The bridge to possible

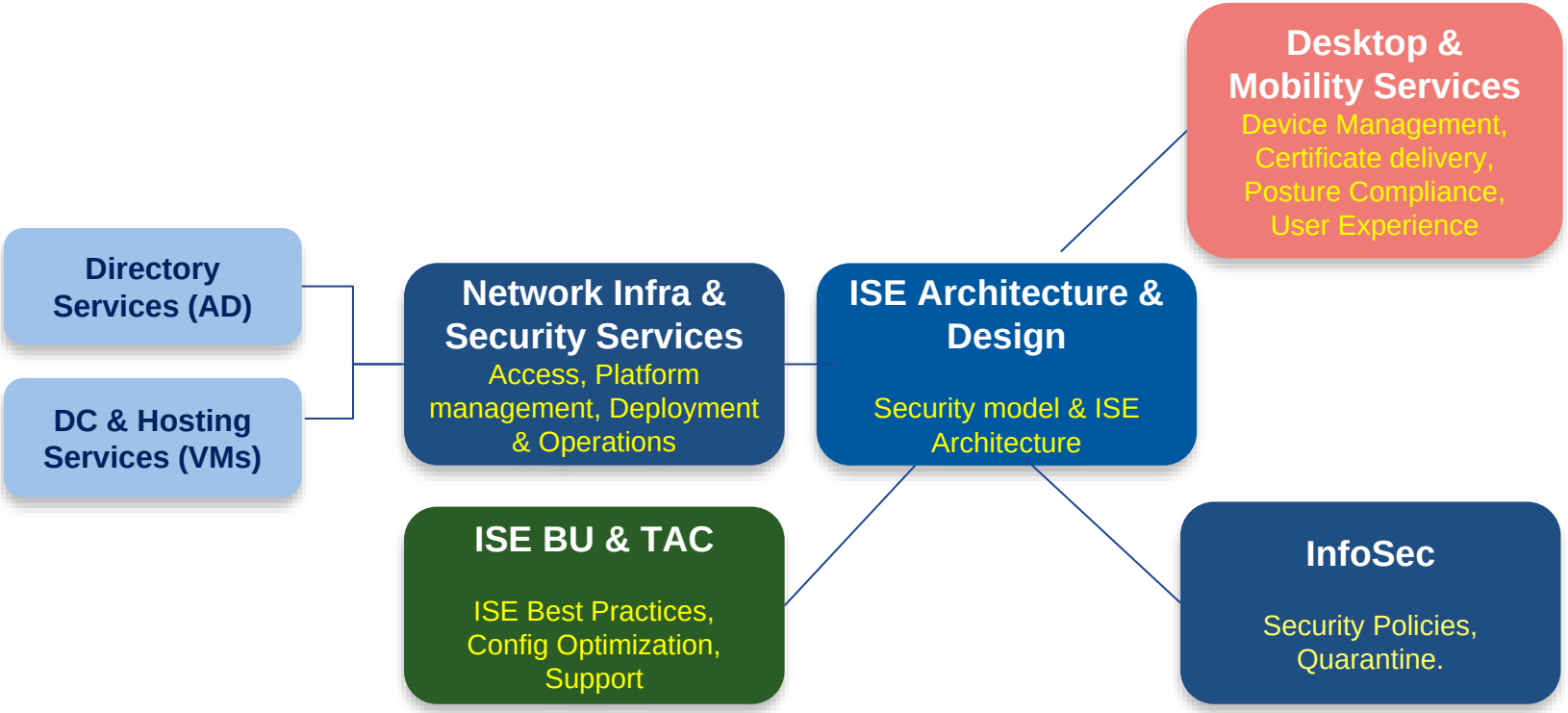
Inside Cisco IT: Zero Trust Workplace with TrustSec and Posture

Callum Corneille, Site Reliability Engineer
Maria Dede, Network Systems Engineer
Adam Cobbsky, Technical Systems Engineer

Agenda

- Cisco Enterprise Environment
- Users vs Devices
- Network Access Controls
  - VPN access controls
  - On-prem, internal network access (Wired & Wireless)
  - Simplifying the network-join experience
- TrustSec

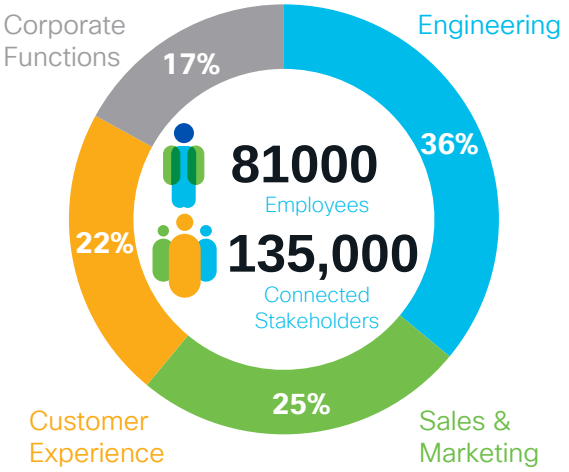
ISE Program Management Structure



Cisco Enterprise Environment

cisco Live!

Cisco Enterprise at a Glance

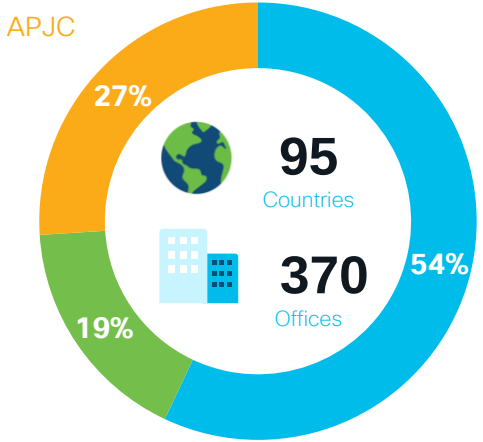


2,483
Routers

7,194
LAN Switches

12,553
Unified Computing System Servers

19.5
Billion DNS requests per day



22,438
TelePresence Units

59,686
Virtual Machines

~527k
Managed End Devices

187 PB
Overall Usable Storage

1.5 M
Webex Meetings per Month

6.25M
Internet Threats Blocked Per Day

Data as of June 2022

Cisco IT ISE Production Deployment Metrics 2022

ISE 3.1, 10 VMs, 2 DCs

Guests/Employee BYOD

CWA

Central Web Auth

Guest Net (Internet)

