
cisco Live!
ALL IN

The bridge to possible

What is Your First Step in Protecting Endpoints and Reducing the Attack Surface?

Identify unknown endpoints and protect your workplace

Krishnan Thiruvengadam, Technical Leader Technical Marketing
Twitter: @KrishnanThiruv1

BRKENS-2850

Cisco Webex App

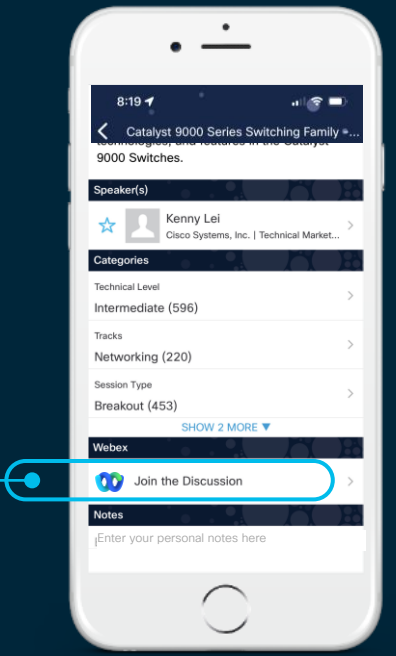
Questions?

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.

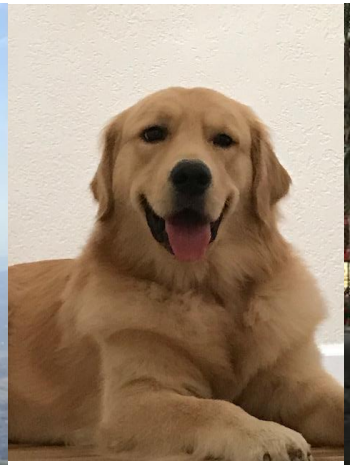


https://ciscolive.ciscoevents.com/ciscolivebot/#BRKENS-2850

Connecting machines and people securely

About me

Married with 2 kids and Max(below). Moved to west coast from Boston 7 years back. Never looked back.
Love music, nature, visiting national parks, travel.

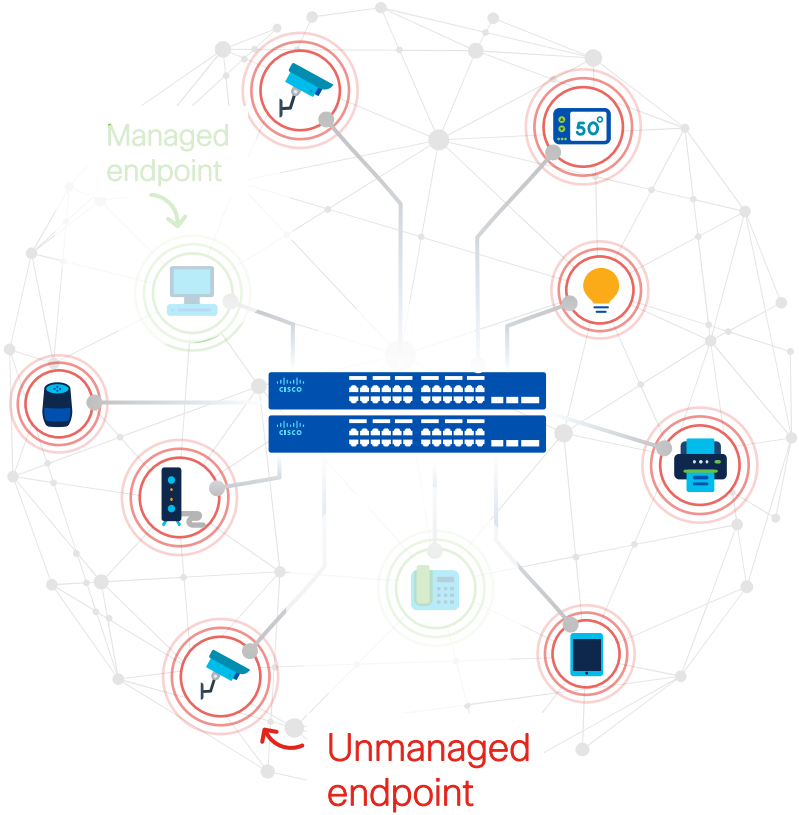


Agenda

- Challenges
- AI Endpoint Analytics: Profiling Overview
- Demo of Endpoint Analytics
- Policy Enforcement with ISE
- Group Based Policy Analytics
- Conclusion

Challenges

What's happening in the workplace?



1:5 ↑

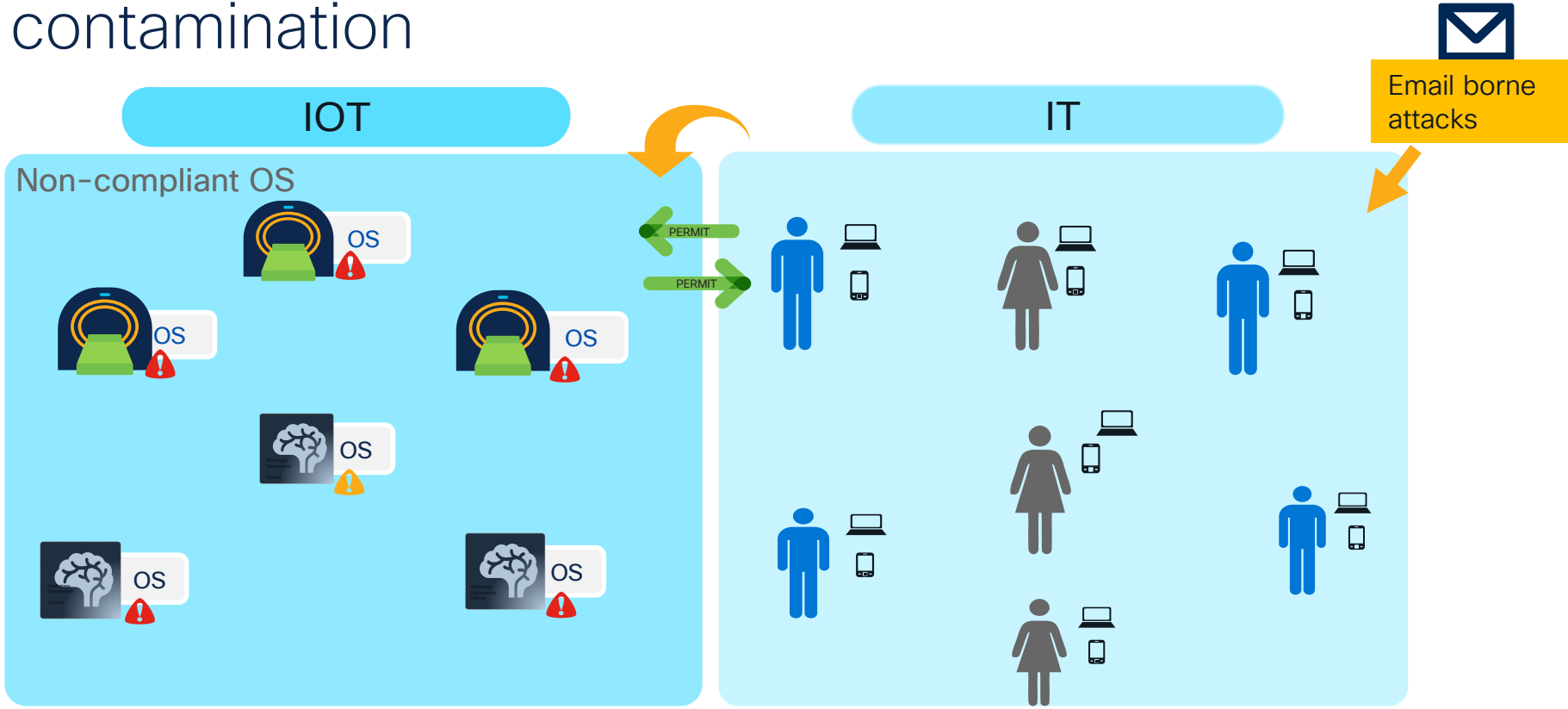
Unmanaged device proliferation.

