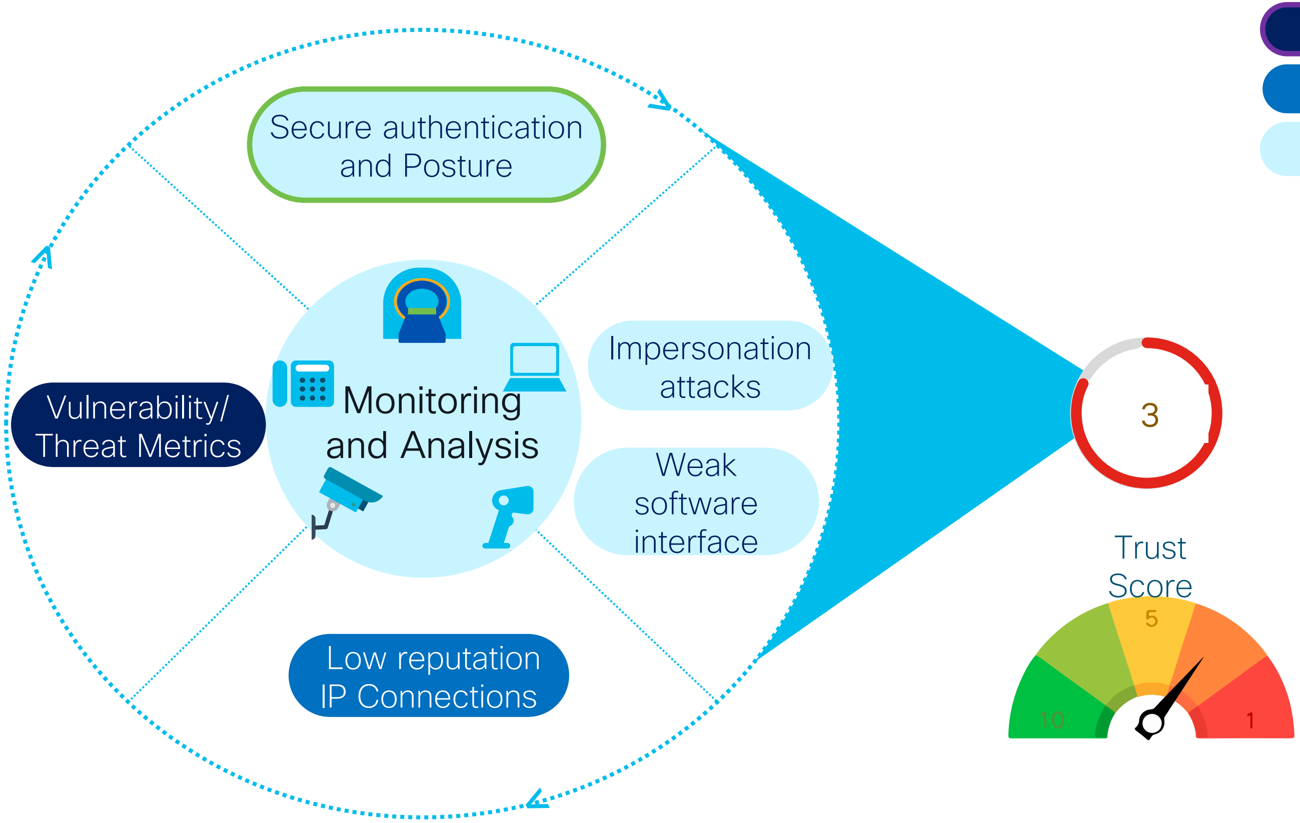
Device type	Hardware manufacturer	Hardware model	Operating system
Laptop	Apple	MacBook Pro	MacOS 10.14.6
CT scanner	GE	Optima CT540	CTT OS 6.3.x Linux
Smartphone	Samsung	Galaxy S8	Android 9.0

Trust Analytics: Continuous evaluation of security posture for Trusted Access

Future

EFT

Supported



Secure authentication and Posture

Vulnerability/ Threat Metrics

Monitoring and Analysis

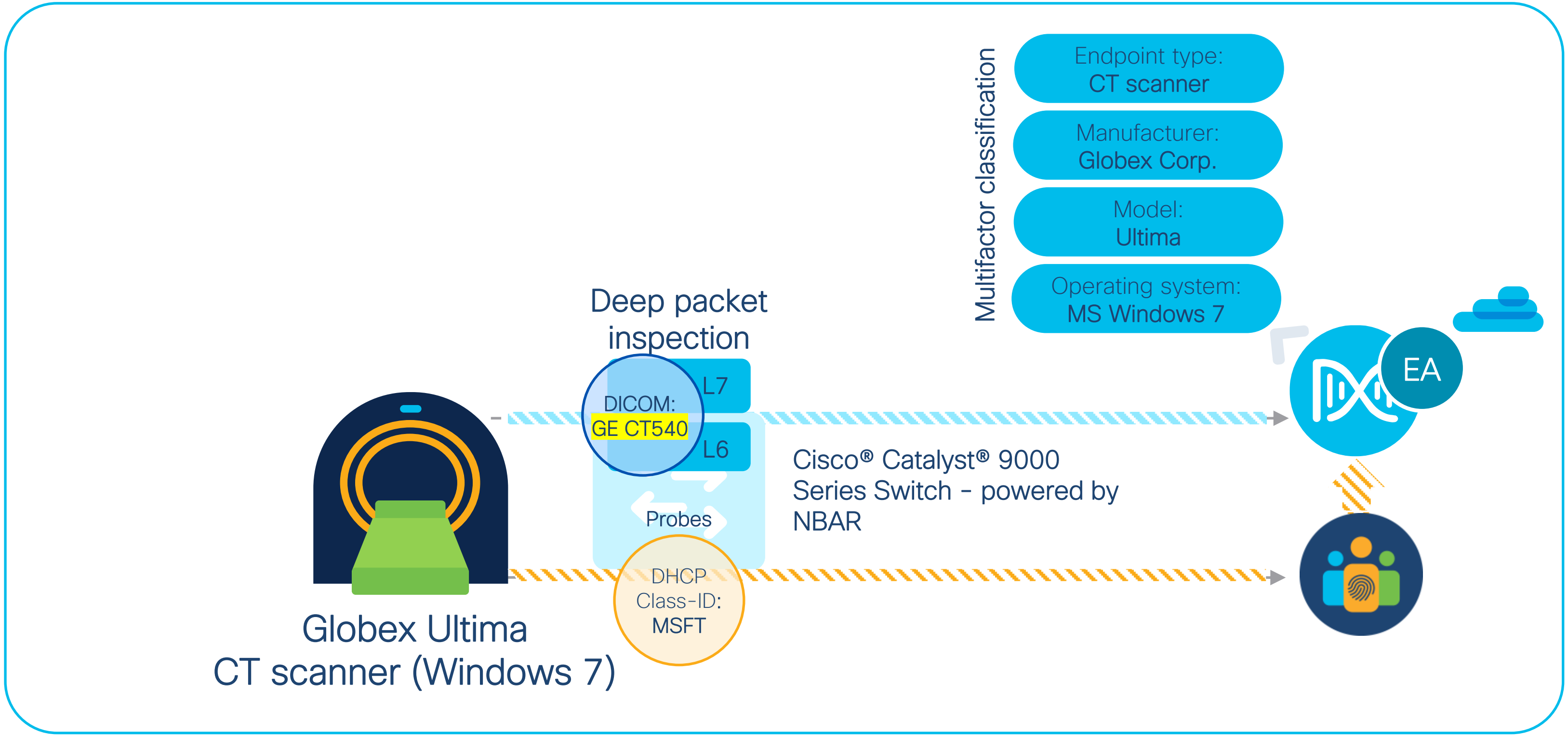
Impersonation attacks

Weak software interface

Low reputation IP Connections

Classification based on Deep Packet Inspection (DPI)

