

CISCO *Live!*



#CiscoLive



The bridge to possible

Identifying Suspicious behavior, Limiting attack exposure on Endpoints

Using Trust Analytics

Krishnan Thiruvengadam, Technical Leader, Technical Marketing

Twitter: @KrishnanThiruv1

BRKENS-2851



#CiscoLive

Cisco Webex App

Questions?

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

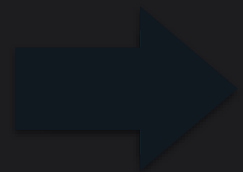
How

- 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-2851>



TRUST



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.

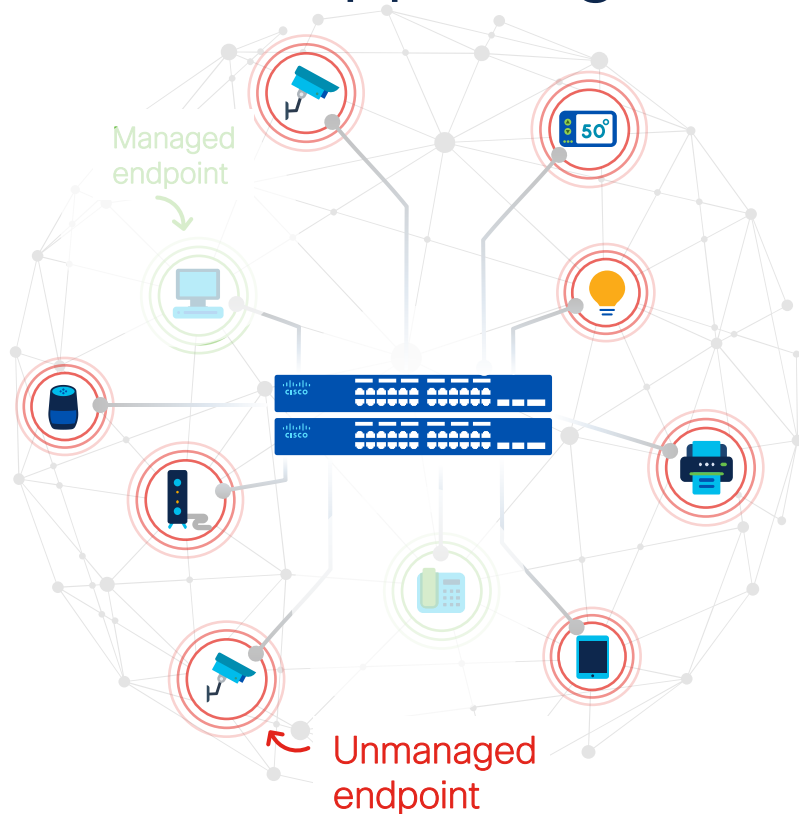




Agenda

- Challenges
- Endpoint Analytics – Quick Overview
- What is Trust Analytics?
- Trust Analytics Use Cases
- Demo
- Conclusion

What's happening in the workplace?



1:5 ↑

Unmanaged device proliferation.