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

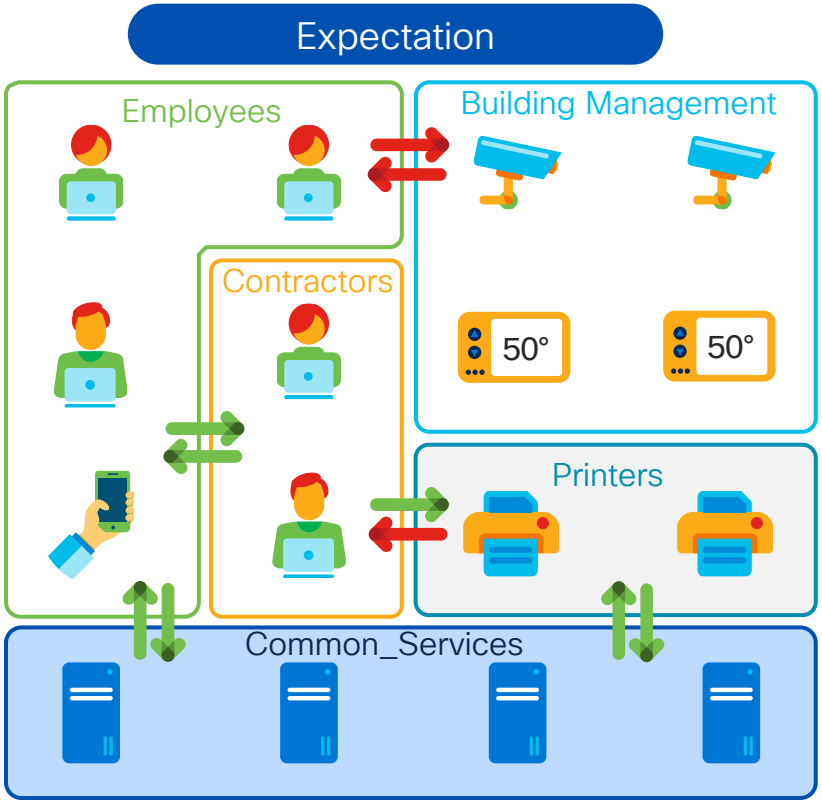
Secure authentication mechanisms unusable on unmanaged endpoints

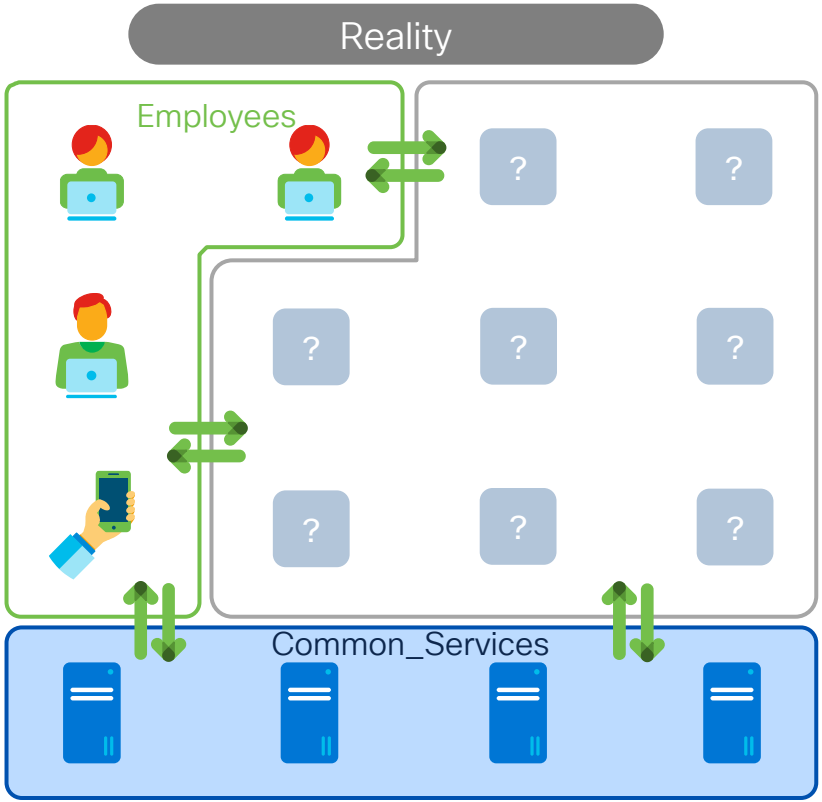
Open, unsegmented networks with IOT devices put organizations at risk

Ineffective segmentation causes cross-contamination

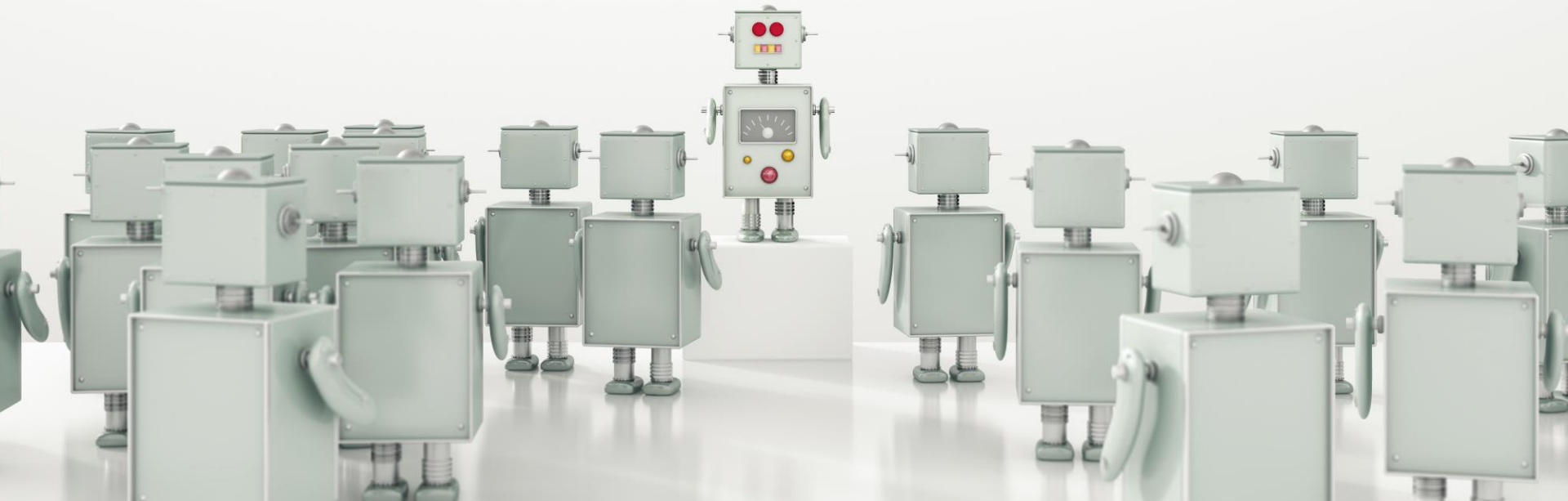


Segmentation: Expectation vs Reality





How can you identify and categorize endpoints you don’t know?