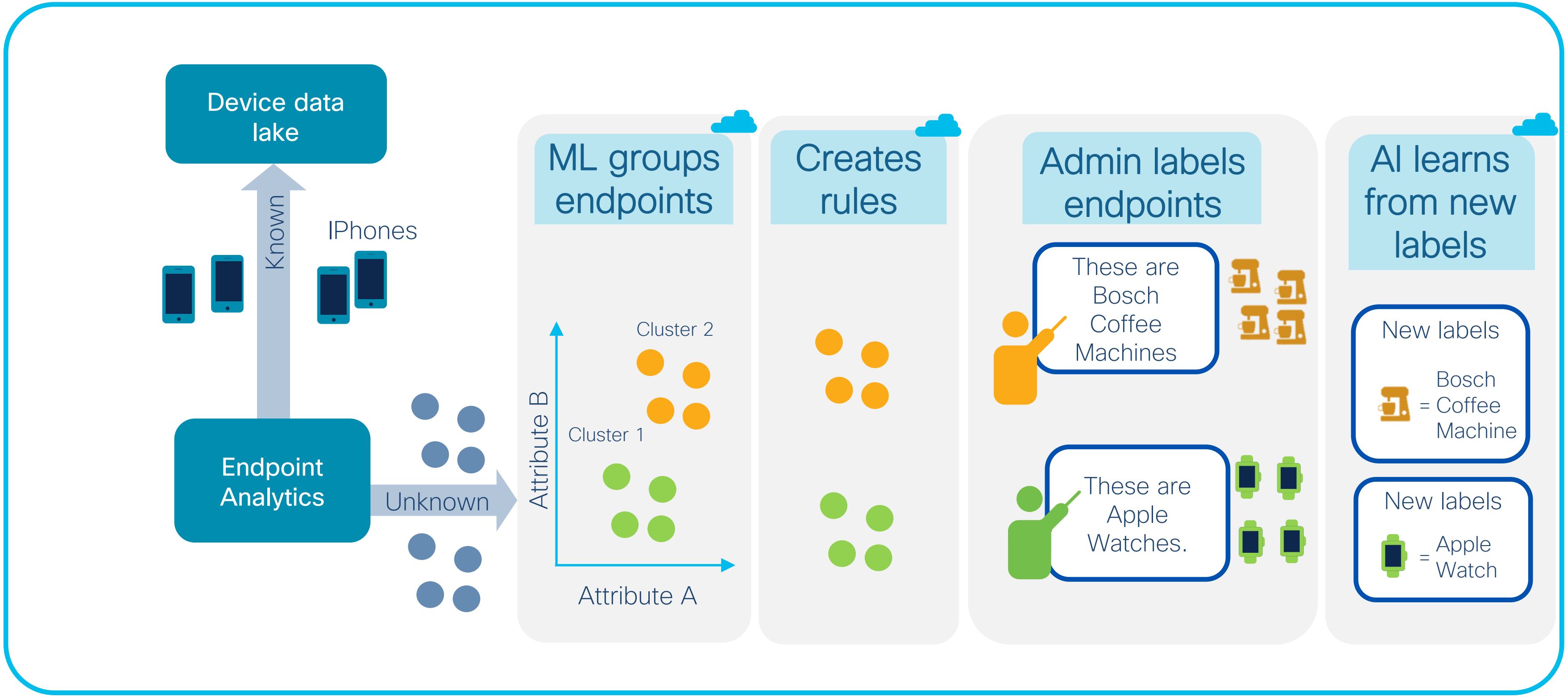
AI Endpoint Analytics



Cisco® Catalyst® 9000 Series Switch – powered by NBAR

Reducing unknowns with machine learning

AI Endpoint Analytics



Device data lake

Known

IPhones

Endpoint Analytics

Unknown

ML groups endpoints

Creates rules

Admin labels endpoints

These are Bosch Coffee Machines

These are Apple Watches.