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

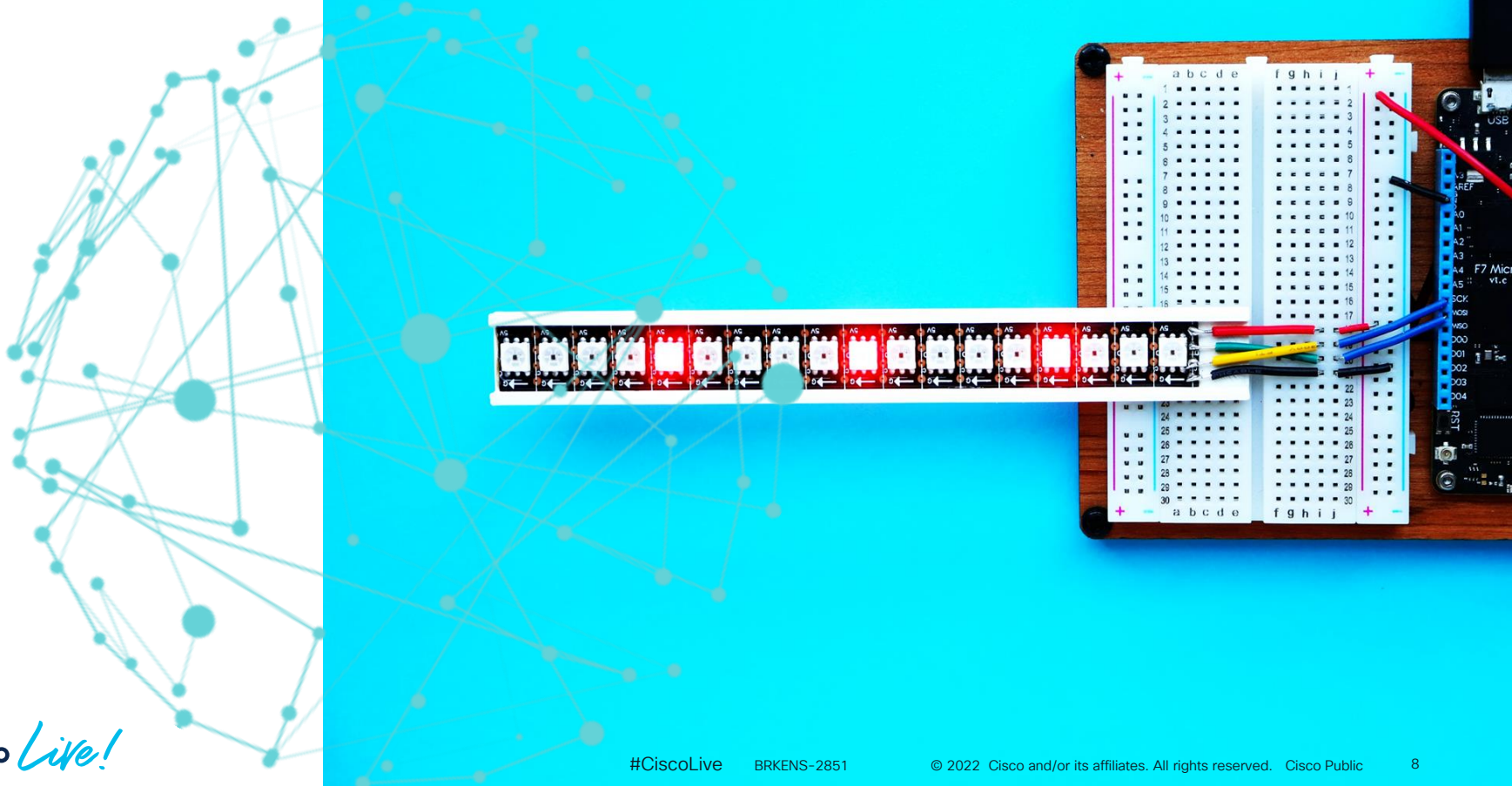


Secure authentication mechanisms **unusable** on unmanaged endpoints

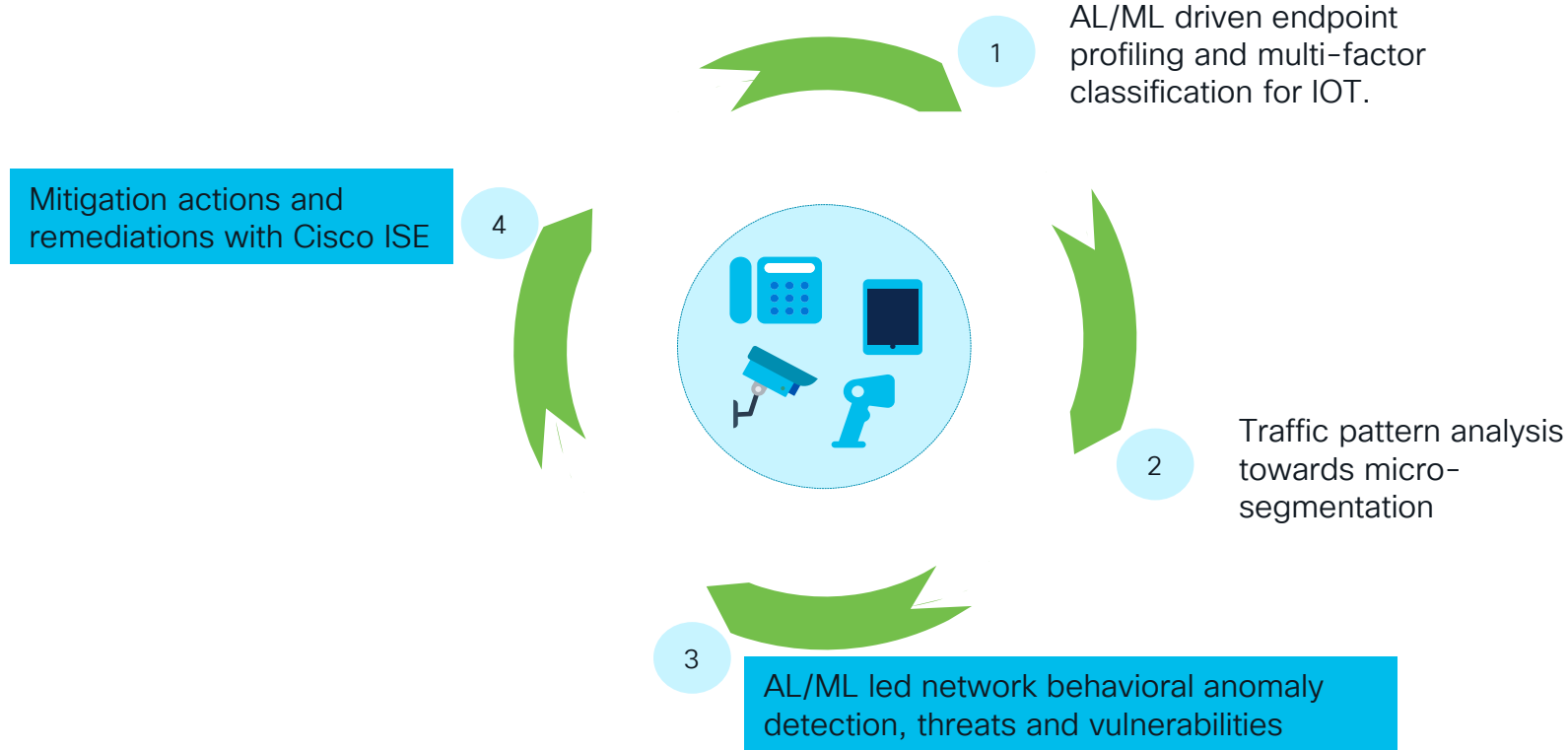


Open, unsegmented networks with IOT devices put organizations at risk

How do we protect our workplace?