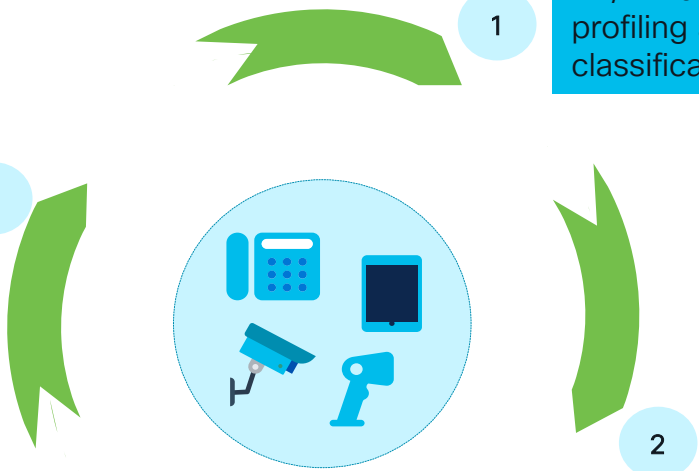


Endpoint Analytics: Deeper visibility and continuous security posture assessment

Deeper endpoint visibility with **AI-driven analytics** and network driven **deep packet inspection.**

Continuous validation of endpoint anomalies/threats/vulnerabilities

SD-Access for Zero Trust for Workplace



1. AL/ML driven endpoint profiling and multi-factor classification for IOT.

2. Traffic Analysis for Granular policy discovery towards micro-segmentation

3. AL/ML led network behavioral anomaly detection, threats and vulnerabilities

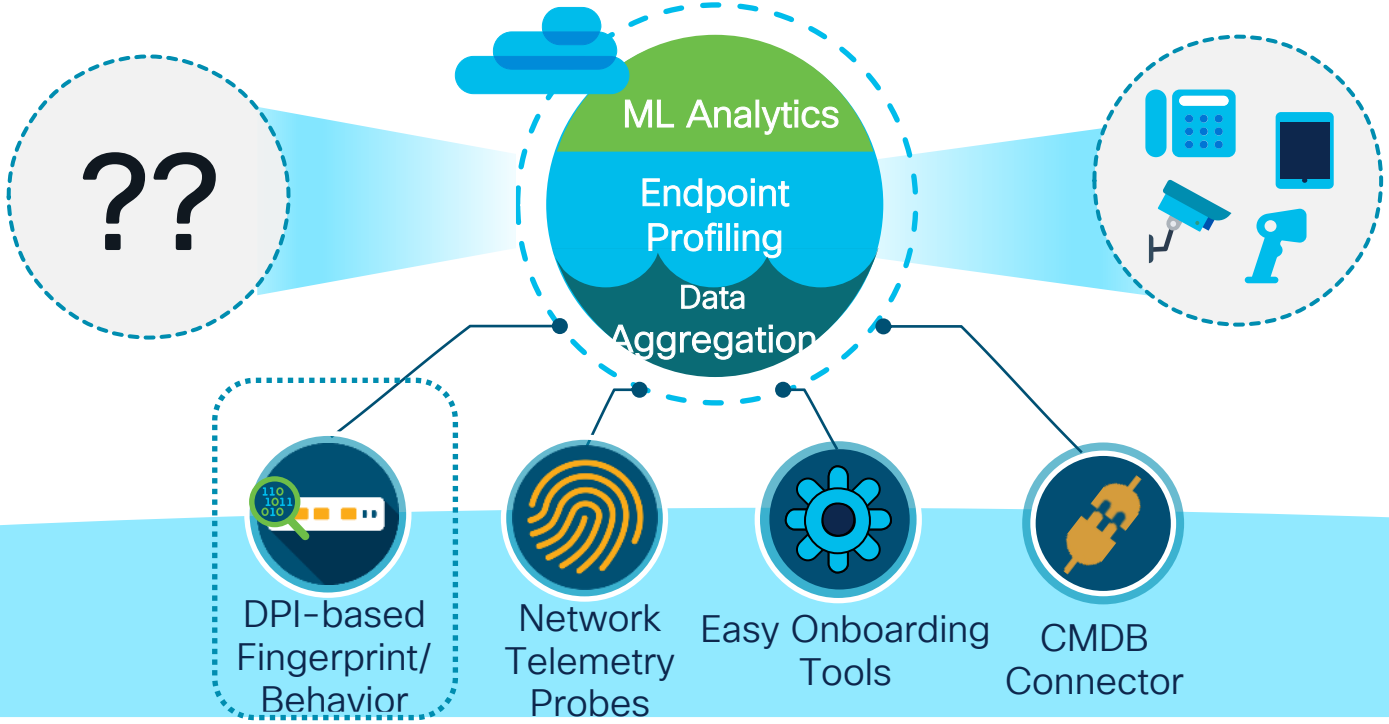
4. Mitigation actions and remediations with Cisco ISE

Endpoint Analytics: Profiling Overview

cisco Live!

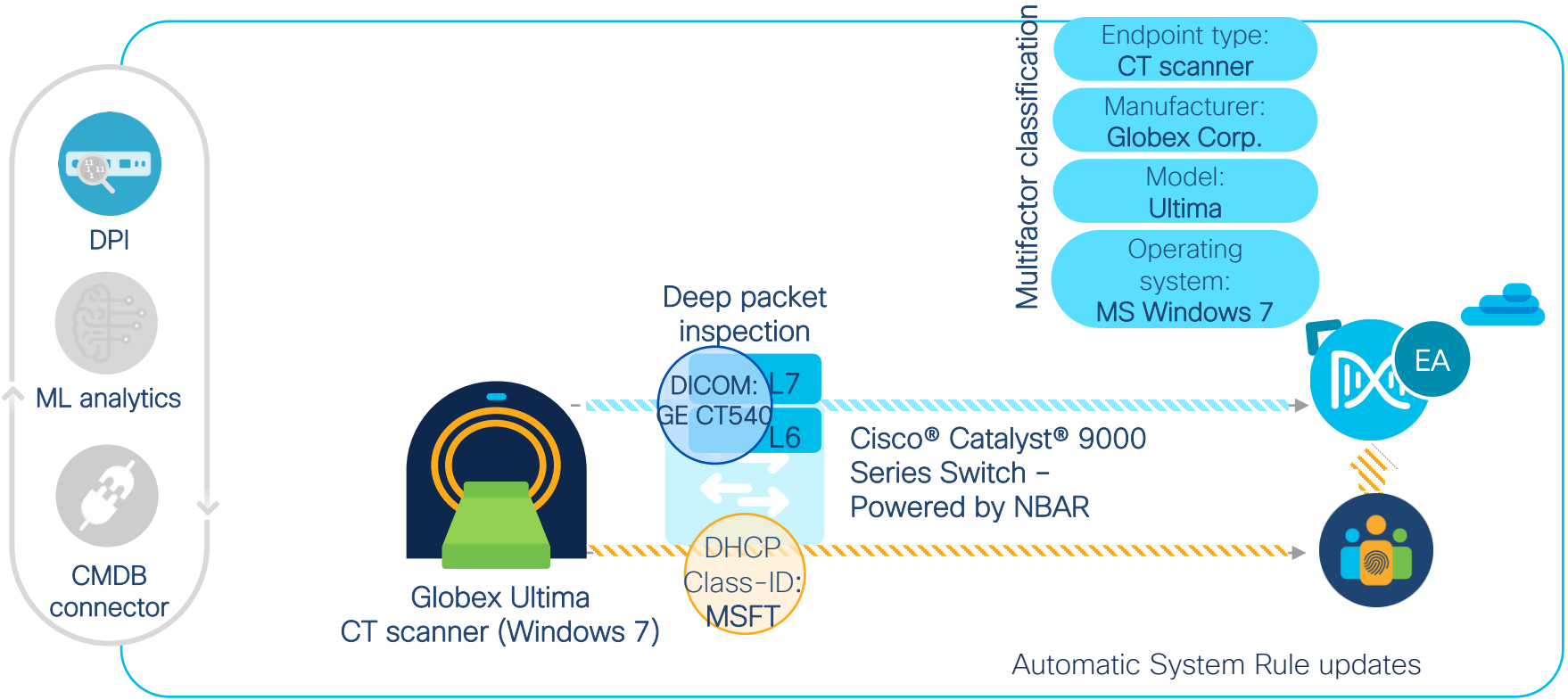
Endpoint profiling, data sources and ML Analytics