AI learns from new labels

New labels

= Bosch Coffee Machine

New labels

= Apple Watch

☁ = done in cloud

Policy analytics

Deploy group polices with confidence

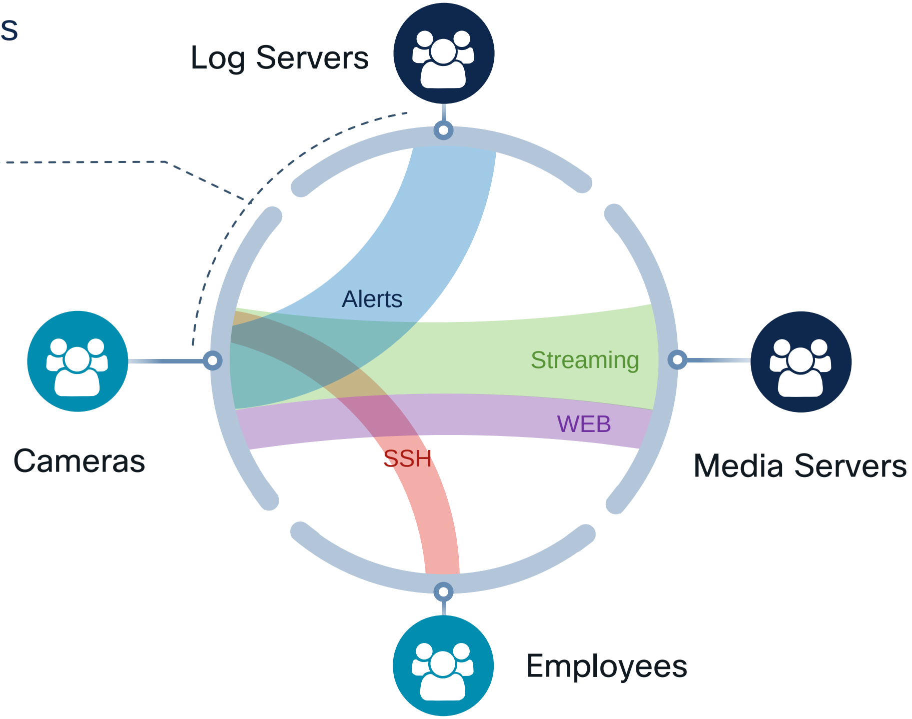
Policy Modeling – With traffic patterns

	Media Servers	Log Servers	Employees
Cameras	✓ RTP ✓ WWW	✓ Syslog	⊖ Any

Unearth critical access that must be allowed / denied

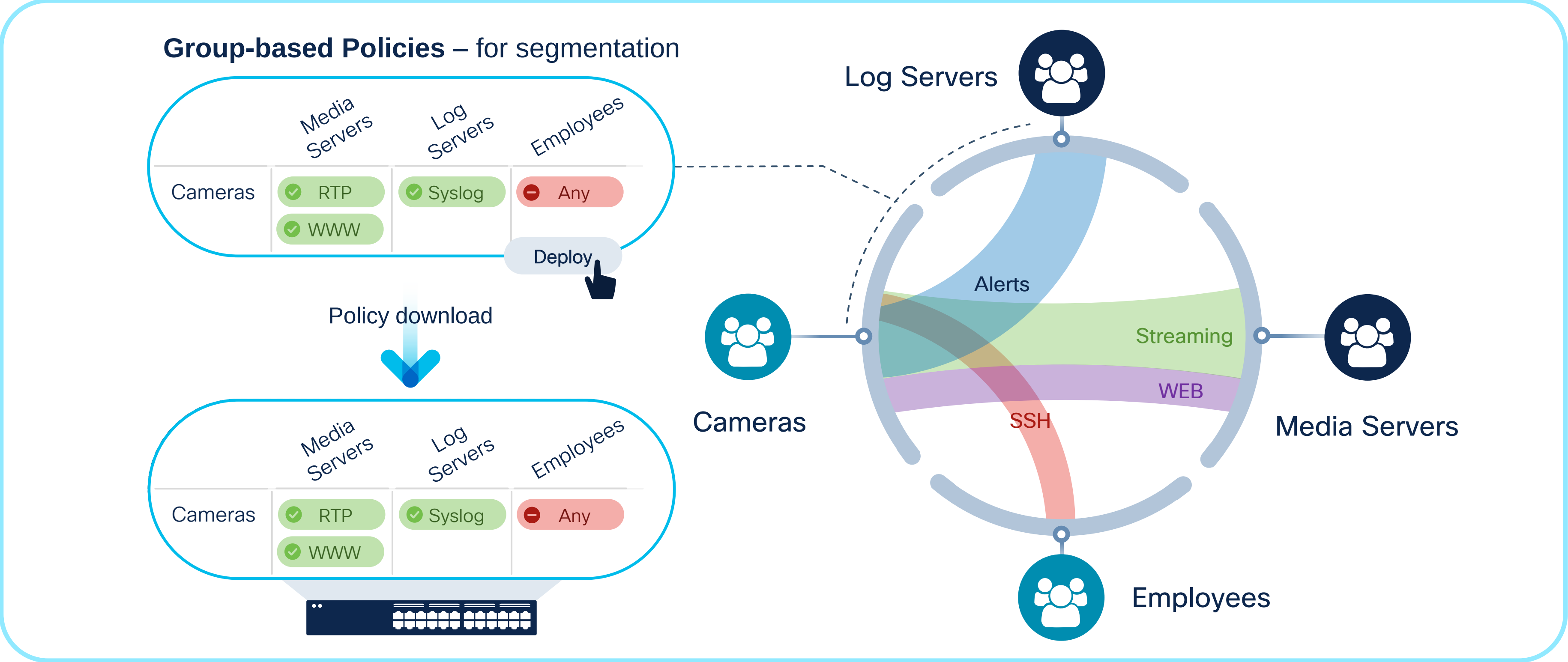
Observe and fine-tune for days/weeks

No policy on the network, yet



Policy analytics

Deploy group polices with confidence



Group-based Policies – for segmentation

	Media Servers	Log Servers	Employees
Cameras	✓ RTP ✓ WWW	✓ Syslog	⊖ Any

Deploy

Policy download

	Media Servers	Log Servers	Employees
Cameras	✓ RTP ✓ WWW	✓ Syslog	⊖ Any

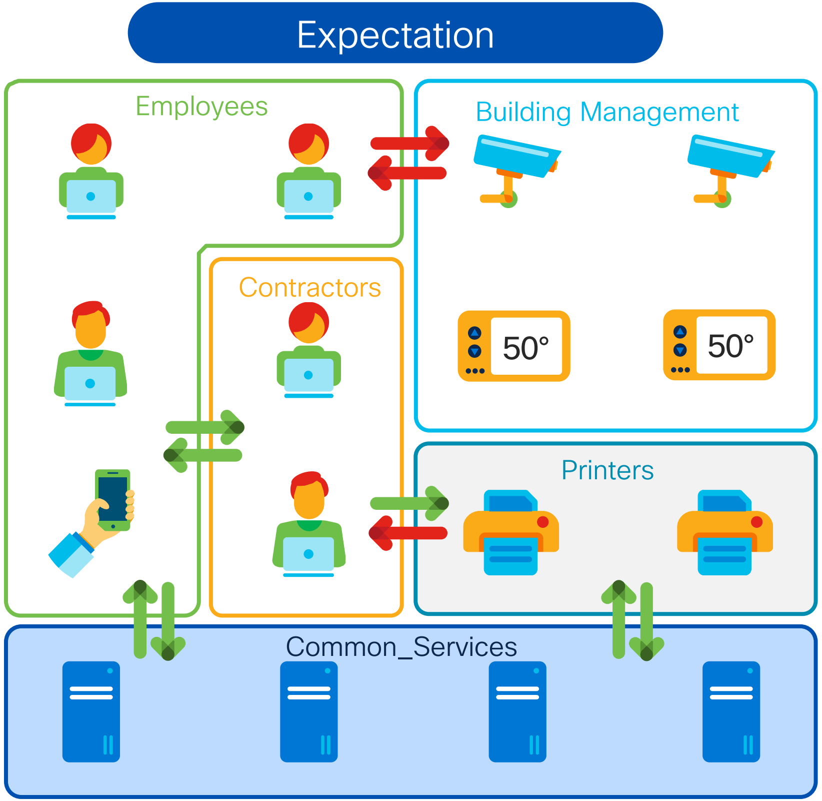
Segmentation

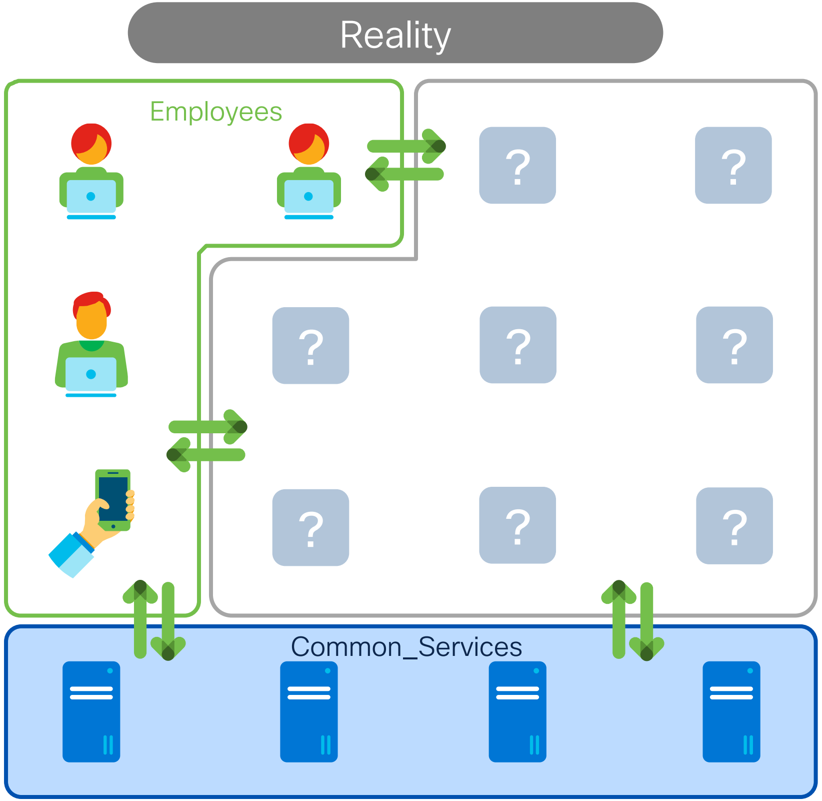
Rollout least-privileged access consistently

Provide Scalable Segmented Access regardless of Endpoint Type, Location, Access Medium, Connectivity Method, or Network Topology