SD-Access - Zero Trust for Workplace



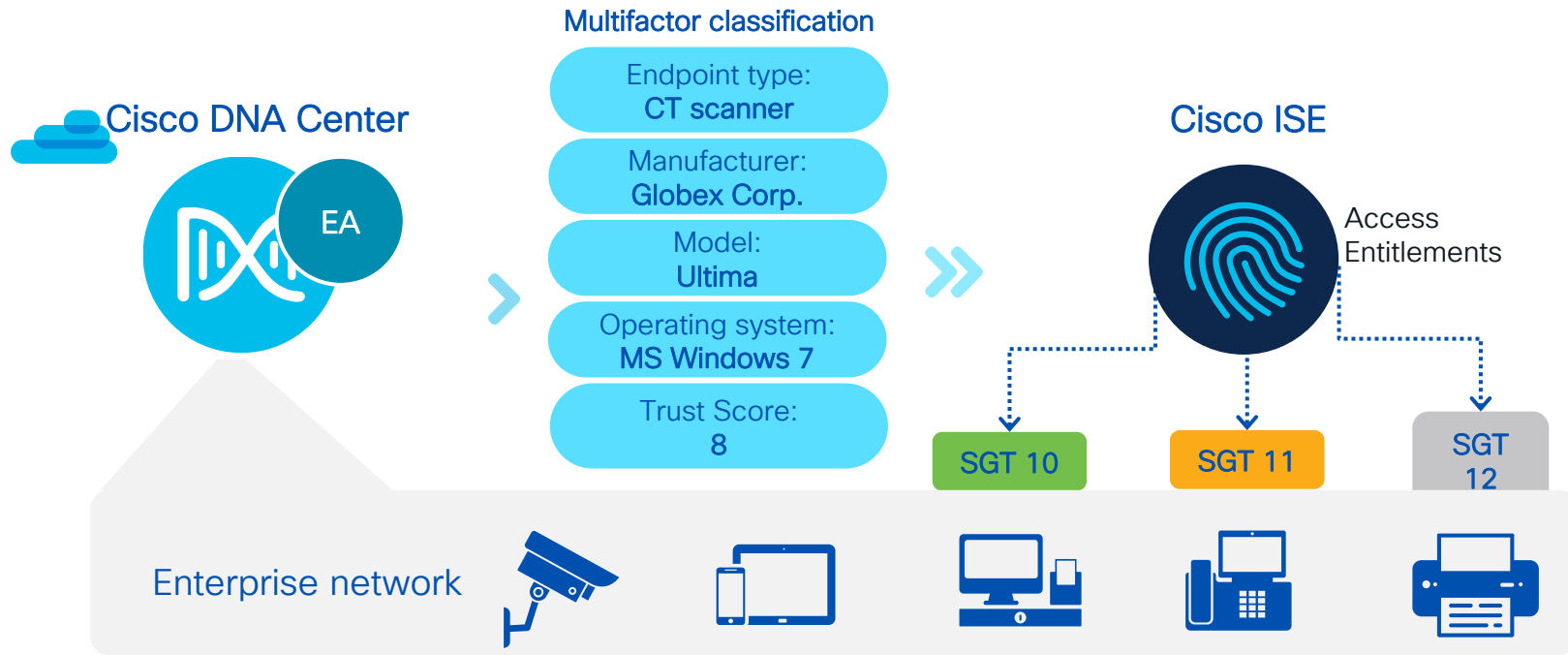
Endpoint Analytics: Deeper visibility and continuous security posture assessment

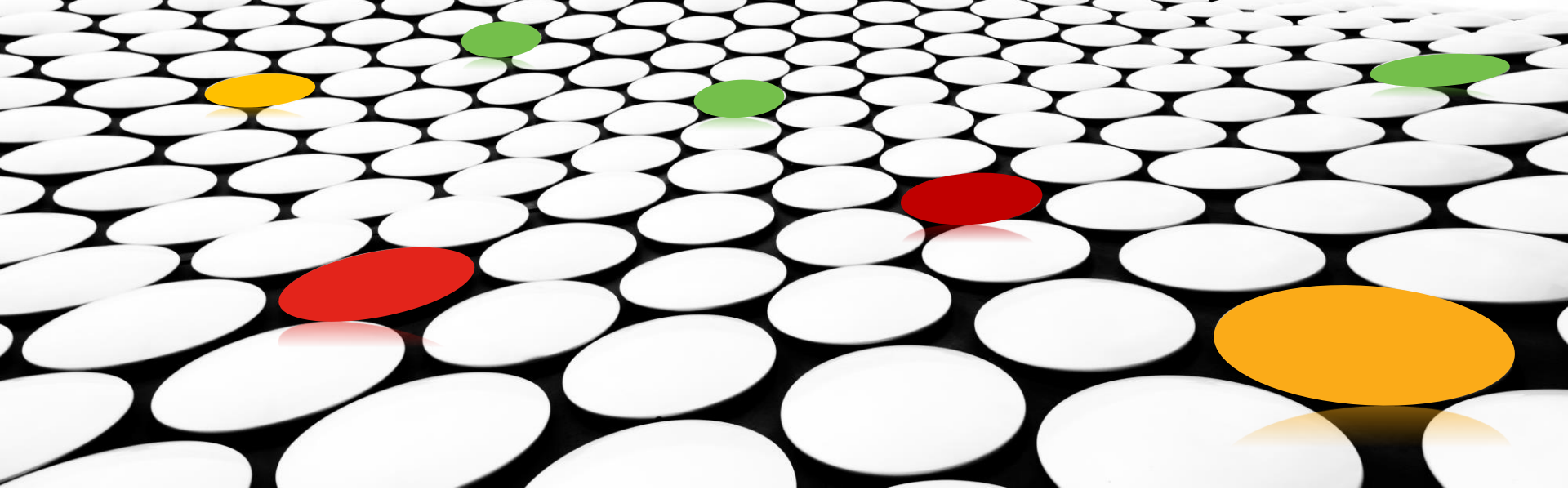


Deeper endpoint visibility with AI-driven analytics and network driven deep packet inspection