Rapidly reducing the unknowns by aggregating data from different sources



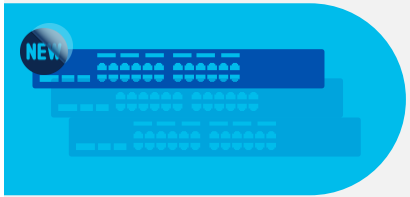
CMDB: Configuration Management Database

Classification based on Deep Packet Inspection (DPI)



Traffic Telemetry Protocols

Support for 1400+ application protocols
Protocol library gets updated via Cisco DNAC



Cisco® Catalyst ® 9000 Series Switch and Catalyst 9800 Wireless (Traffic Telemetry-Embedded)

Data plane protocols:

Healthcare:	DICOM, HL7,
Web/IOT:	HTTP, SSL,
Building automation:	MQTT, COAP, BACNET...
Multicast:	mDNS...
Media and communication:	RTSP, RTCP, SIP...
Others:	CIFS, MS-SQL,

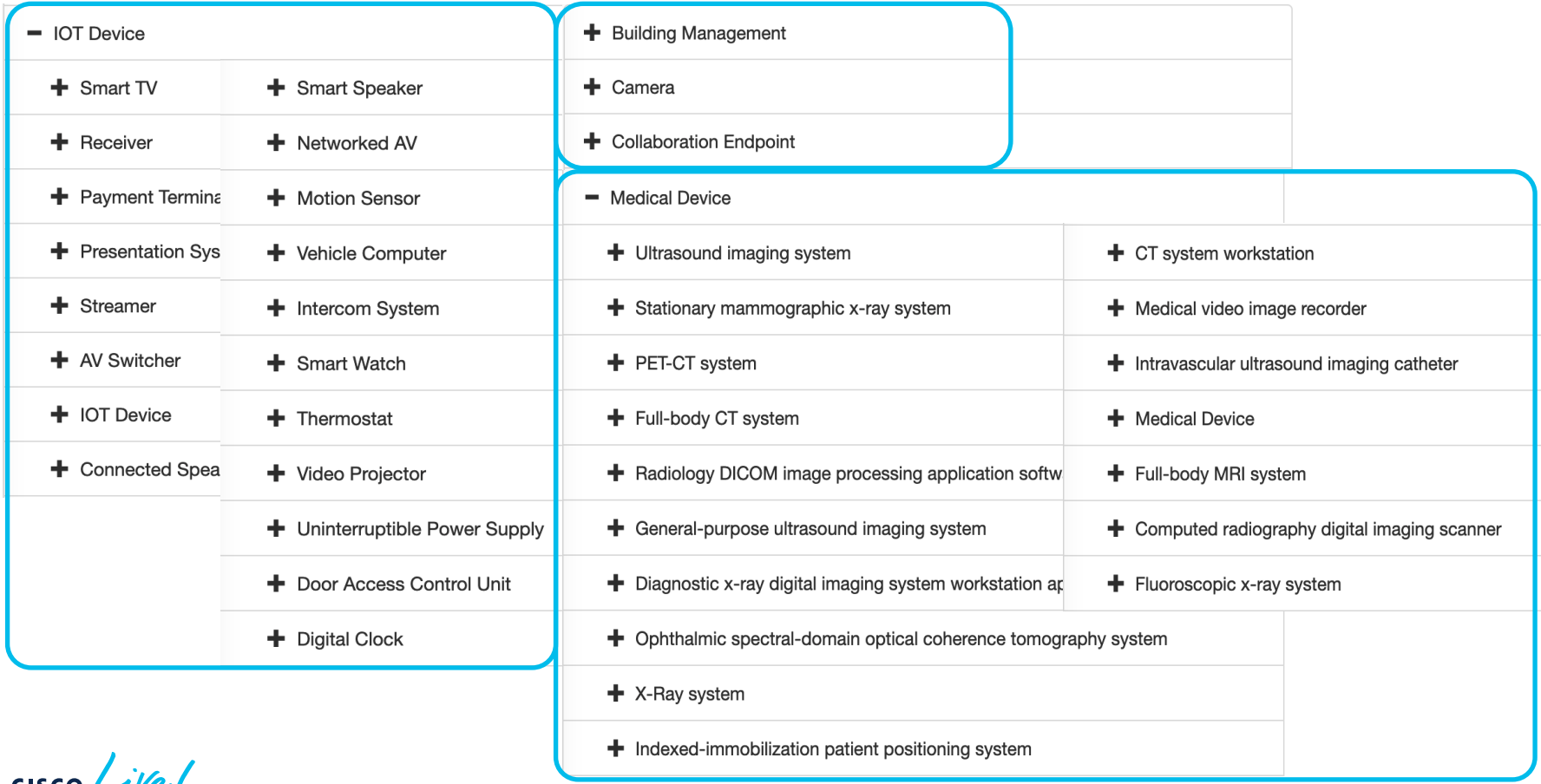
Discovery protocols:

CDP, LLDP, SNMP, DHCP, ...