Segmentation: expectation vs. reality

Least Privilege Access





Network fabric enables zero trust at scale

Leverage the ubiquitous nature of the network

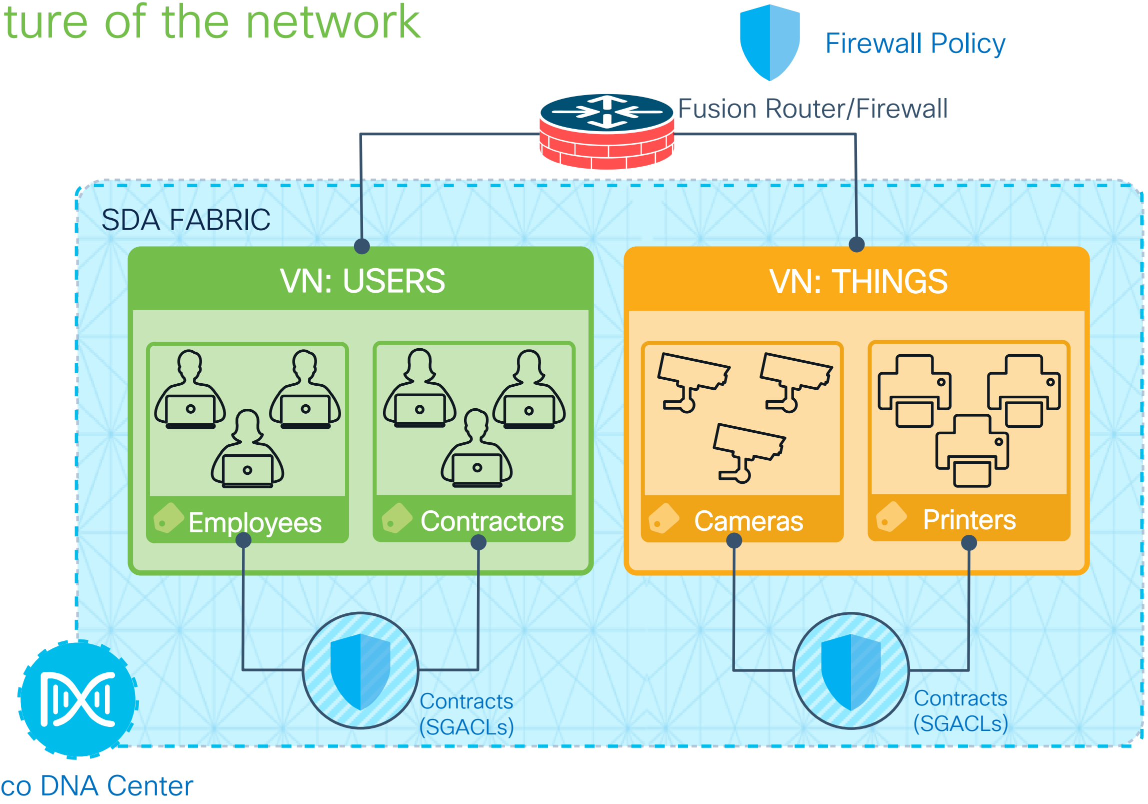
Macro segmentation with ‘Virtual Networks’

Micro segmentation with ‘Scalable Groups’

Integrated Wireless
Campus & Branches
Integrated WAN, DC

Fabric Assurance – KPIs, Health Scores, Issues, Remediations, Reports, Event Viewers

Fusion router or Firewall for Inter-VN routing & policy



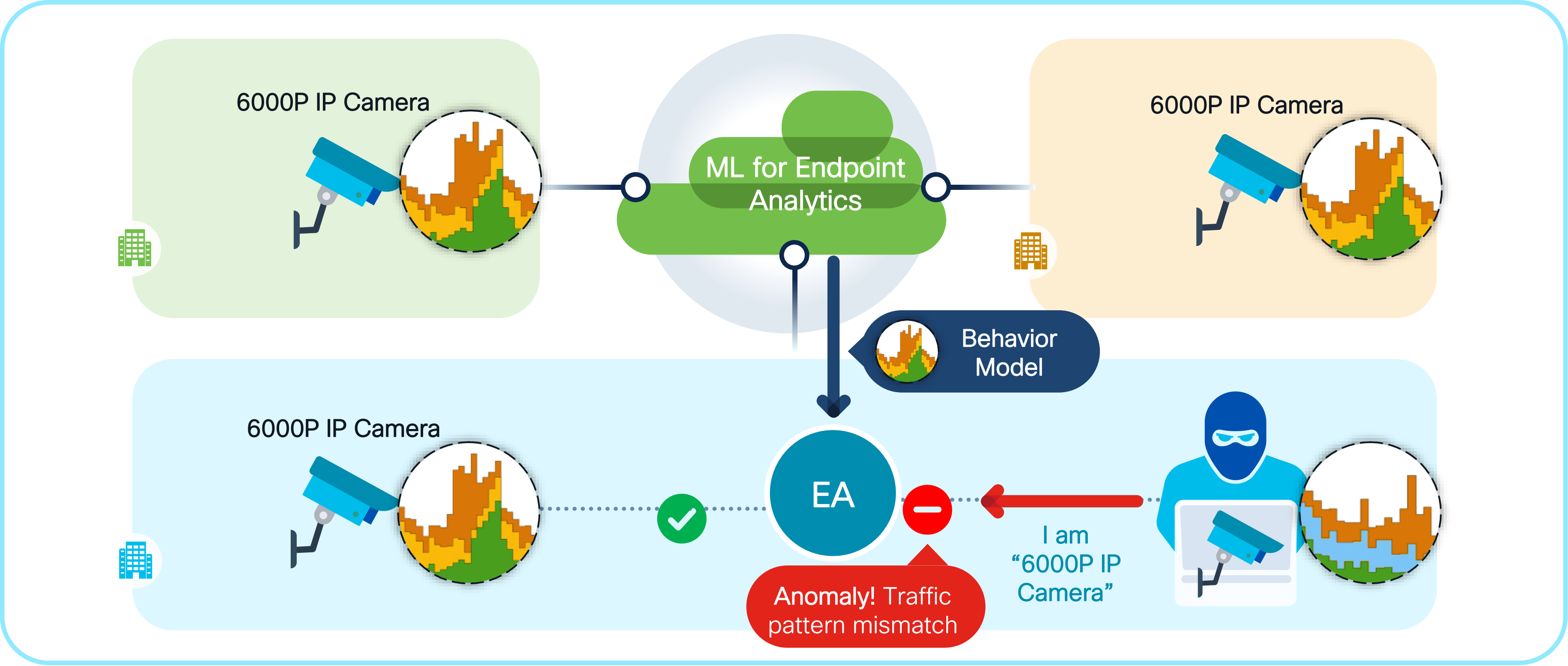
AI Trust Analytics & Containment

Realize zero trust workplace

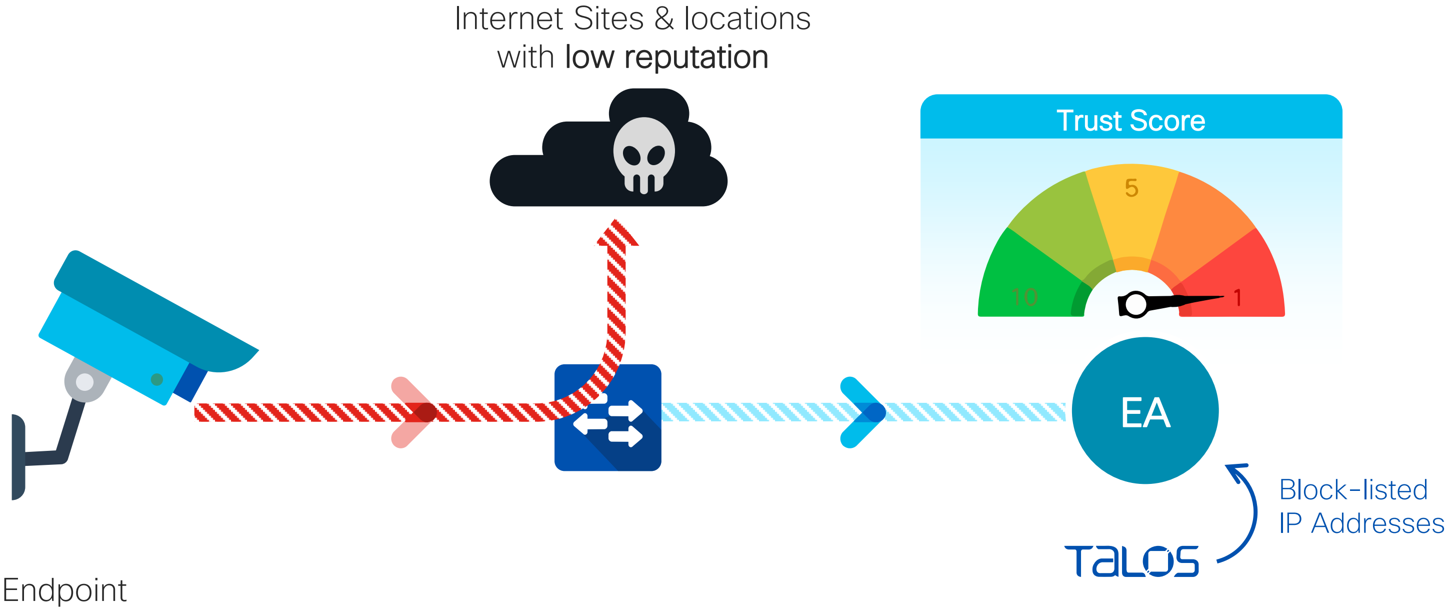
Continuously evaluate trust of connected endpoints & automate threat response by enlisting your network for security