278 WLC

802.1x

8-9K CVO

802.1x

62 ASA

802.1x

1774 SW

SGT

75 Sites

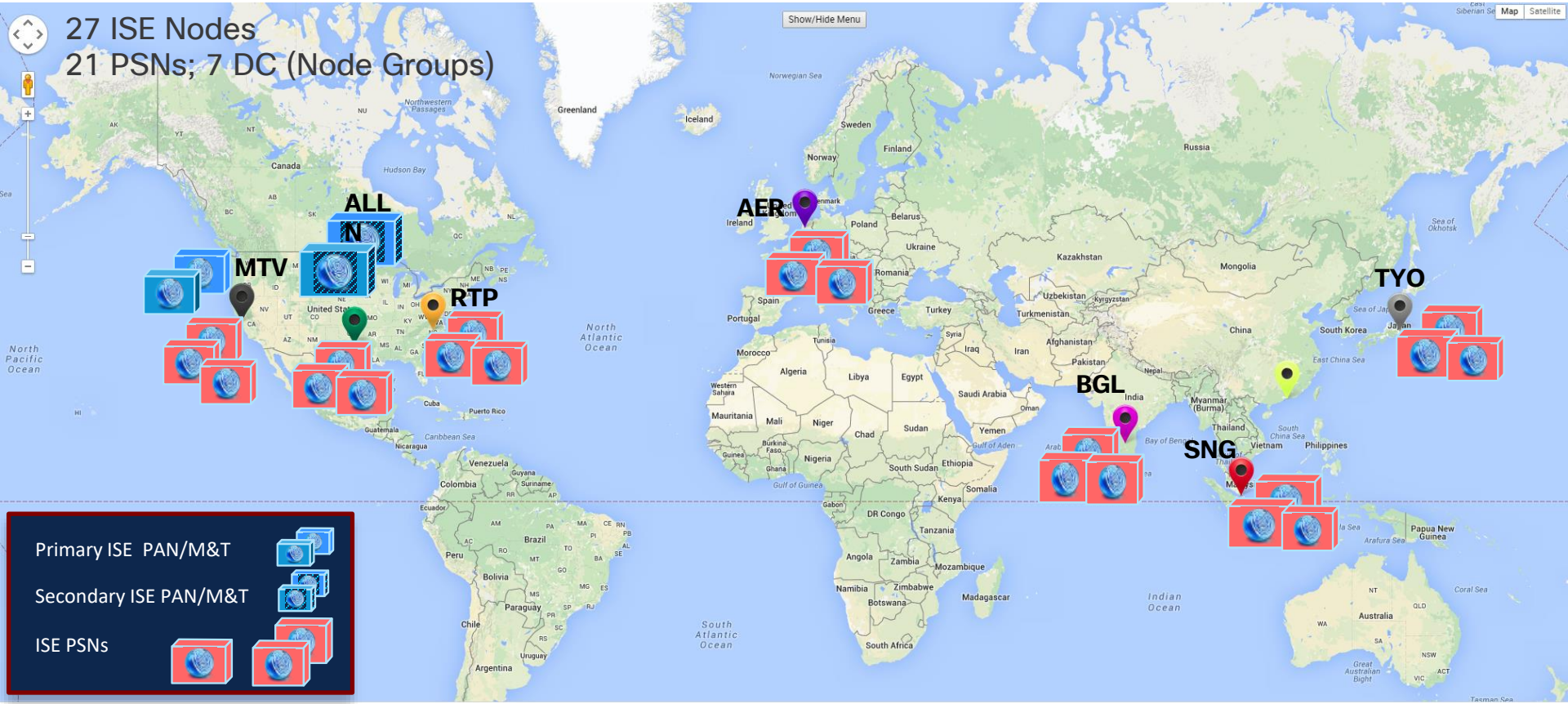
Corporate Access

WLAN, CVO, VPN, LAN

ISE 3.1, 27 VMs, 7 DCs

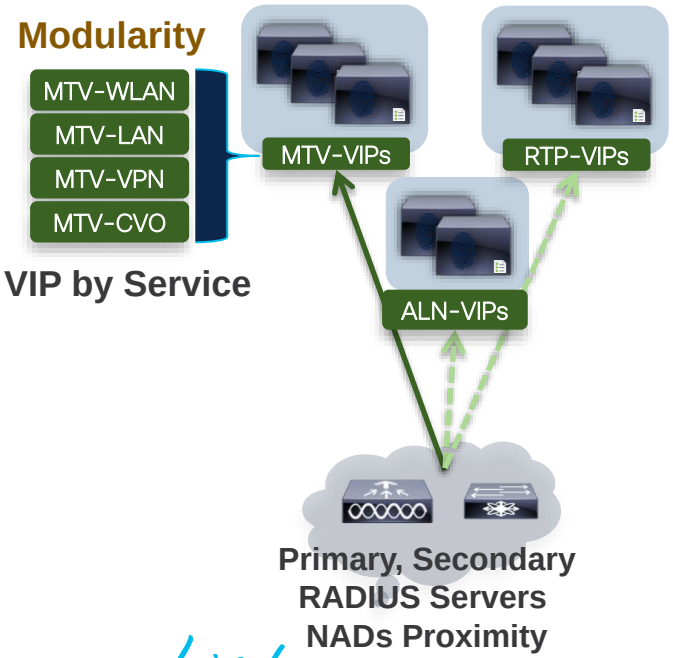
1.36 Million profiled "Endpoints"