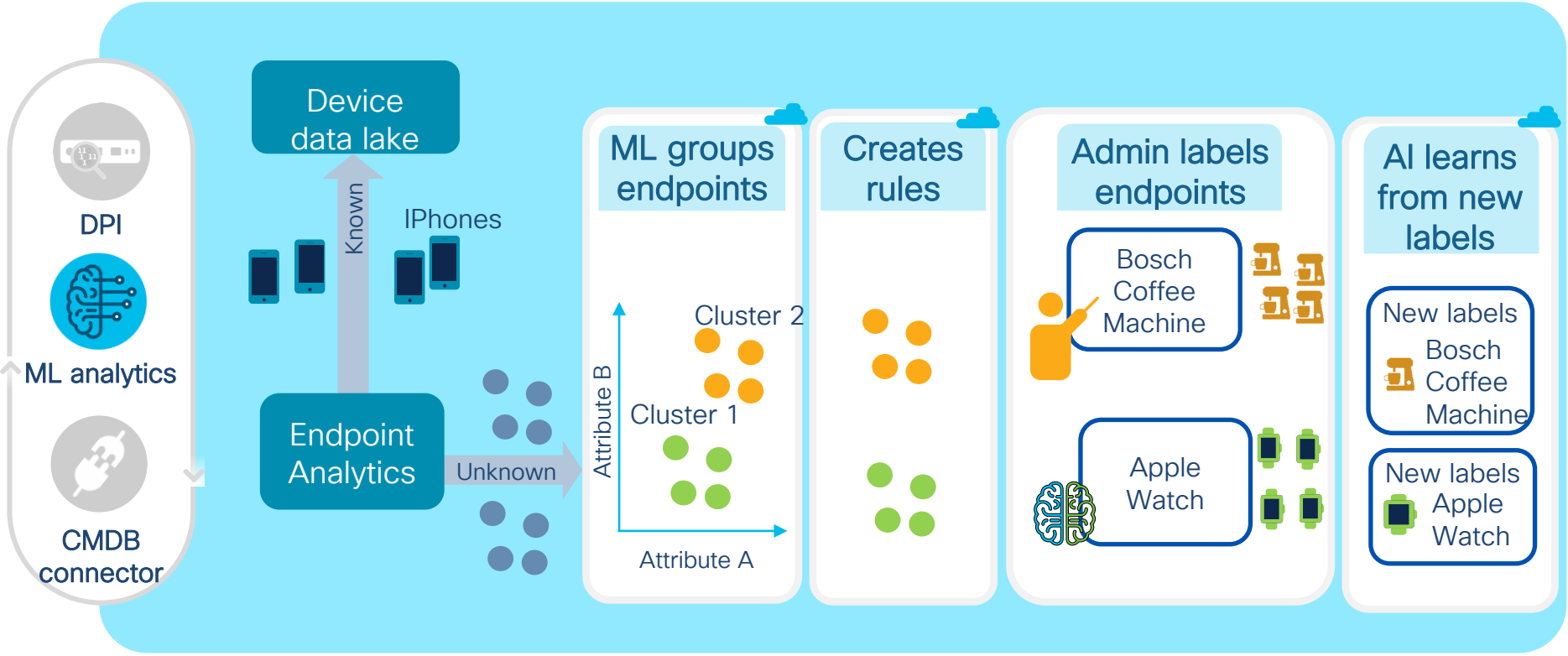
Available from IOSXE:v17.3.1

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

Device Insights: Sample Devices Identified

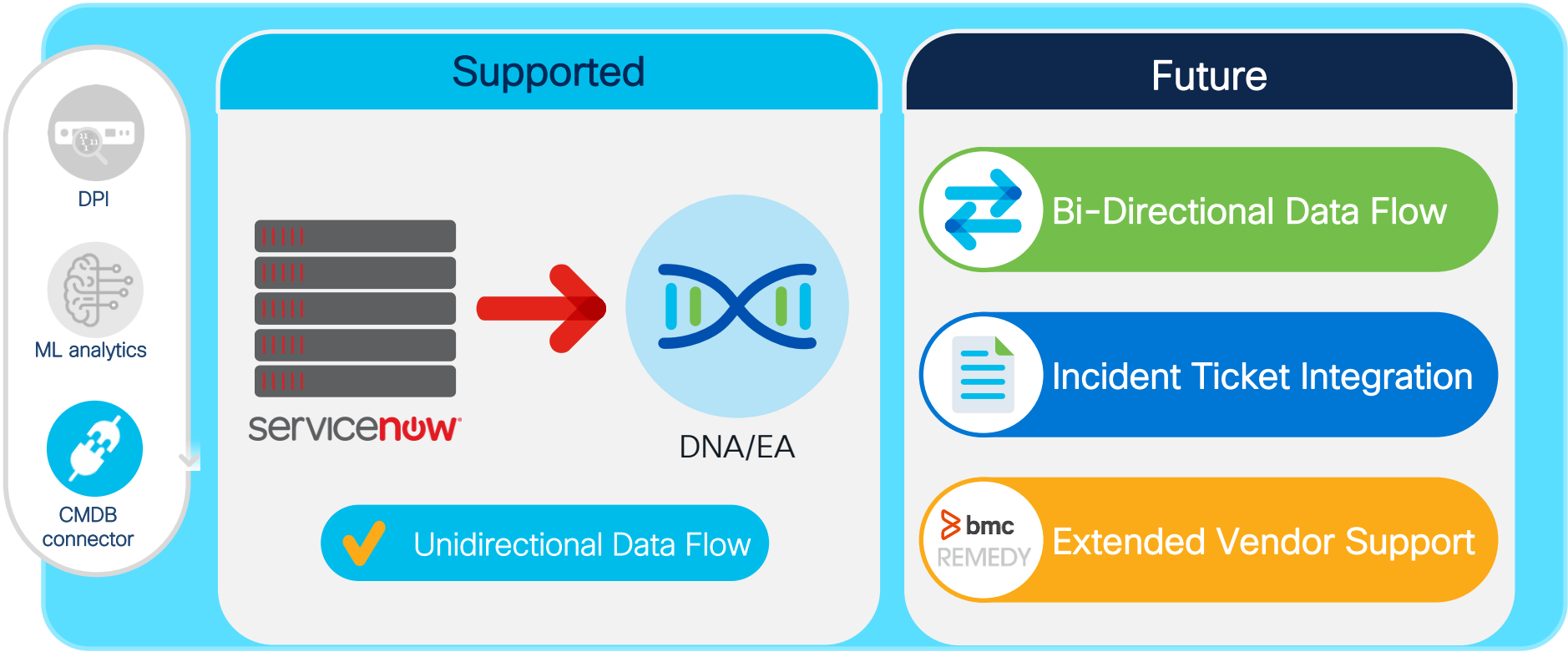


Reducing Unknowns with Machine Learning



= done in cloud

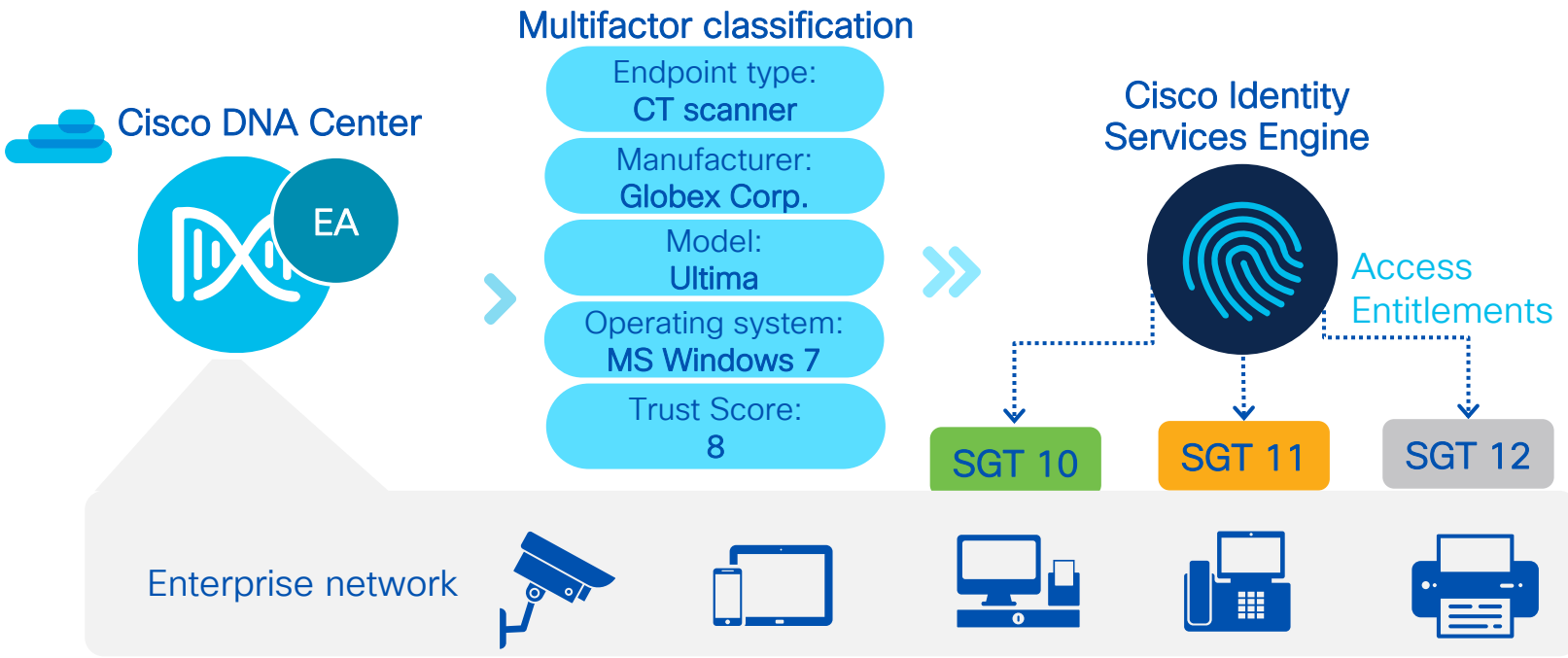
Exchange information with your CMDB



Demo

Policy Enforcement with Cisco ISE

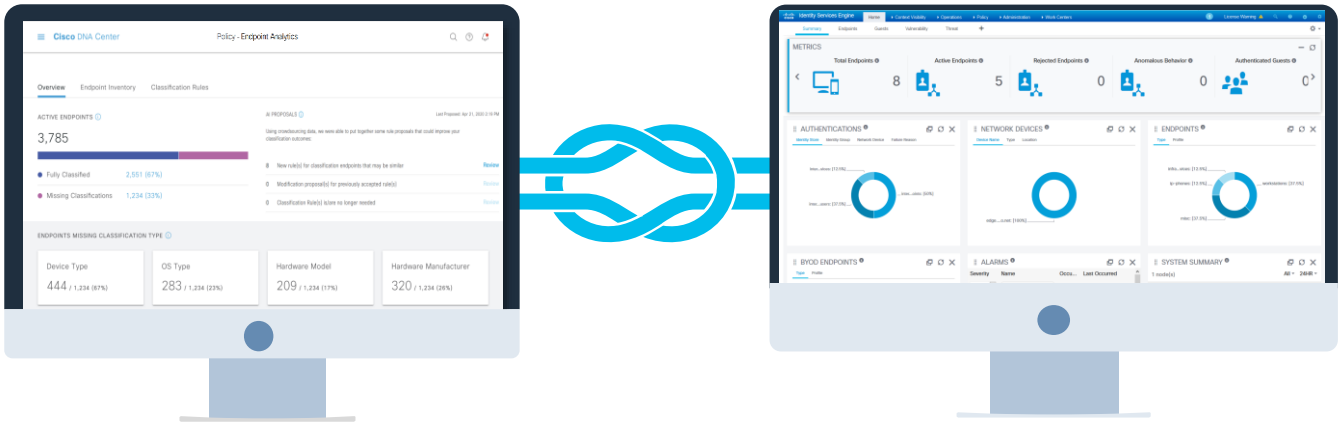
Granular profiling reduces unauthorized access



DNAC 2.2.3

ISE 3.1

Seamless integration with Cisco ISE



Endpoint Analytics attributes in authorization policy