NEW

Machine learning augments network intelligence



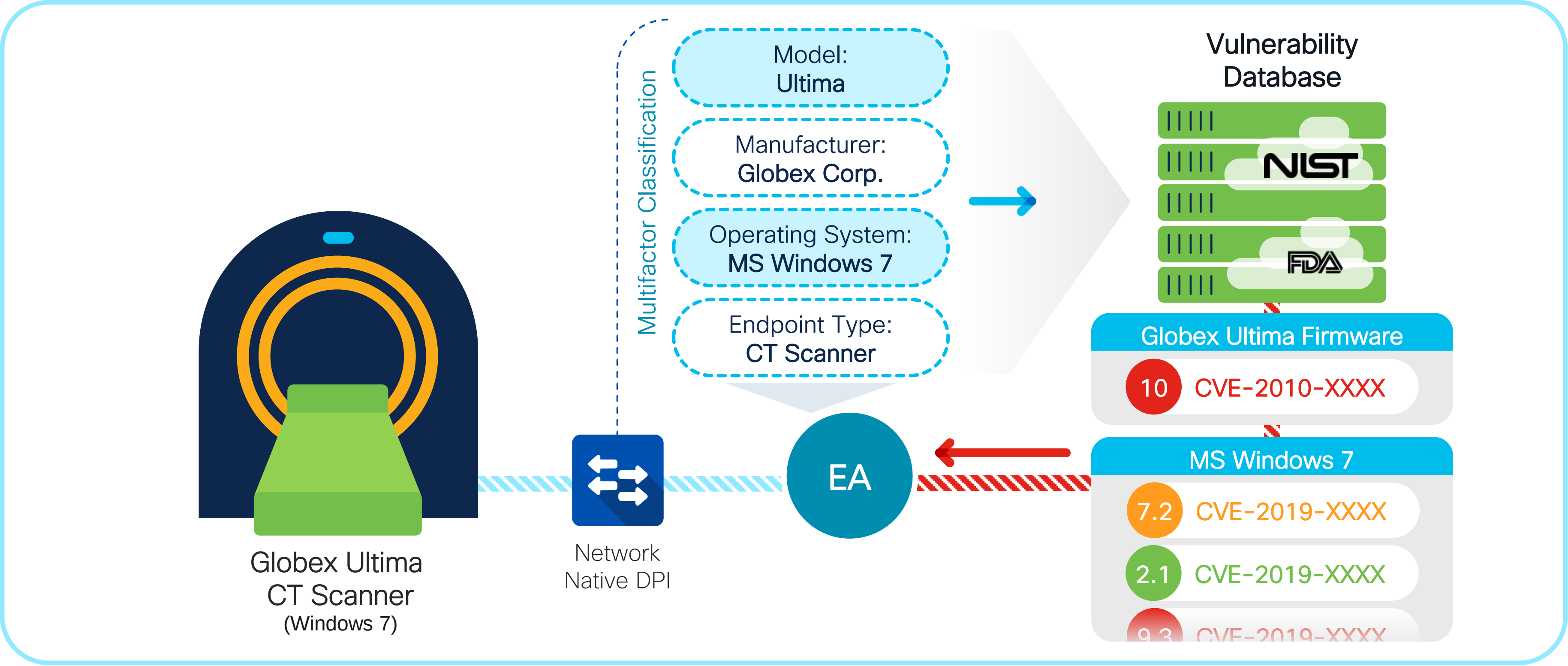
Detect anomalous transactions



- ✓ Detect compromised endpoints
- ✓ Realtime update of Block listed IP address
- ✓ Manual/Automatic remediation

Native vulnerability assessment for endpoints

Passive posture assessment



Multifactor Classification

Model:
Ultima

Manufacturer:
Globex Corp.

Operating System:
MS Windows 7

Endpoint Type:
CT Scanner

Vulnerability Database

Globex Ultima Firmware

10	CVE-2010-XXXX

MS Windows 7

7.2	CVE-2019-XXXX
2.1	CVE-2019-XXXX
9.3	CVE-2019-XXXX

Globex Ultima
CT Scanner
(Windows 7)

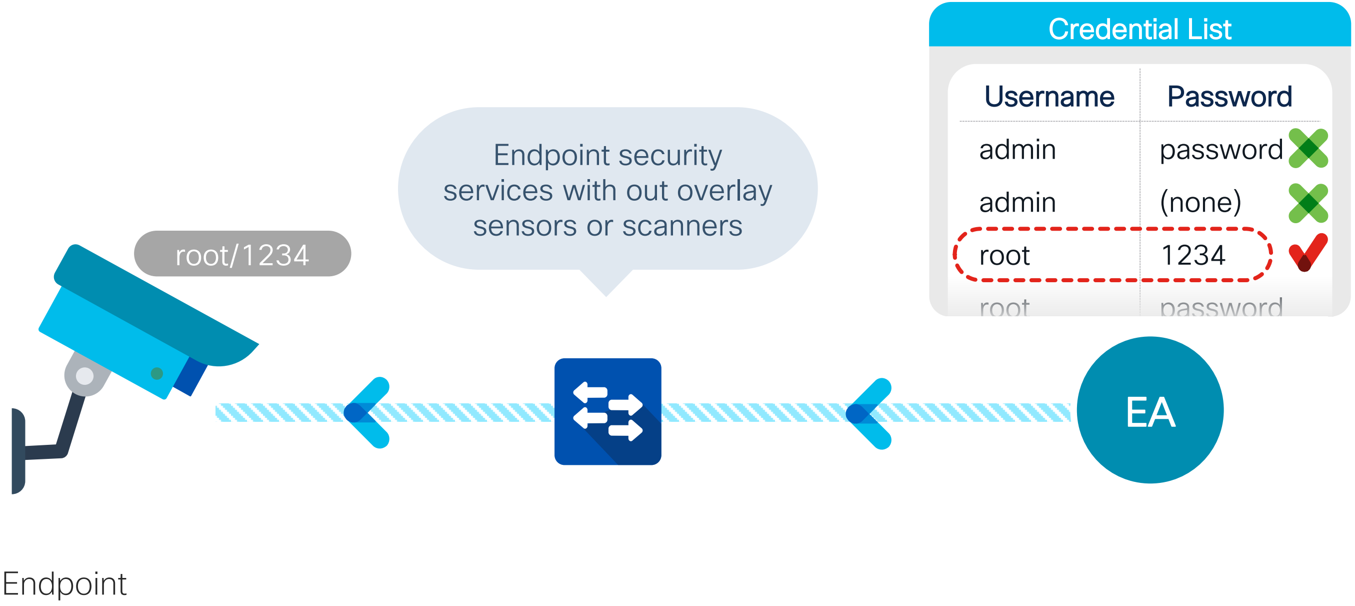
Network
Native DPI

EA: Endpoint Analytics

[1]In Planning

Weak credentials scan

Active posture assessment


root/1234
Endpoint security services with out overlay sensors or scanners
EA
Endpoint