Global ISE Deployment

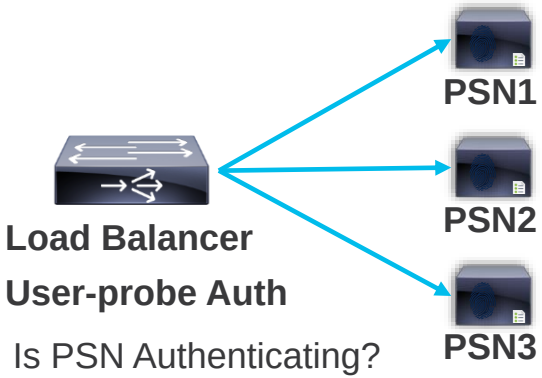


ISE Deployment High Availability Architecture

HA NAD Configuration



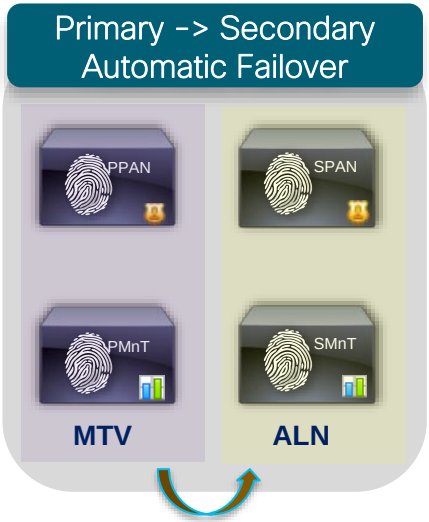
HA SLB Configuration



Is PSN Authenticating?

- Interval = 10 sec
- Down Time = 30 sec
- Retries = 3

ISE Product Evolution



Guest Access (Internet)

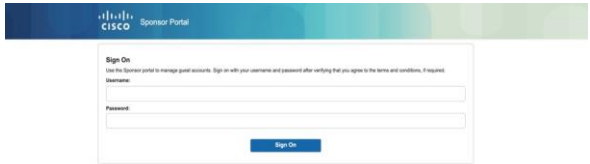
Registration via Visitor Management System (VMS)