Continuous evaluation of endpoint anomalies/threats/vulnerabilities

Endpoint Analytics - Granular profiling reduces unauthorized access

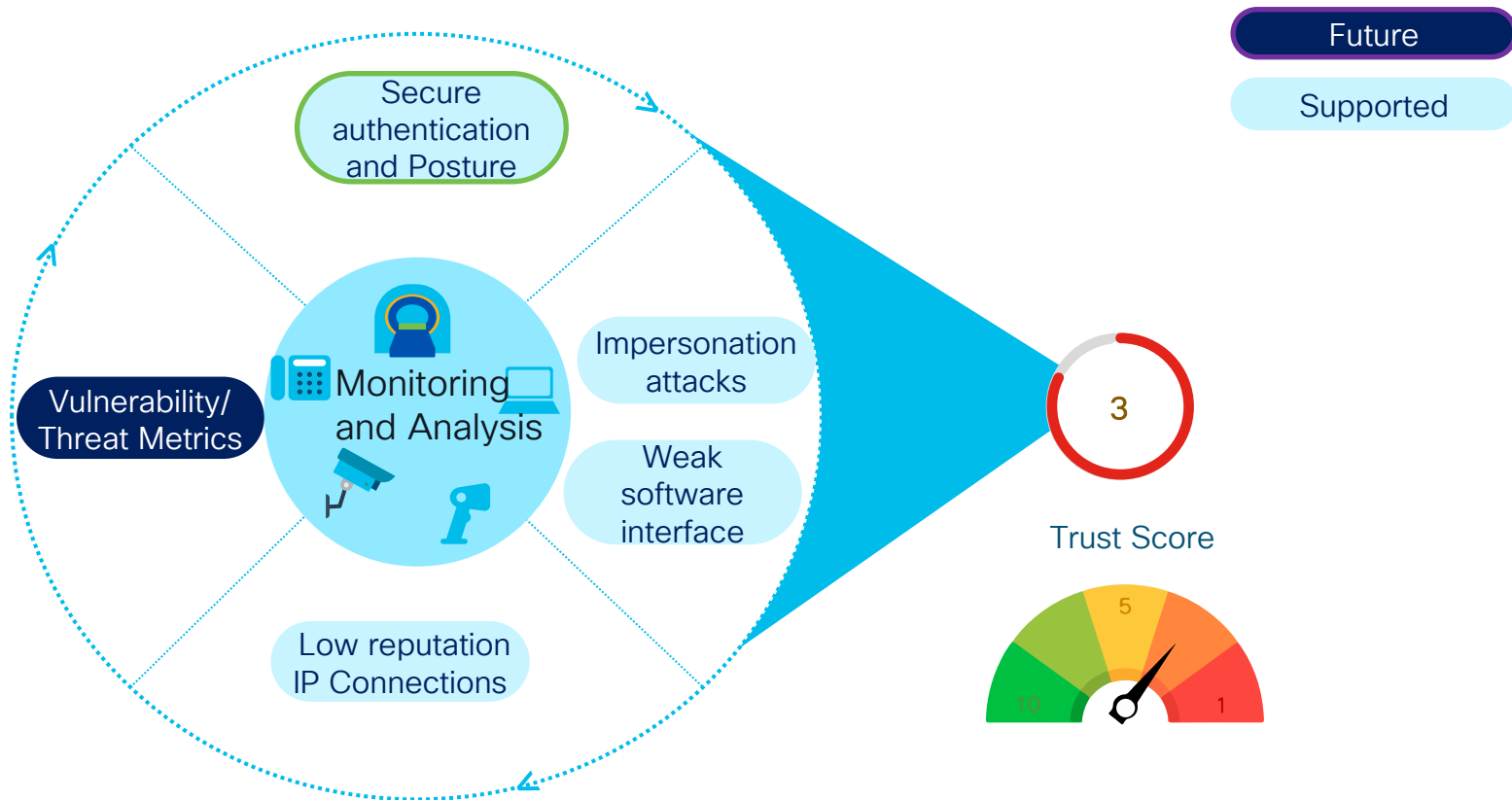




Trust Analytics:

Continuous evaluation of endpoint posture and mitigation actions.

Trust Analytics: Continuous evaluation of security posture for Trusted Access



Trust context and influence on Trust score

Positive Influence

- Secure Authentication
- Posture Compliance



Negative Influence

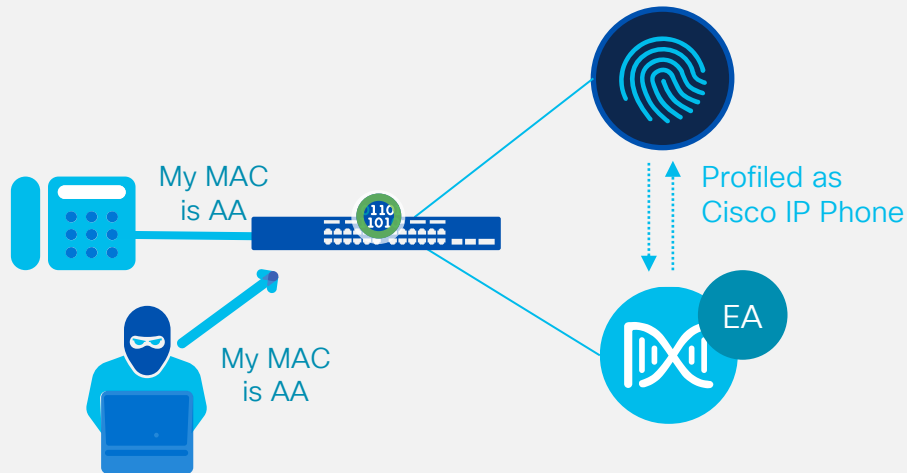
- Impersonation using MAC/Attribute spoofing
- Detecting Insecure software interface
- Connections to Low reputation IP's.

...

...