Credential List

Username	Password	
admin	password	✗
admin	(none)	✗
root	1234	✓
root	password	

✓ Check IoT Devices for Weak Credentials

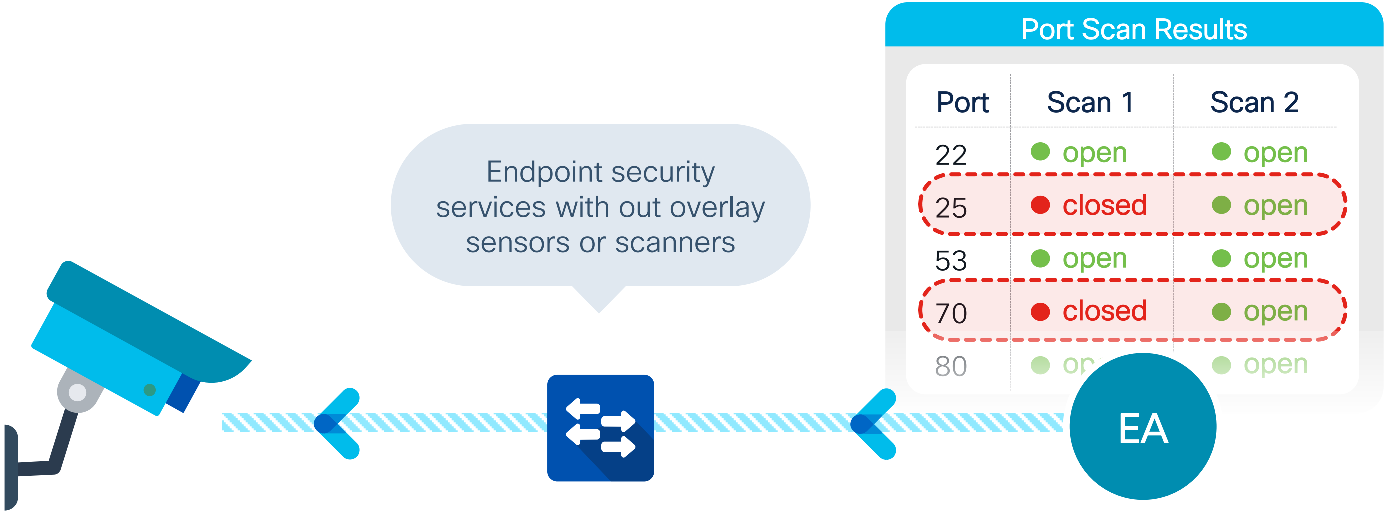
✓ Check common and custom credential lists

✓ SNMP, SSH and Telnet Support

[1]In Planning

Port scanning

Active posture assessment



Port Scan Results

Port	Scan 1	Scan 2
22	● open	● open
25	● closed	● open
53	● open	● open
70	● closed	● open
80	● op	● open

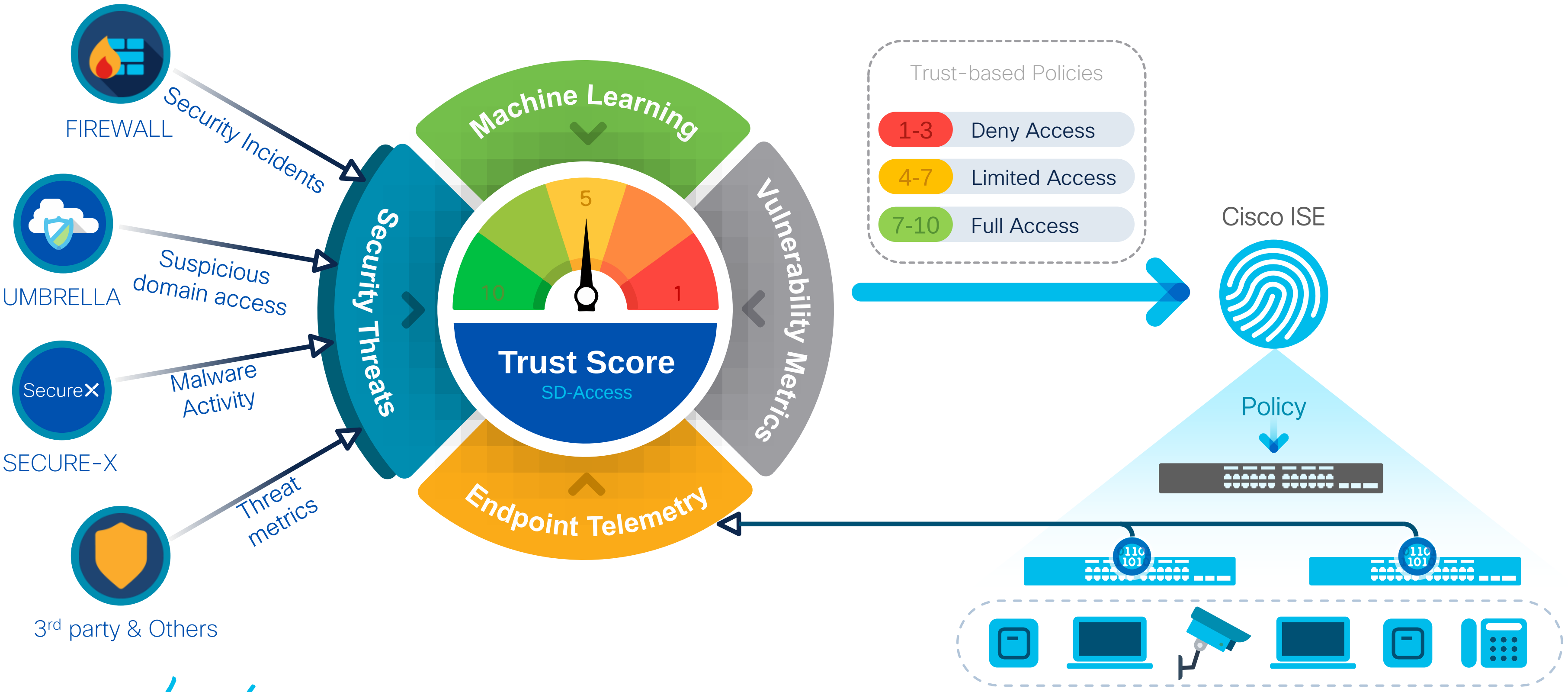
Endpoint security services with out overlay sensors or scanners

Endpoint

- ✓ Automatically baseline normal port behavior
- ✓ Flag variances from the baseline
- ✓ TCP/UDP Port Support