VMS creates Guest Account using API

Guest Credentials printed on Visitor Badge

ISE

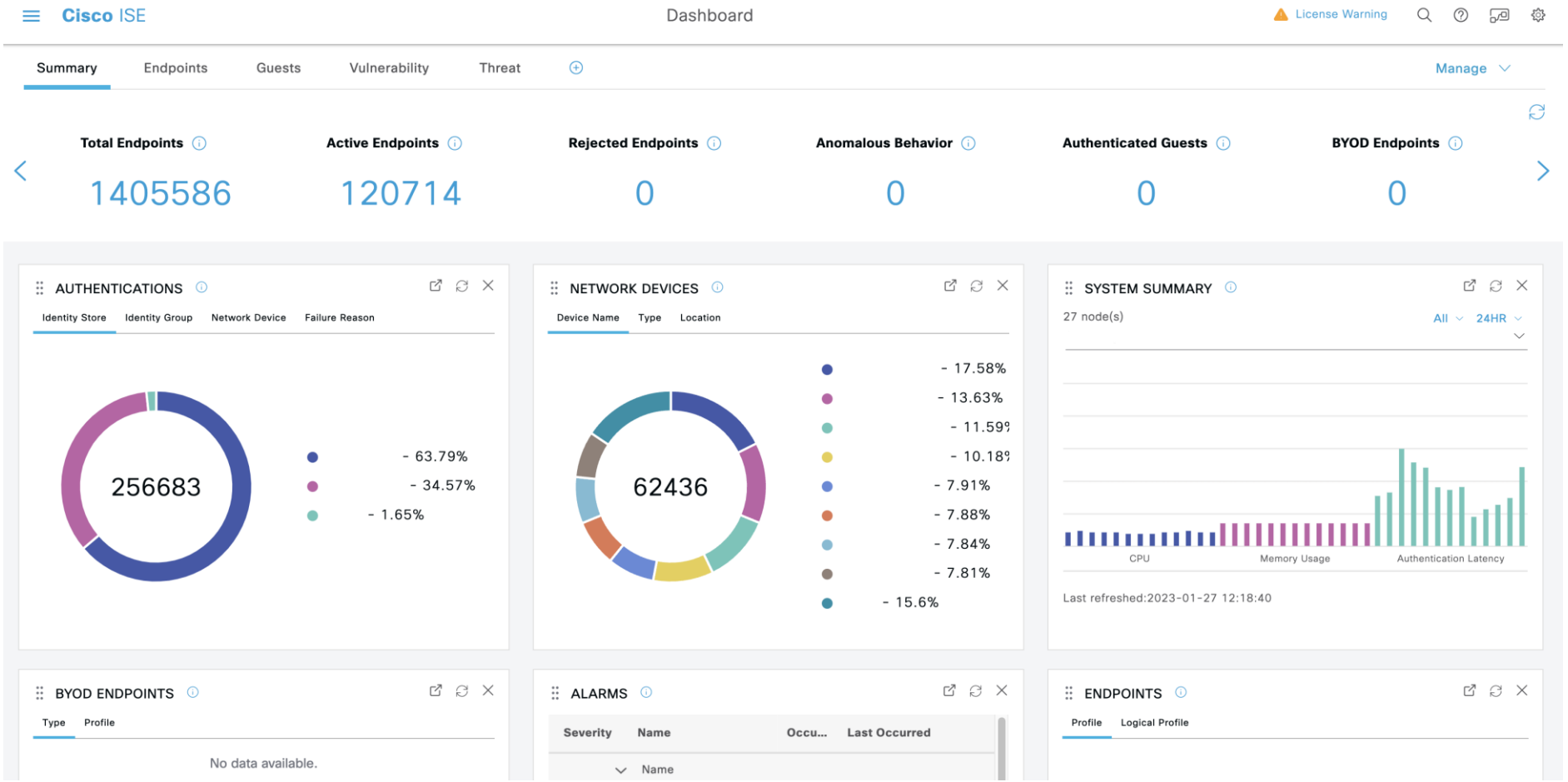
Employee Sponsored Access



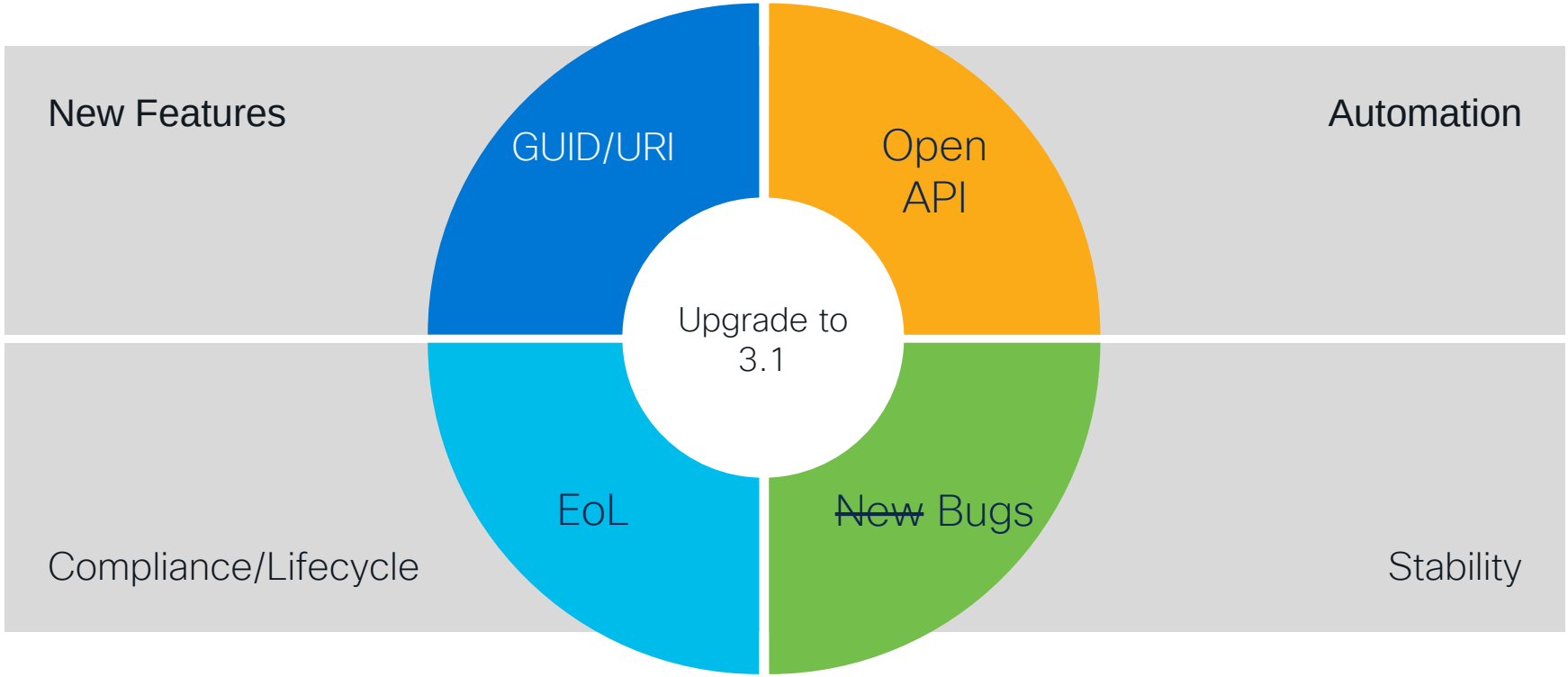
ISE hosted Sponsor Portal

ISE

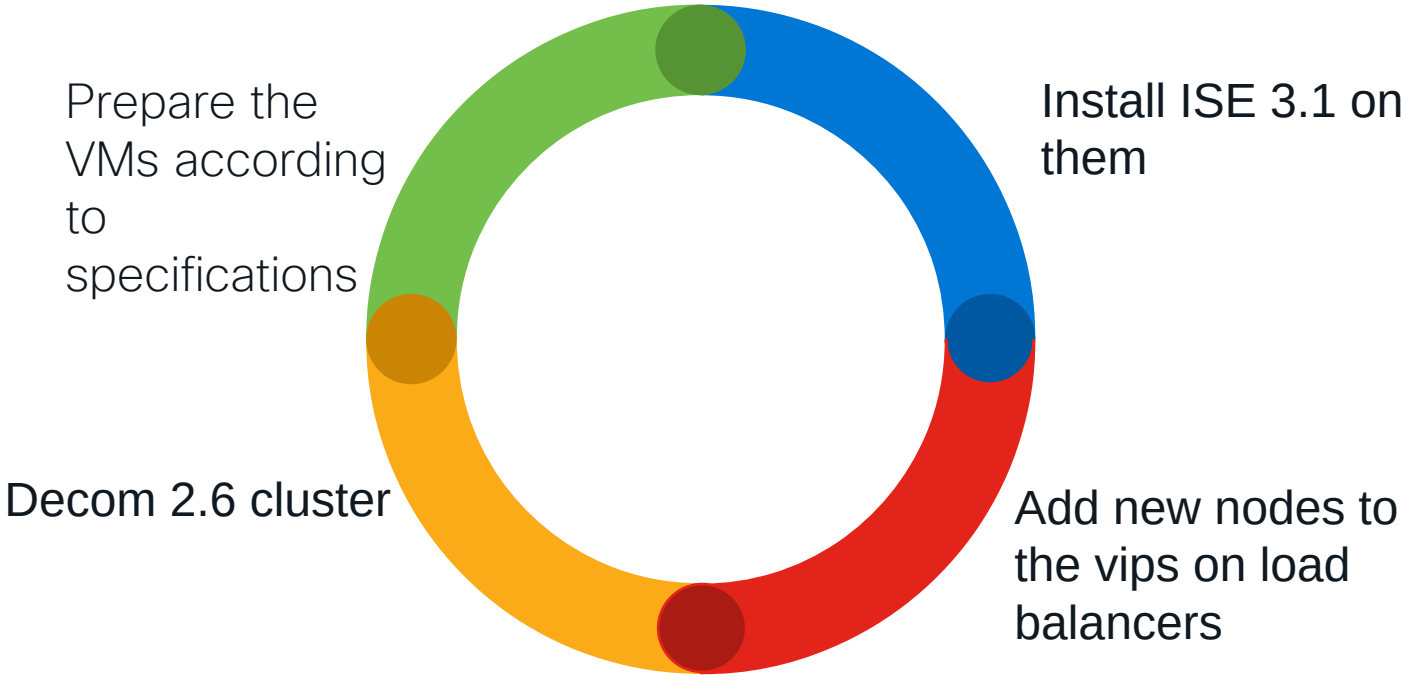
Employees have differentiated privileges to create Guest Accounts based on Active Directory attributes.
For example, guest accounts longer than 3 months requires manager approval.
Create guest accounts in bulk.