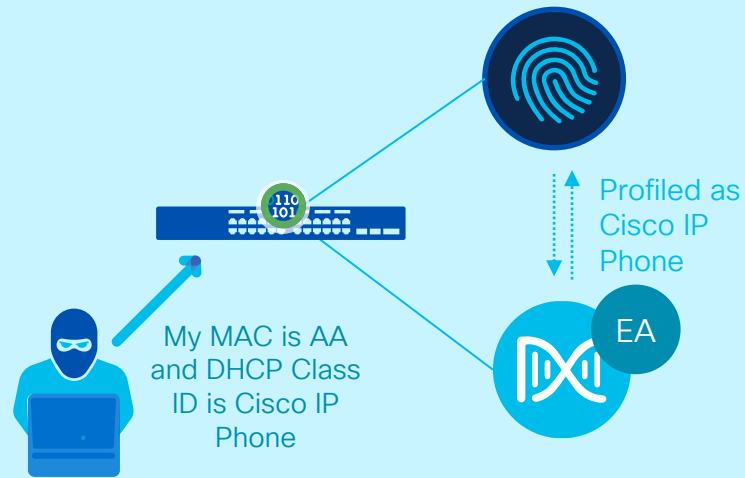
Impersonation with MAC/Attribute spoofing

MAC Spoofing



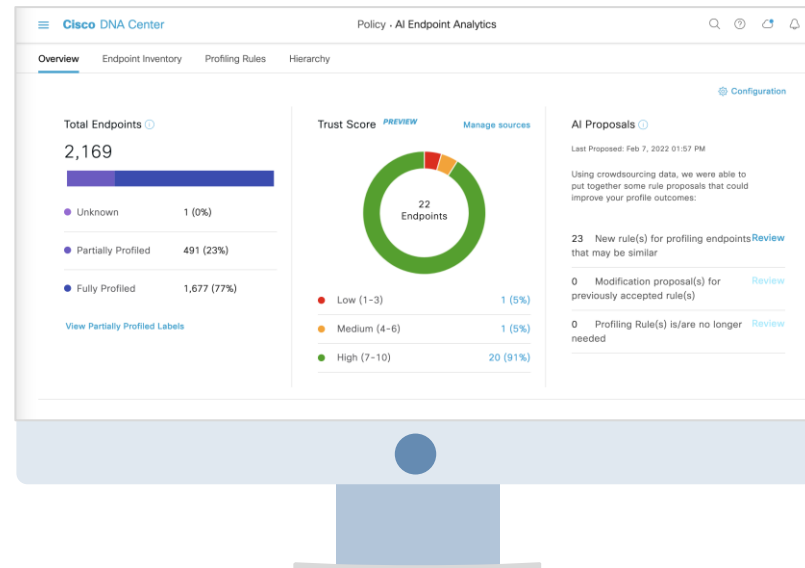
Impersonate MAC address of another authorized endpoint in order to gain the same network access privileges

Attribute Spoofing



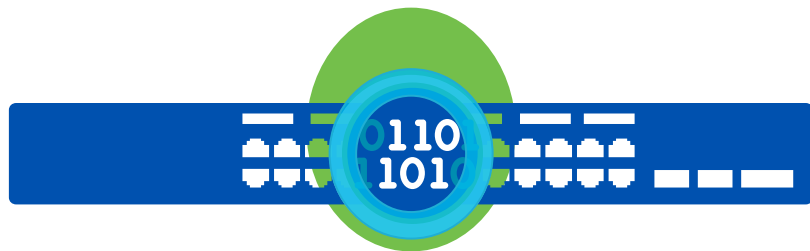
Impersonate class/type of the device in order to get privileged network access

Demo 1: Impersonation attack with MAC/Attribute spoofing



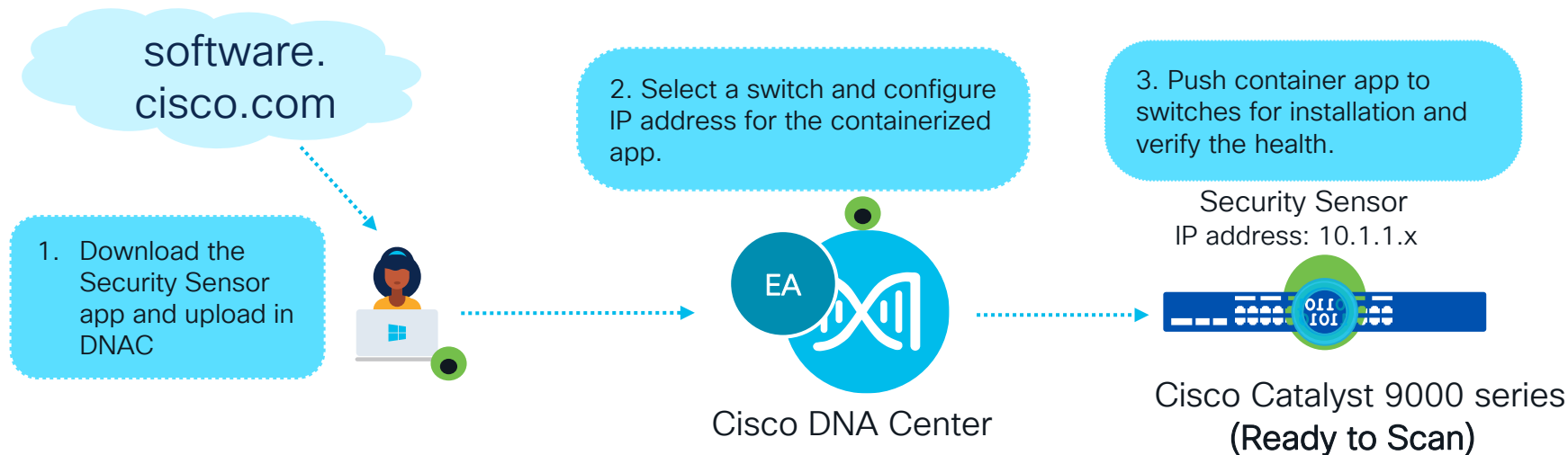
Detecting insecure software interfaces in endpoints