Workplace zero trust manifested as Trust Score

Automate threat response with trust-based policies



FIREWALL — Security Incidents

UMBRELLA — Suspicious domain access

SECURE-X — Malware Activity

3rd party & Others — Threat metrics

Security Threats

Machine Learning

Vulnerability Metrics

Endpoint Telemetry

Trust Score

SD-Access

Trust-based Policies

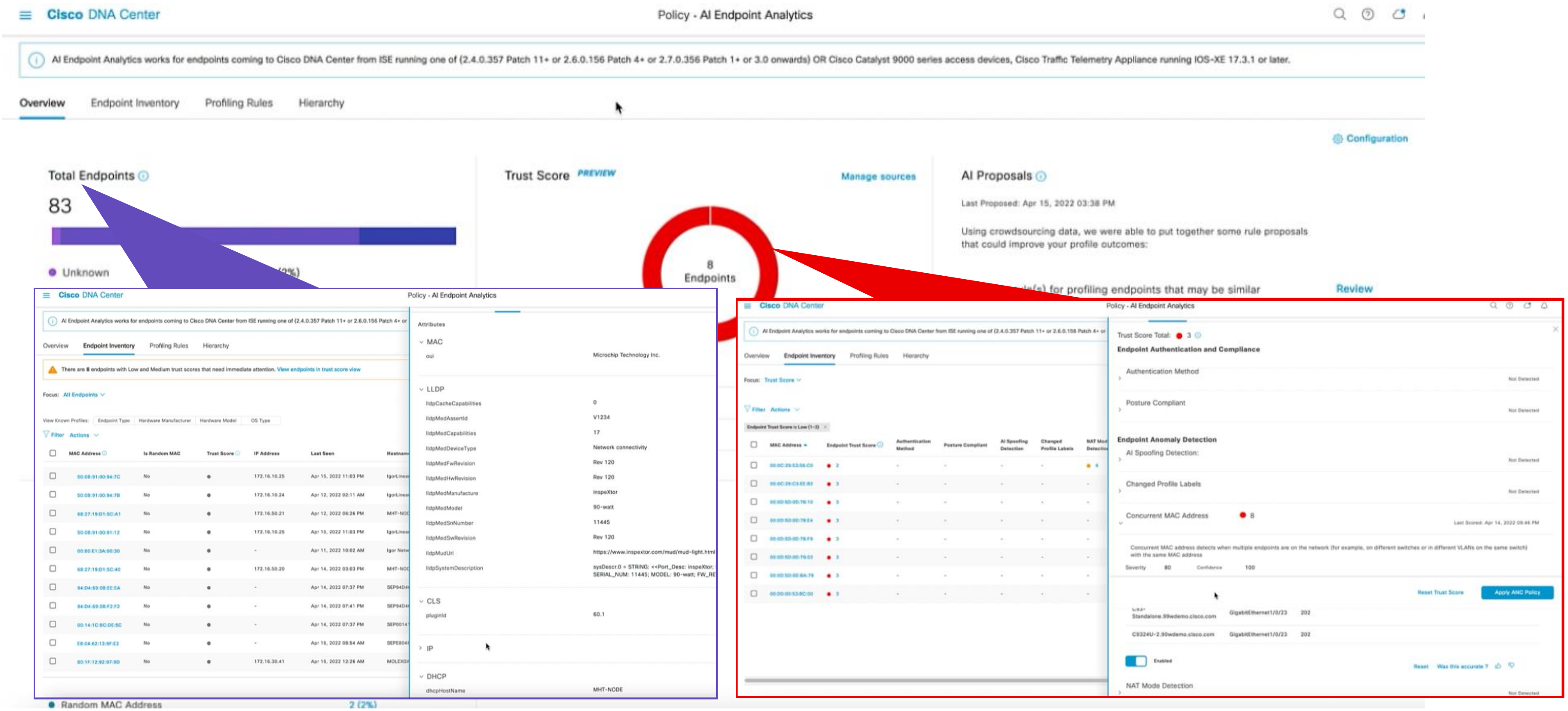
1-3	Deny Access
4-7	Limited Access
7-10	Full Access

Cisco ISE

Policy

cisco Live!

AI Endpoint, Trust Analytics – Cisco DNA Center



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.

Total Endpoints

83

- Unknown (2%)
- Random MAC Address 2 (2%)

Trust Score PREVIEW

AI Proposals

Last Proposed: Apr 15, 2022 03:38 PM

Using crowdsourcing data, we were able to put together some rule proposals that could improve your profile outcomes:

...rule(s) for profiling endpoints that may be similar

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

There are 8 endpoints with Low and Medium trust scores that need immediate attention. View endpoints in trust score view

Focus: All Endpoints

View Known Profiles: Endpoint Type | Hardware Manufacturer | Hardware Model | OS Type

	MAC Address	Is Random MAC	Trust Score	IP Address	Last Seen	Hostname
□	50:0B:91:00:94:7C	No	●	172.16.10.25	Apr 15, 2022 11:03 PM	IgorLinea
□	50:0B:91:00:94:7B	No	●	172.16.10.24	Apr 12, 2022 02:11 AM	IgorLinea
□	68:27:19:D1:5C:A1	No	●	172.16.50.21	Apr 12, 2022 06:26 PM	MHT-NOD
□	50:0B:91:00:91:12	No	●	172.16.10.25	Apr 15, 2022 11:03 PM	IgorLinea
□	00:80:E1:3A:00:30	No	●	-	Apr 11, 2022 10:02 AM	Igor Netw
□	68:27:19:D1:5C:40	No	●	172.16.50.20	Apr 14, 2022 03:03 PM	MHT-NOD
□	94:D4:69:0B:EE:EA	No	●	-	Apr 14, 2022 07:37 PM	SEP94D4
□	94:D4:69:0B:F2:F2	No	●	-	Apr 14, 2022 07:41 PM	SEP94D4
□	00:14:1C:BC:DE:5C	No	●	-	Apr 14, 2022 07:37 PM	SEP0014
□	E8:04:62:13:9F:E2	No	●	-	Apr 16, 2022 08:54 AM	SEPE804
□	80:1F:12:92:97:9D	No	●	172.16.30.41	Apr 16, 2022 12:26 AM	MOLEXGV

Attributes

MAC	
oui	Microchip Technology Inc.
LLDP	
lldpCacheCapabilities	0
lldpMedAssertId	V1234
lldpMedCapabilities	17
lldpMedDeviceType	Network connectivity
lldpMedFwRevision	Rev 120
lldpMedHwRevision	Rev 120
lldpMedManufacture	inspeXtor
lldpMedModel	90-watt
lldpMedSnNumber	11445
lldpMedSwRevision	Rev 120
lldpMudUrl	https://www.inspextor.com/mud/mud-light.html
lldpSystemDescription	sysDescr.0 = STRING: <<Port_Desc: inspeXtor; SERIAL_NUM: 11445; MODEL: 90-watt; FW_RE
CLS	
pluginId	60.1
IP	
DHCP	
dhcpHostName	MHT-NODE

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

Focus: Trust Score

Endpoint Trust Score is Low (1-3) ×

	MAC Address	Endpoint Trust Score	Authentication Method	Posture Compliant	AI Spoofing Detection	Changed Profile Labels	NAT Mod Detectio
□	00:0C:29:53:56:C0	● 2	-	-	-	-	● 6
□	00:0C:29:C3:EE:B2	● 3	-	-	-	-	-
□	00:0D:5D:0D:78:10	● 3	-	-	-	-	-
□	00:0D:5D:0D:78:E4	● 3	-	-	-	-	-
□	00:0D:5D:0D:78:F9	● 3	-	-	-	-	-
□	00:0D:5D:0D:79:02	● 3	-	-	-	-	-
□	00:0D:5D:0D:8A:79	● 3	-	-	-	-	-
□	00:D0:00:53:8C:00	● 3	-	-	-	-	-

Trust Score Total: ● 3

Endpoint Authentication and Compliance

Authentication Method	Not Detected
Posture Compliant	Not Detected

Endpoint Anomaly Detection

AI Spoofing Detection:	Not Detected
Changed Profile Labels	Not Detected
Concurrent MAC Address ● 8	Last Scored: Apr 14, 2022 08:46 PM

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

C93- Standalone.99wdemo.cisco.com	GigabitEthernet1/0/23	202
C9324U-2.90wdemo.cisco.com	GigabitEthernet1/0/23	202

NAT Mode Detection	Not Detected

Enhanced App Hosting with Catalyst 9000X

Consolidate Physical Infrastructure

ThousandEyes

kibana

WIRESHARK

perfSONAR powered

Enhance Visibility & Security Enforcement

ASAc

codilime

Attivo NETWORKS.