Is it worth the pain?



This is how we avoid the pain



Users vs Devices
Authentication & Authorization

Authentication (AuthC) & Authorization (AuthZ)

Authentication - “The Process of Verifying the User”

examples:

Authentication: dot1x / EAP-TLS Certificate based / Duo MFA / MAB

Access: VPN, Wireless, Wired

Data source: Active Directory, Duo

Authorization - “The Process of Verifying what you have access to”

examples:

Authorization policies: Differentiated Network Access based on Device Posture, Quarantine

Agents: AnyConnect Posture Module, Duo Health Agent (DHA)

Data source: Barcode, Secure X, Active Directory

Enforcement: ACLs, Trustsec, Blacklist

Authentication

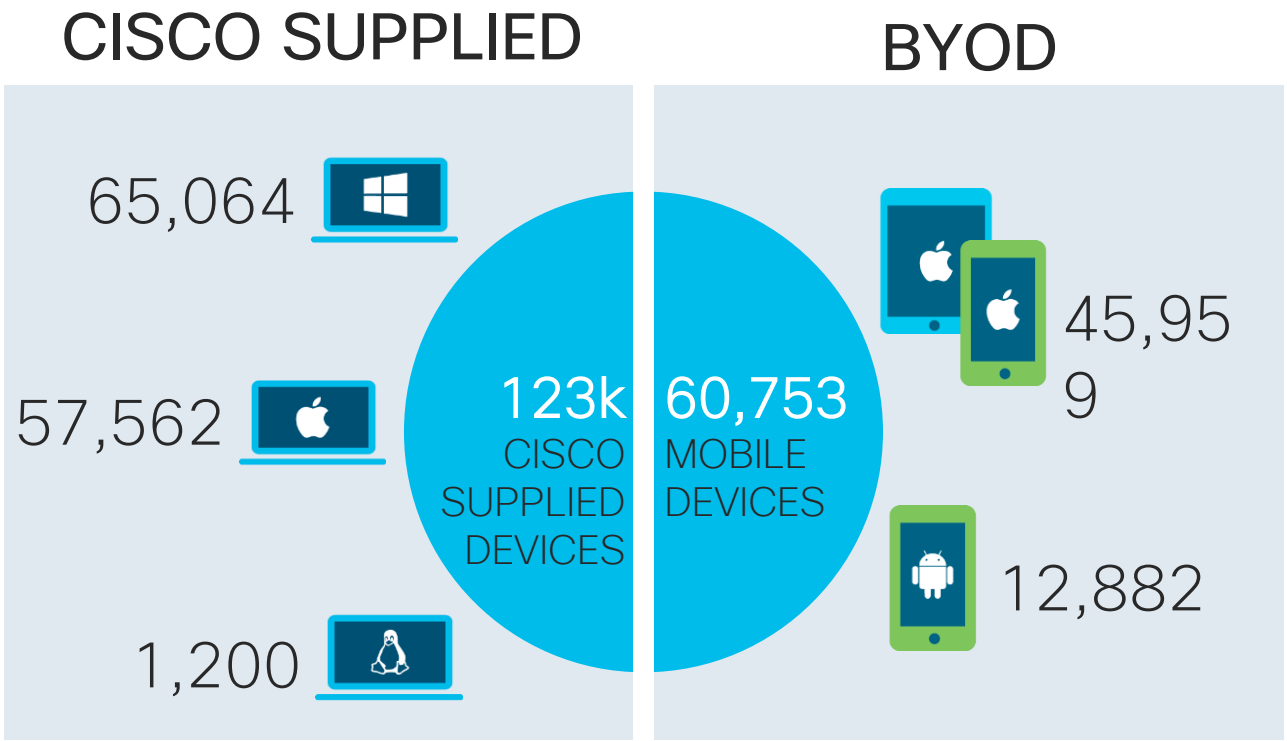
Dot1x enabled globally

Certificate (EAP/TLS)

Username & Password (PEAP)