Endpoint Analytics attributes in ISE authorization policy

Assessment score for anomalies detected

aiAnomalyResult
concurrentmacaddress Result
mfcAnomalyResult
natAnomalyResult

Endpoint Analytics profile labels

deviceType
hardwareManufacturer
hardwareModel
operatingSystem

EA Hierarchy

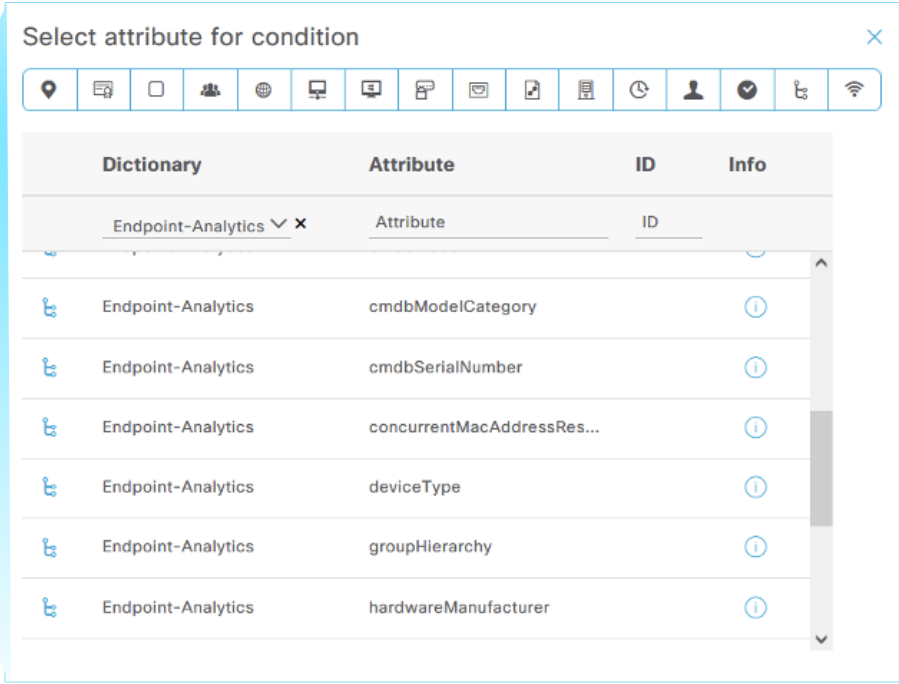
groupHierarchy

ServiceNow attributes

cmdbxxxxxx

Overall TrustScore

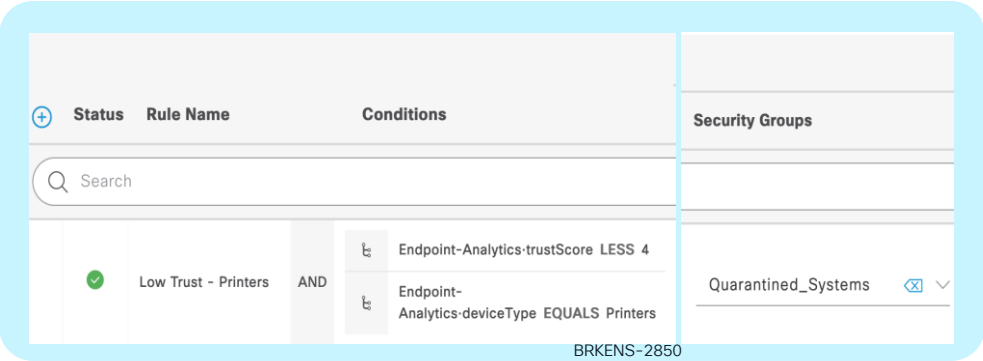
trustScore



Using Endpoint Analytics attributes in authorization policy

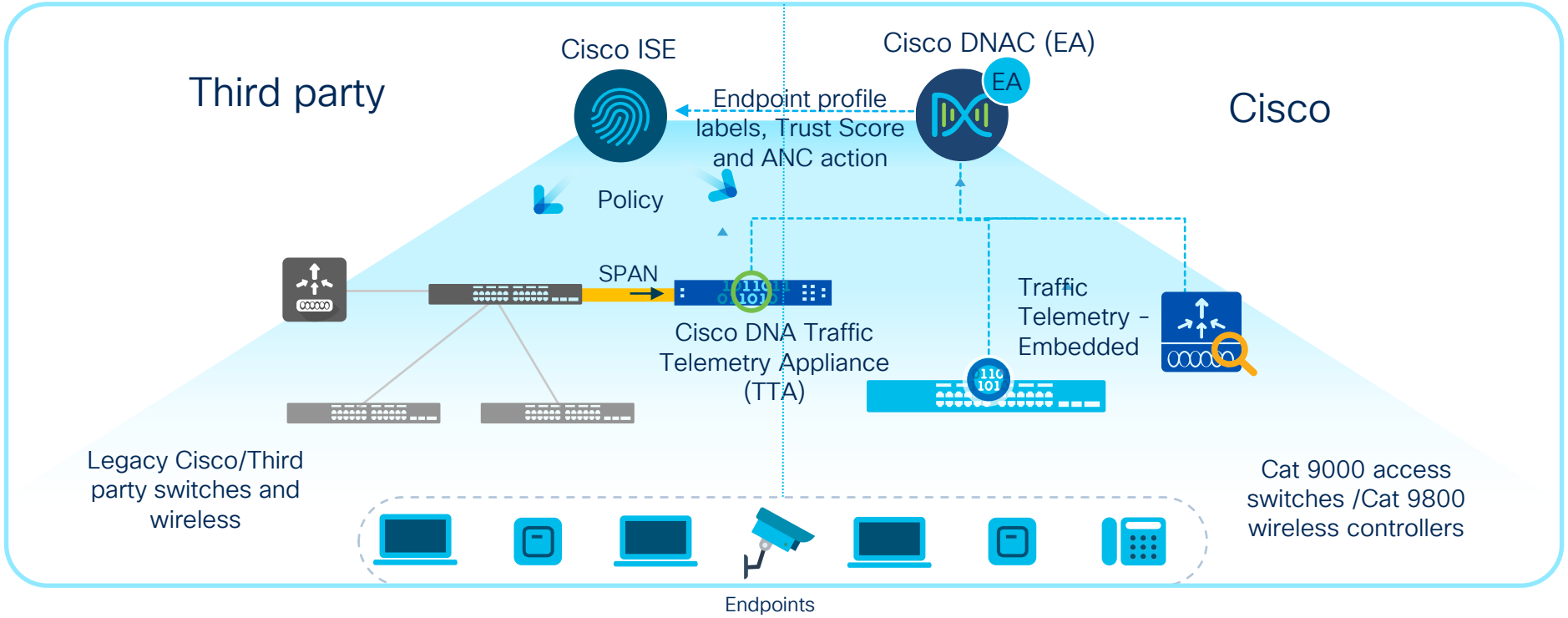
For example, authorization policy for **Low Trust - Printers**:

If Endpoint Analytics: device type is Printer + Endpoint Analytics: trust score is less than 4 ,Then Assign SGT = Quarantine System



ISE 3.1→16 attributes

Supported Deployment Scenarios

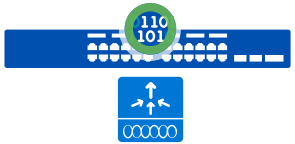


Cisco DNAC TTA supports SPAN, RSPAN and ERSPAN

Minimum EA requirements for visibility and policy

Cisco DNA Center: 2.1.2.4 (General Availability)
License: DNA Advantage

Cisco ISE: 2.4 p11+, 2.6 p5+, 2.7 p1 and upwards
License: ISE Plus or equivalent



Wired: Cisco® Catalyst® 9200/9300/9400: 17.3.1
Wireless: Cisco® Catalyst® 9800 WLC: 17.3.1

Cisco DNA Traffic Telemetry Appliance (DN-APL-TTA-M)

"AI endpoint analytics has greatly simplified how we manage our network. We get the granular details we need for every device, and with its intelligent grouping of similar devices, we save precious time and reduce complexity by orders of magnitude."

"We plan to build on this feature to bolster organizational security through our network."

-Brian Jensen, Network Analyst, North Carolina Department of Health and Human Services

"It is now a centerpiece of our security strategy, and we are using the unprecedented visibility and insights endpoint analytics provides to keep our healthcare network secure and compliant with HIPAA regulations"

"We signed up to test Cisco's new AI endpoint analytics application as soon as it was available. Right away it exceeded our expectations by identifying a large majority of the 58,000 devices we have in our system."

– Ed Vanderpool, Senior IT Manager, Adventist Health

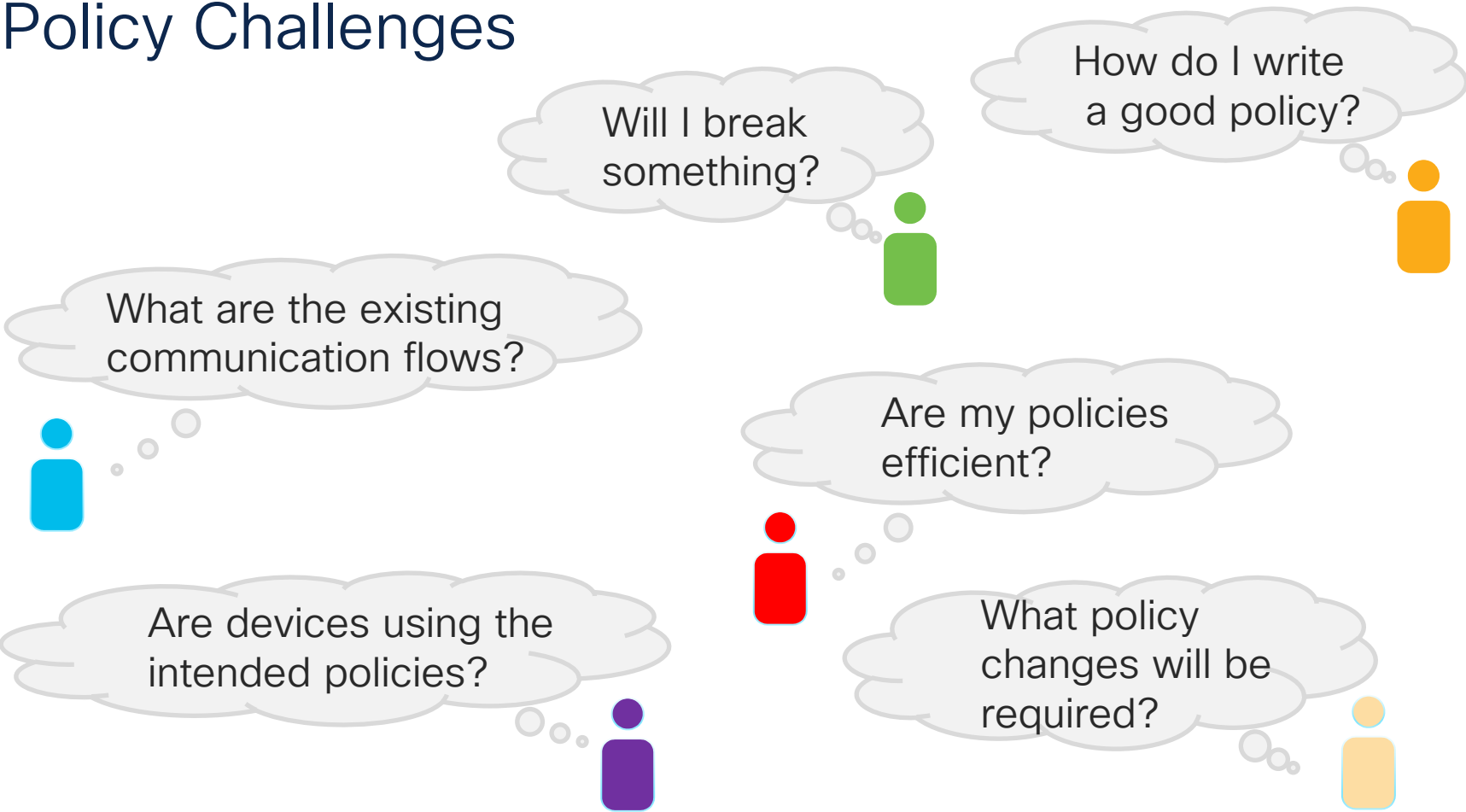
Reference: https://blogs.cisco.com/networking/north-carolina-dhhs-uses-ai-endpoint-analytics-to-simplify-network-control

Reference: https://blogs.cisco.com/networking/adventist-health-deploys-ai-endpoint-analytics-to-keep-its-network-in-shape

Group based policy Analytics

cisco Live!