Security Sensor – A containerized application to actively scan for unauthorized open ports and weak login credentials on endpoints



Cisco Catalyst 9000 series

Provisioning Security Sensor Application in 3 steps



Security Sensor → SDAVC app

Scanning for unauthorized open ports and weak login Credentials

1. Admin creates scan lists and schedule scanning

Alert!!
Port 80 open
Using admin/admin for SSH
credentials

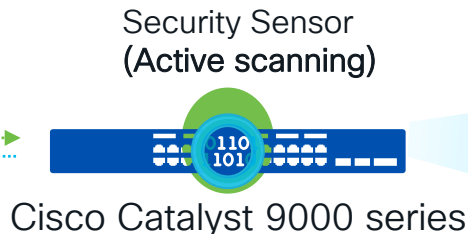
2. Scan results sent to Admins to take action

Unauthorized Port Scan List

Protocol	Ports
TCP	10 - 100
UDP	10 - 100

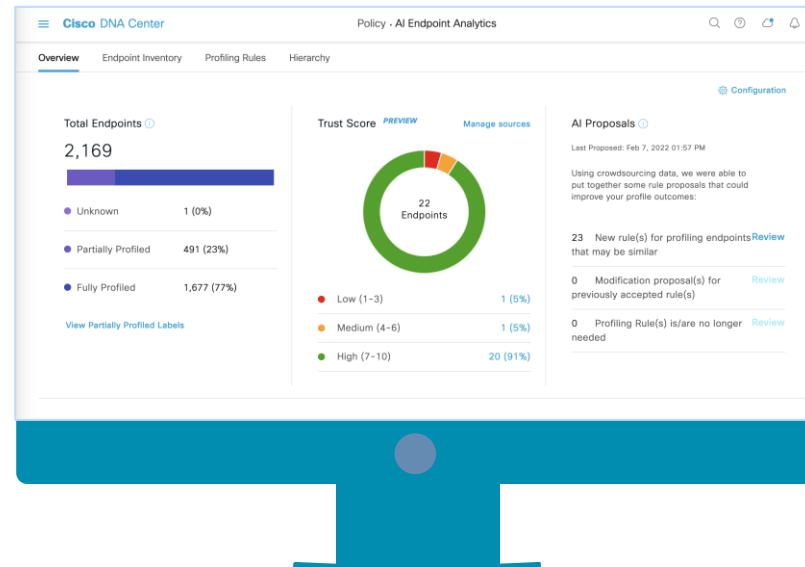
Weak Credential List

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



Customer Network

Demo 2: Detecting weak software interface



Unauthorized connections to low Reputation IP

Use case

- Endpoints have unauthorized connections to ill reputed sites and and malicious IP's that indicates underlying security concern.

Capability

- Enabling Cisco Talos IP Reputation feature in Endpoint Analytics to identify and alert admins.