Exception / MAB

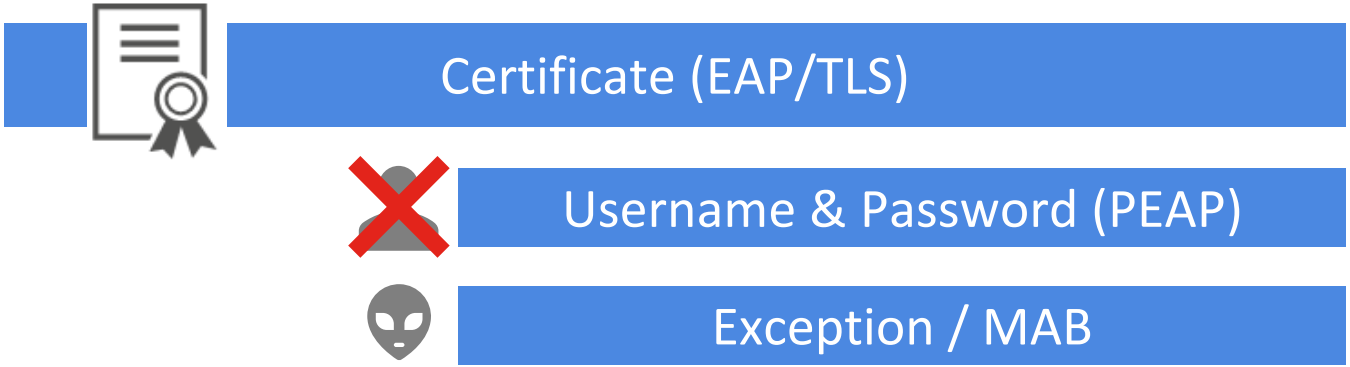
Cisco IT End User Device Landscape



Network Access Controls

Certificate based authentication

Passwordless Authentication



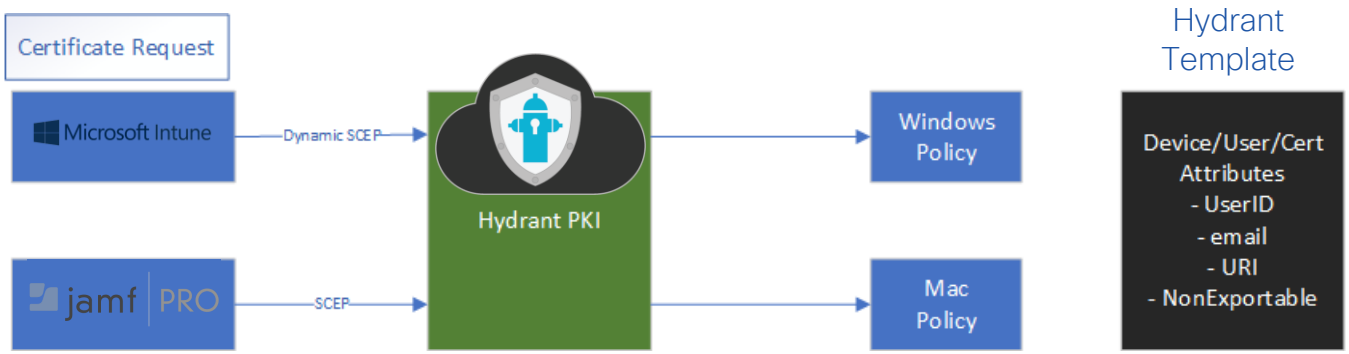
Certificate deployment with Device Management