Policy Challenges



Policy Analytics

Deploy group polices with confidence

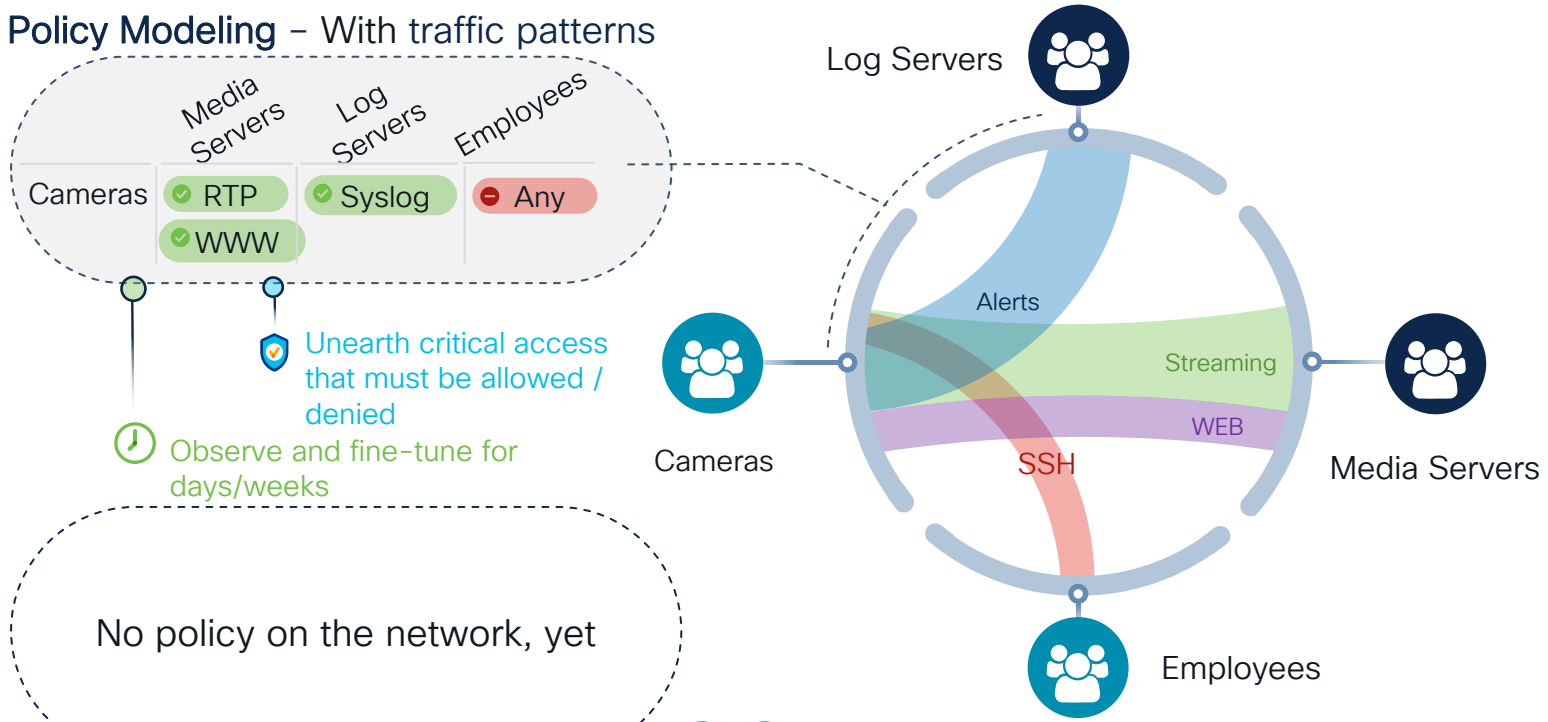
Policy Modeling – With traffic patterns

	Media Servers	Log Servers	Employees
Cameras	RTP WWW	Syslog	Any

Unearth critical access that must be allowed / denied

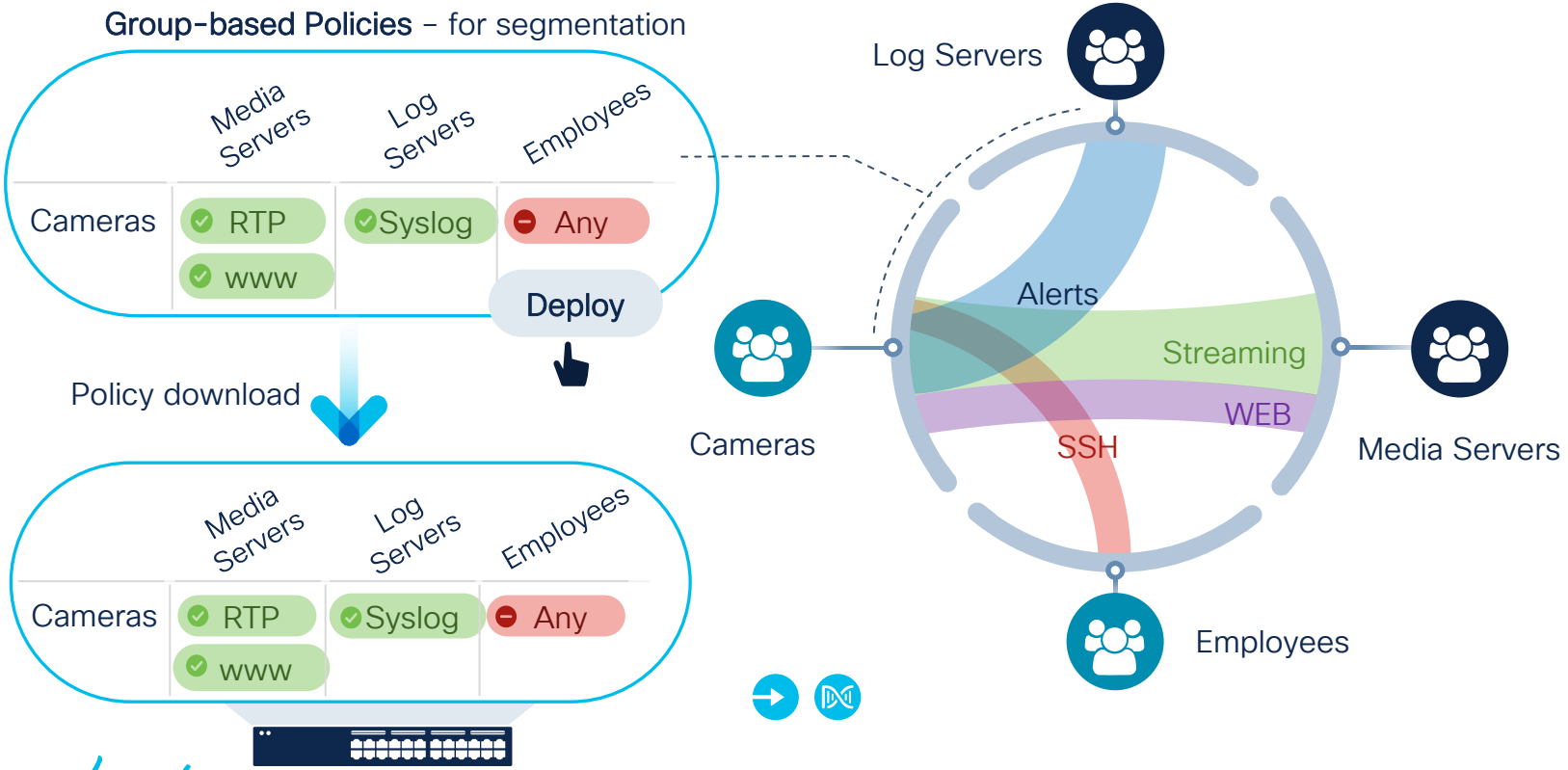
Observe and fine-tune for days/weeks

No policy on the network, yet



Policy Analytics

Deploy group polices with confidence



AI Endpoint Analytics References

Introduction: What is AI Endpoint Analytics?
Whitepaper: Cisco AI Endpoint Analytics: A New Path Forward

Podcast: Network Insights with AI Endpoint Analytics
Presentation: Advanced Endpoint Visibility with Cisco AI Endpoint Analytics
Endpoint Analytics solution for MAC/Attribute Spoofing

Case Study: Adventist Health
Case Study: North Carolina DHHS

Blog: To secure your organization begin at the end
Blog: Identify Endpoints, Enforce Policies, and Stop Threats with Network Segmentation

Video: AI Endpoint Analytics Demo
Demo: AI Endpoint Analytics dCloud Demo

Deployment Guide: Cisco AI Endpoint Analytics

Cisco TTA Datasheet

Cisco SDA resources Cisco ISE resources

Group-based Policy Analytics References

Deployment Guide: https://community.cisco.com/t5/networking-documents/group-based-policy-analytics-deployment-guide/ta-p/4096076

TDM: https://salesconnect.cisco.com/#/search/Group-Based%2520Policy%2520Analytics%2520TDM%2520Presentation/content

Hot off the press, new Video/demo: https://cisco.box.com/v/GBPA-Demo-Video

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

Learning map:
https://www.ciscolive.com/global/attend/education/learning-maps.html

- 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

Thank you


cisco Live!
ALL IN