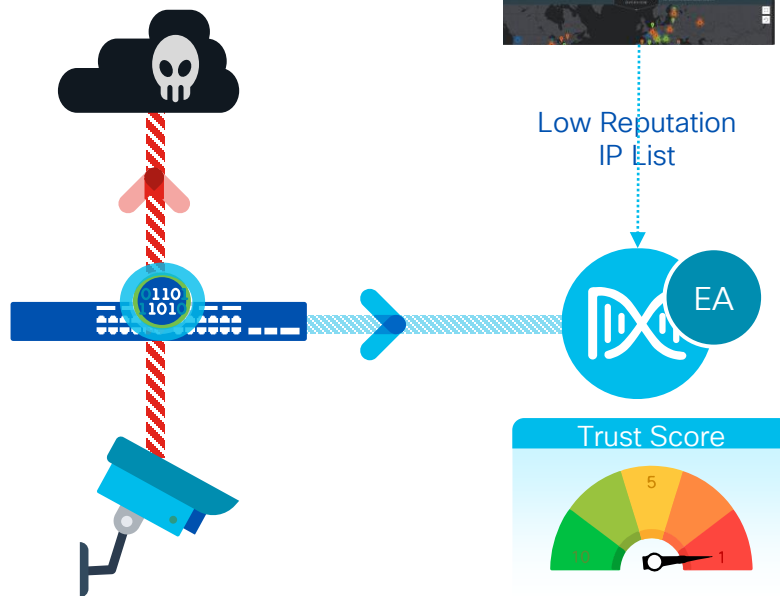
Considerations

- Catalyst 9K w/ IOS-XE: 17.7+
- NetFlow configuration
- DNAC 2.3.3

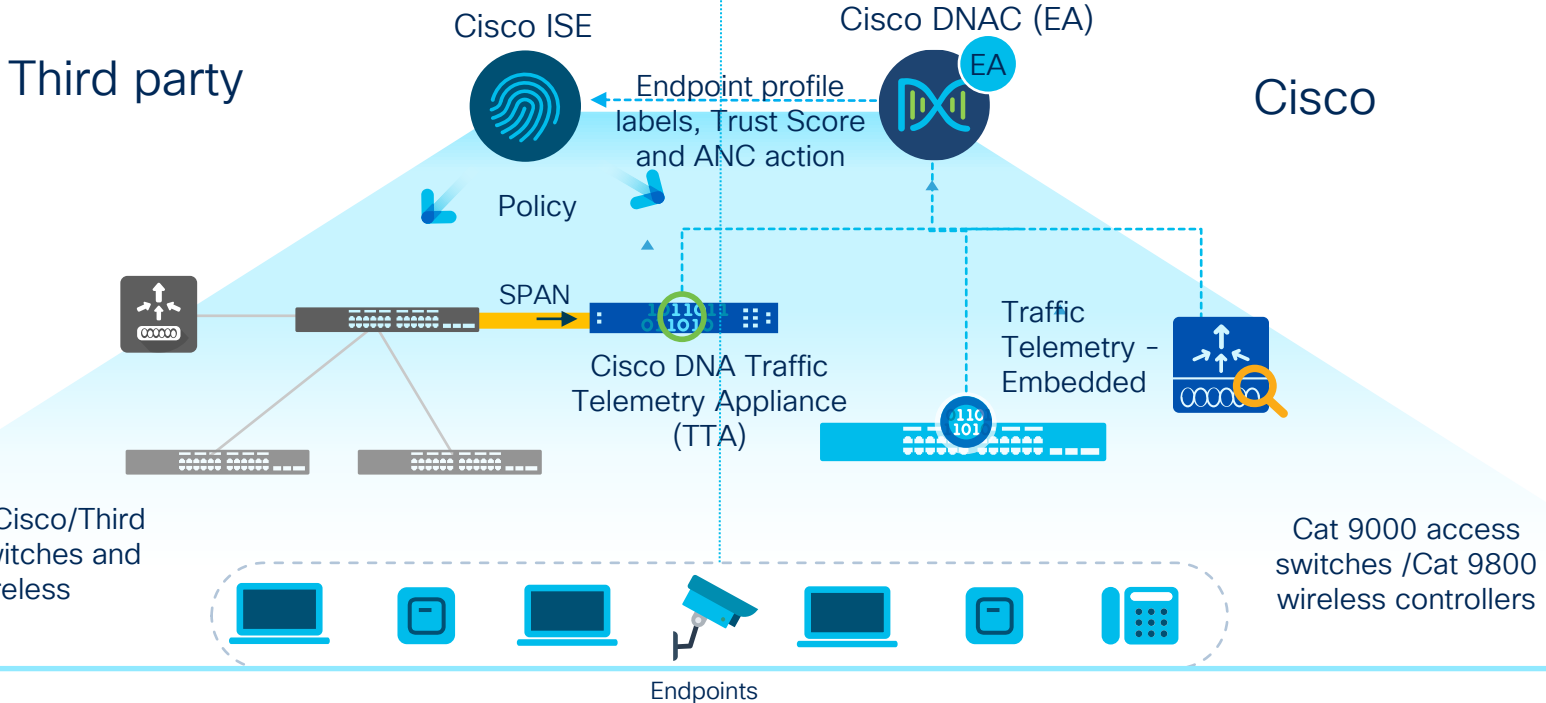
Note: Mitigation action for this vulnerability is with existing ISE integration using Adaptive Network Control APIs

Note: This requires Cisco DNAC to be registered in Cisco DNAC cloud.

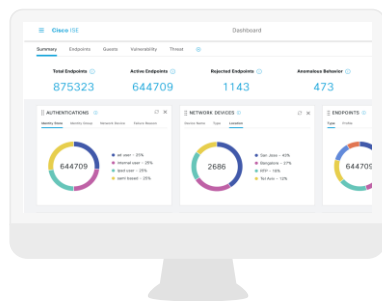
Internet Sites & locations
with low reputation