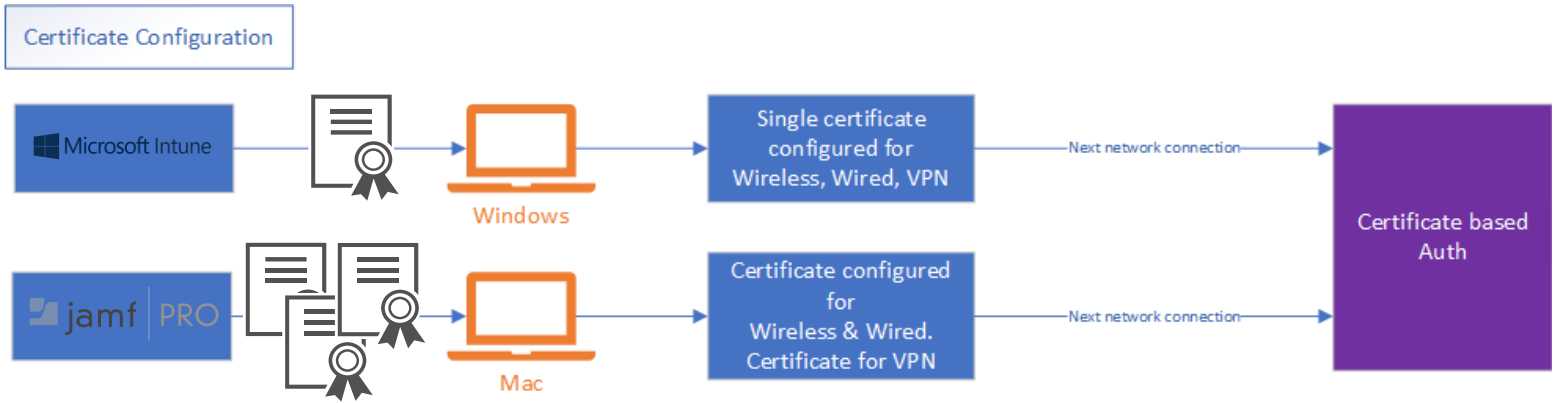
cisco Meraki

jamf | PRO

Microsoft Intune

Certificate request & delivery





Lessons Learnt

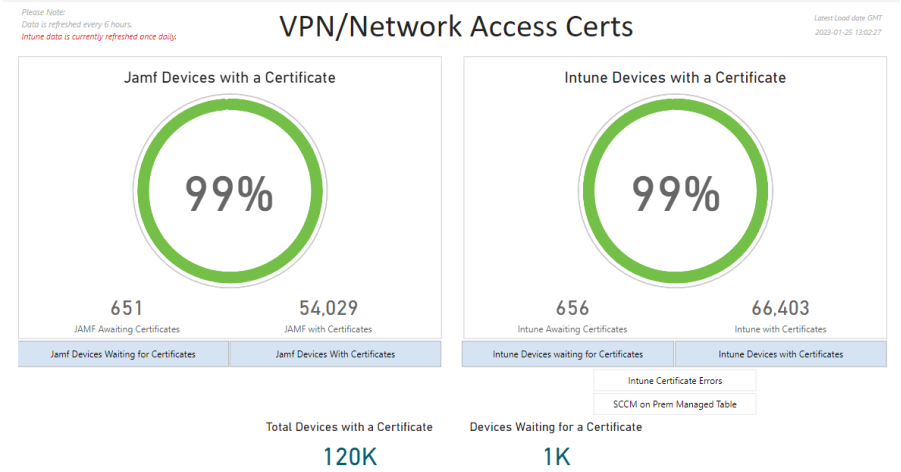
Cloud MDM

cisco Meraki

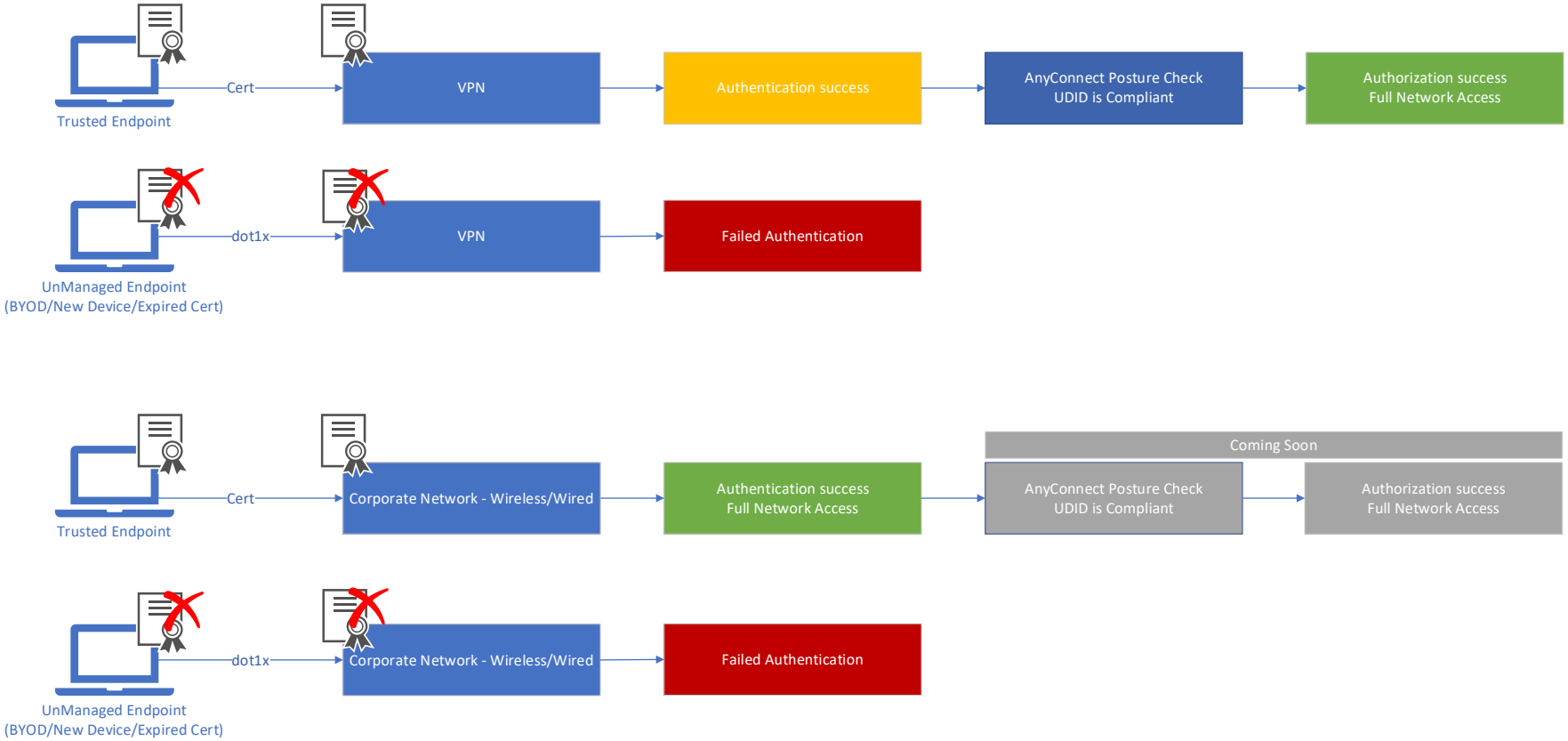
jamf PRO

Microsoft Intune

Data driven decisions

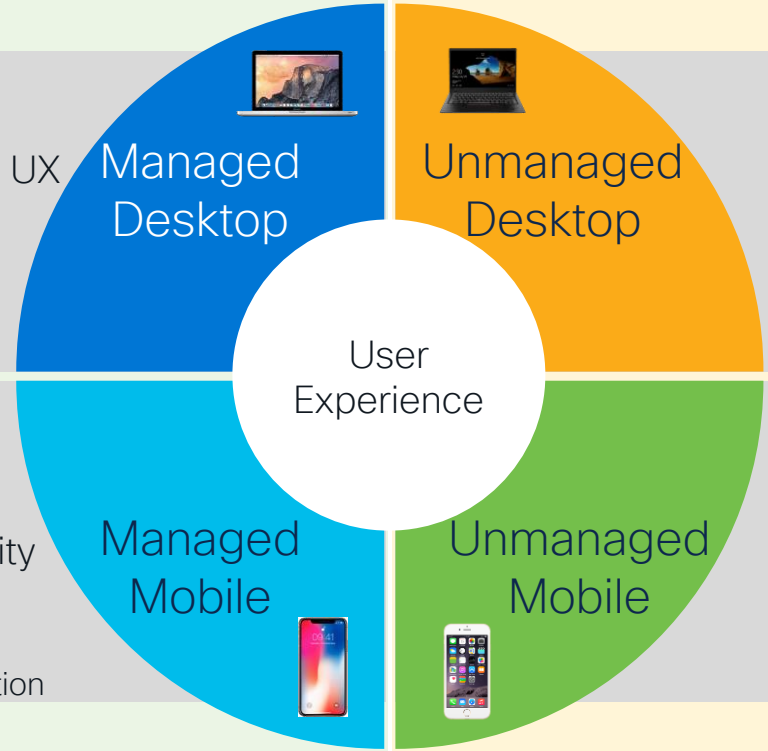


Certificate based Authentication User Experience



The User Experience

Improved UX VPN



Improved passwordless UX
One Click VPN access

Home Internet access

Enroll in management for VPN access

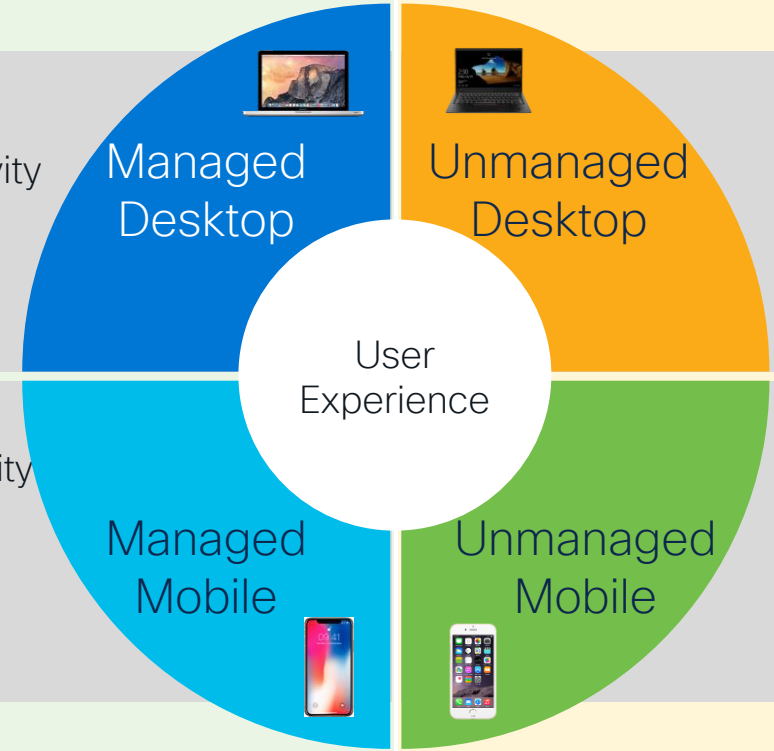
No change in connectivity & access

Cert-based VPN authentication

Home Internet access

Enroll in management for full access

New UX Corporate Network (Wired/Wireless)