TRAPX SECURITY

Reduce App Latency & Optimize App Traffic

Cybervision

Cisco DNA Spaces

NS1.

Alleantia ALL <THINGS> JOINED

3rd Party App Hosting

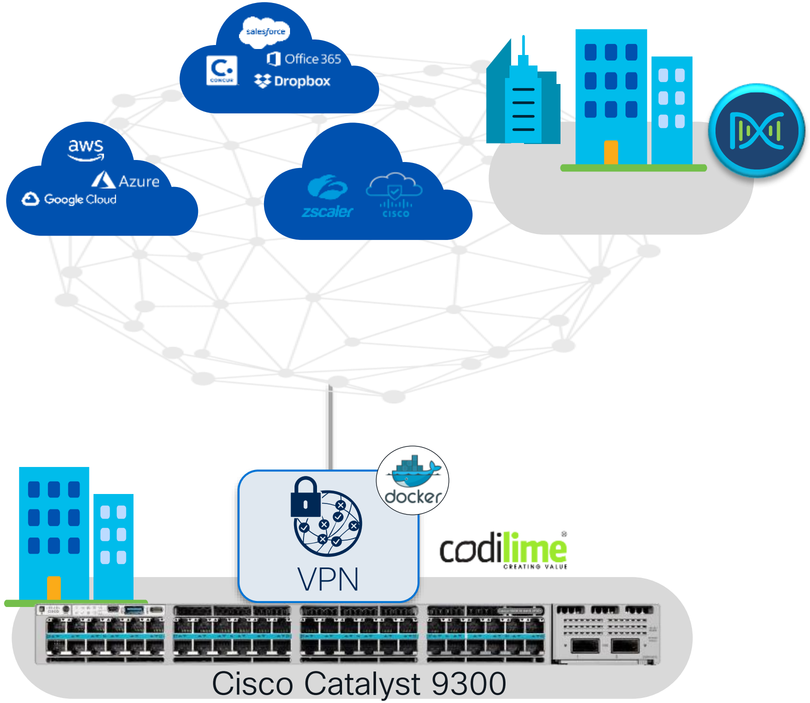
Rich ecosystem partnership with 25+ certified apps and 200+ active customer

	Resource type	Catalyst 9300	Catalyst 9300X	Catalyst 9400	Catalyst 9400X	Catalyst 9500	Catalyst 9500X	Catalyst 9600	Catalyst 9600X
Networking	AppGig Port	1x1G	2x10G	1x1G	2x10G	Mgmt Port*	2x10G	Mgmt Port*	Mgmt Port* (2x10G CPU ports)
Resources	Memory	2GB	8GB	8GB	8GB	8GB	8GB	8GB	8GB
	CPU	1 core	2 core	1 core	1 core	1 core	1 core	1 core	1 core
	Storage	240GB (USB3.0/SSD)	240GB (USB3.0/SSD)	480-960GB (SATA)	480-960GB (SATA)	480-960GB (SATA)	480-960GB (SATA)	480-960GB (SATA)	480-960GB (SATA)

* Using loopback with any external ports

New IPsec App enabled via App Hosting

Purpose built for IPsec



- ✓ VPN Application hosted on Catalyst 9000
- ✓ Runs in Docker container
- ✓ WebUI for IPsec config
- ✓ Life Cycle Management via DNA Center
- ✓ HW & SW IPsec – Catalyst 9300X
- ✓ SW IPsec – C9300/9300L/C9300LM
- ✓ Will be available on Devnet

docker

- Minimal resources required
  - 1 CPU core
  - < 1 GB memory
- 200-500M throughput
- QAT for higher throughput*

Open Source

IPSEC VPN: strongSwan

Routing: FRROUTING

Expands IPsec capabilities to all Catalyst 9300 models at lower throughput

* On Catalyst 9300X Models

Future of work at Cisco Penn1

"When challenged to lead by example and create a digitized real estate that delivers both outcomes and the needed agility to continually amplify the intersection of people and space, we knew we could bank on Cisco's Smart building framework to get us there" – *Cisco WPR*

- Midtown Manhattan Location
- 54,000 sq. ft. Global Destination
- First Talent and Collaboration Center
- 100% Hybrid, No Assigned Workspaces
- Space Serves Multiple Business Units and Groups

Challenge

- Cisco's opportunity and responsibility to showcase smart buildings that define the future of work
- Cisco WPR and IT created 'the office of the future' to improve experience, increase collaboration and meet NYC goal of 80% carbon emission reduction by 2050.
- This office is a customer experience center, a showcase and a state of art lab of smart building technologies

Penn1 - Design strategy and outcomes

Smart Building Framework

- *Connect*
  - ✓ Catalyst 9000 90W switches and APs
- *Configure*
  - ✓ Meraki surveillance cameras
  - ✓ WEBEX room kits, desk pros
  - ✓ Molex & Igor PoE lights/sensors
  - ✓ Mecho & Somfy shade control
  - ✓ Delta VAV HVAC control
  - ✓ Smart energy metering PDU
  - ✓ 90W USB-C dongles
  - ✓ 90W connected desks (prototype)
- *Control*
  - ✓ Cisco SDA endpoint analytics and PoE Assurance
- *Consume*
  - ✓ Cisco DNA spaces workspace application

Business outcomes

LEED Building Alignment	✓
WELL Building Alignment	✓
Consistent End User Experience	✓
Touchless Room Control	✓
Integrated Base Building Control	✓
People Count and Density Monitoring	✓
People Count Data to BMS	✓
Air Quality Monitoring and Display	✓
IT Ops Model Reinvention	✓
USB-C Adoption	✓
Low Voltage Connected Desk	✓
Flexible Technology Swap Out	✓

~5% CapEx Savings, $250k Cost Avoided

Technical Session Surveys

- Attendees who fill out a minimum of four session surveys and the overall event survey will get Cisco Live branded socks!
- Attendees will also earn 100 points in the Cisco Live Game for every survey completed.
- These points help you get on the leaderboard and increase your chances of winning daily and grand prizes.

Cisco Learning and Certifications

From technology training and team development to Cisco certifications and learning plans, let us help you empower your business and career. www.cisco.com/go/certs

Pay for Learning with Cisco Learning Credits

(CLCs) are prepaid training vouchers redeemed directly with Cisco.

Learn

Cisco U.
IT learning hub that guides teams and learners toward their goals

Cisco Digital Learning
Subscription-based product, technology, and certification training

Cisco Modeling Labs
Network simulation platform for design, testing, and troubleshooting

Cisco Learning Network
Resource community portal for certifications and learning

Train

Cisco Training Bootcamps
Intensive team & individual automation and technology training programs

Cisco Learning Partner Program
Authorized training partners supporting Cisco technology and career certifications

Cisco Instructor-led and Virtual Instructor-led training
Accelerated curriculum of product, technology, and certification courses

Certify

Cisco Certifications and Specialist Certifications
Award-winning certification program empowers students and IT Professionals to advance their technical careers

Cisco Guided Study Groups
180-day certification prep program with learning and support

Cisco Continuing Education Program
Recertification training options for Cisco certified individuals

Here at the event? Visit us at **The Learning and Certifications lounge at the World of Solutions**

Continue your education

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

The bridge to possible

Thank you

cisco Live!

#CiscoLive