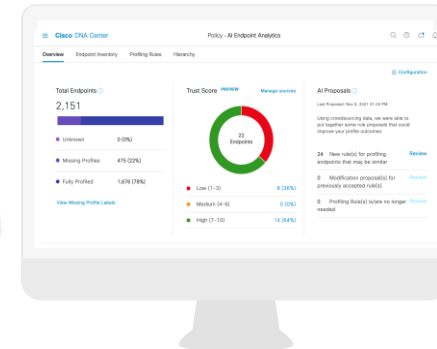
Supported Deployment Scenarios



Cisco DNAC TTA supports SPAN, RSPAN and ERSPAN



Cisco ISE



Cisco DNAC

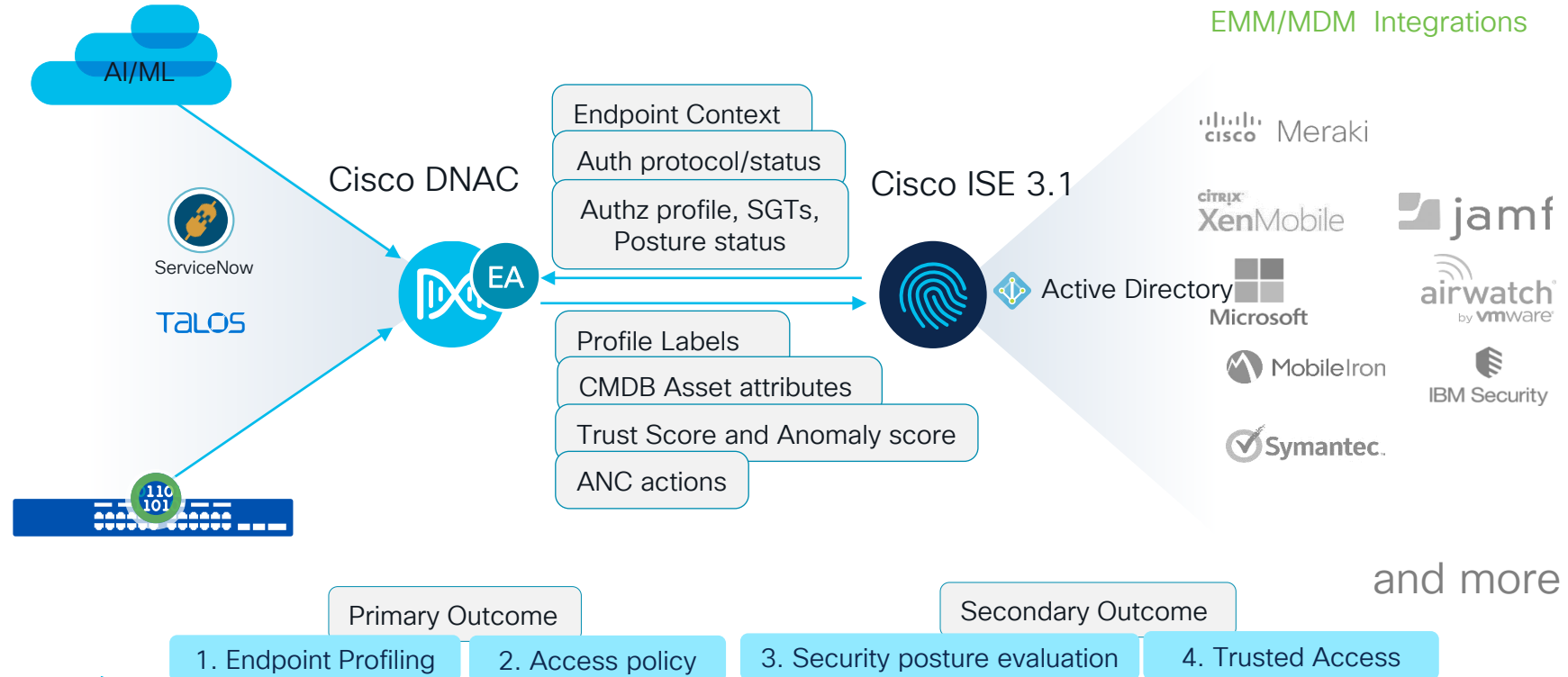


Admins



Users

Endpoint Analytics integrations and outcomes



Endpoint Analytics Compatibility Matrix

Capability	DNAC	Wired CAT9k		Wireless CAT9800 ⁴		Traffic Telemetry Appliance (TTA)
		Fabric	Non-Fabric	Local	Flex	
DPI Based Profiling	2.1.2.x	✓	✓	✓	✓	✓
AI Smart Grouping	2.1.2.x	✓	✓	✓	✓	✓
AI Spoofing Detection ²	2.2.2.x	✓	✓	✓	✓	✓
Changed profile labels	2.2.3.x	✓	✓	✓	✓	✓
NAT Detection	2.2.3.x	✓	✓	✓	✓	✓
Concurrent MAC Address	2.2.3.x	✓	✓	✓ ¹	✓ ¹	✗
Open Port Scan ³	2.3.2.x (CA)	✓	✓	✗	✗	✗
Weak Credential Scan ³	2.3.2.x (CA)	✓	✓	✗	✗	✗
Talos Low Reputation ² IP	2.3.3.x	✓	✓	✓	✓	✓

¹ - Concurrent MAC violations can not occur on wireless CAT9k Controller, but can detect concurrent MACs between wired and wireless.

² - AI Spoofing Detection and Talos low reputation needs netflow configuration, other functionalities need NBAR.

³ - Open port scan, weak credential scan needs security sensor (SDAVC app provisioned as container in Cat9k switch)

⁴ - Support for Fabric and Flexconnect from IOSXE 17.7+. Local mode supported in 17.6 for Enterprise SSID

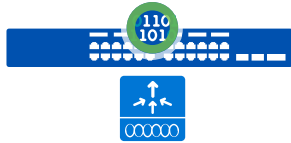
Minimum EA requirements for Endpoint visibility



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 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](#)

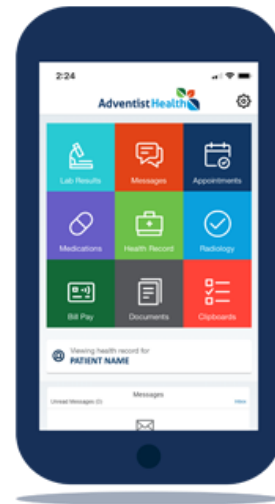
[Demo: AI Endpoint Analytics dCloud Demo](#)

[Deployment Guide: Cisco AI Endpoint Analytics](#)



[Cisco TTA Datasheet](#)

[Cisco SDA resources](#) [Cisco ISE resources](#)



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

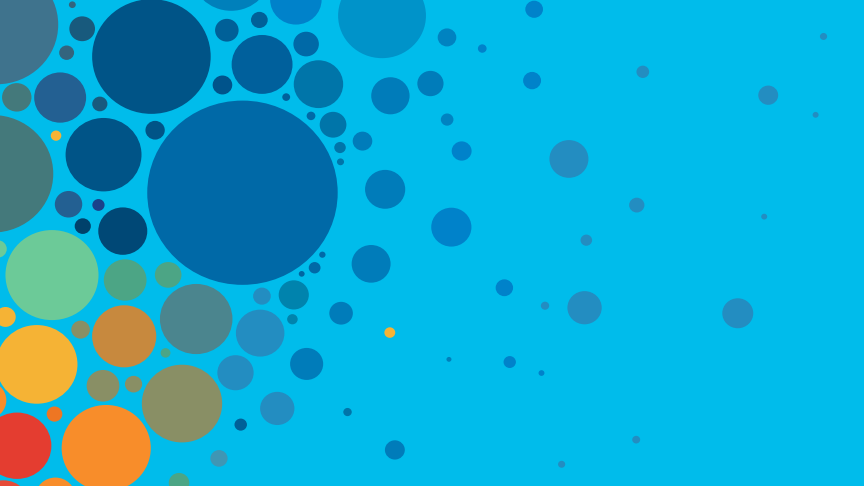
Cisco Guided Study Groups

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



The bridge to possible

Thank you

CISCO *Live!*



#CiscoLive