No change in connectivity & access

Internet only available

Enroll in management for full access

May need to login every day

No change in connectivity & access

(Automatic connection to Corporate WiFi

Internet only available.

Enroll in management for full access

May need to login every day

Expected UX: On-prem Wired/Wireless – Corporate Network

Corporate SSID

Cert presented

Success: Full network access

Certificate expired or No Certificate

Fail to Connect to Corporate SSID

Internet SSID

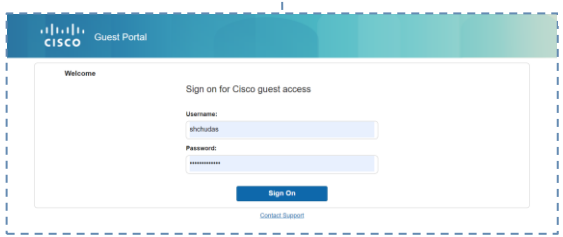
Captive Portal

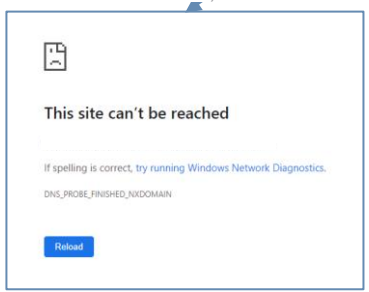
User creds required

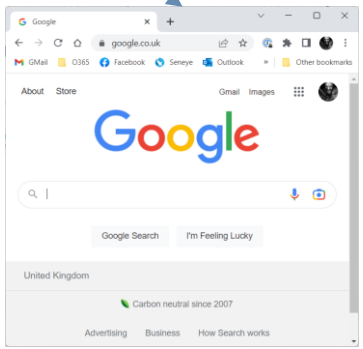
Internet only access

Internal page (if device is not ZT enabled)

Internet







Expected UX: CVO

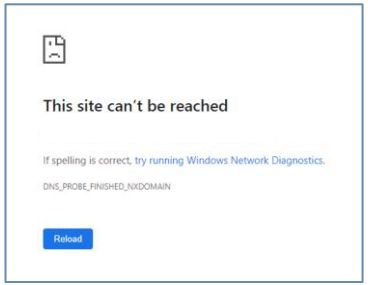
Corporate CVO SSID

Cert presented → Success: Full network access

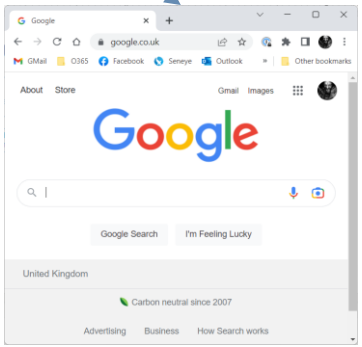
Certificate expired or No Certificate → Fail to Connect to CVO SSID

Home Internet → Internet only access
(New builds, remediation, BYOD, ZT)

Internal page (if device is not ZT enabled)



Internet



Network Access Controls

Posture Based Authorization

Authorization

Only allow “trusted devices”
on the Cisco Corporate Network

VPN – Wireless – Wired

What is a Trusted Device?

1. Device Registration
2. Anti-Malware
3. Encryption (Cisco Data)
4. Minimum OS
5. Software Patching
6. Remote Wipe (Cisco Data)
7. Password/Screen-lock Enforcement
8. Hardware/Software Inventory
9. Rooted Device Detection (Mobile Only)

Trusted Device with Device Management

cisco Meraki

jamf | PRO

Microsoft Intune

What is Posture?

Posture

Security configuration of the device

Assessment

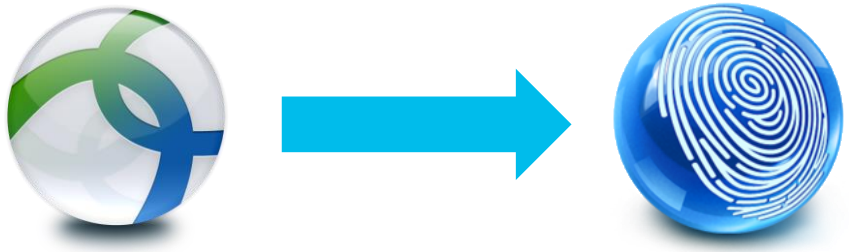
Measure and check against Company requirements

Device Manager

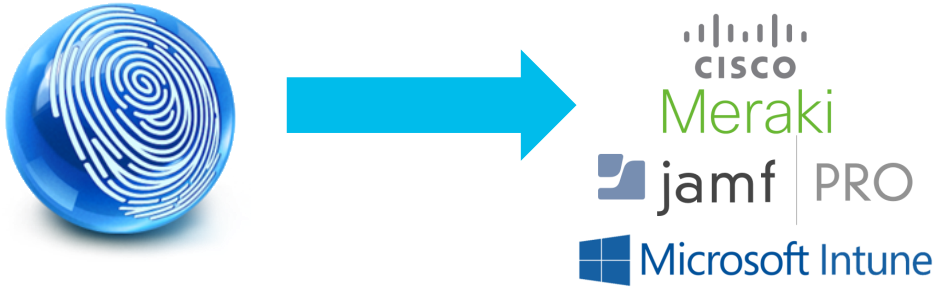
Access Policy

Posture with ISE & AnyConnect

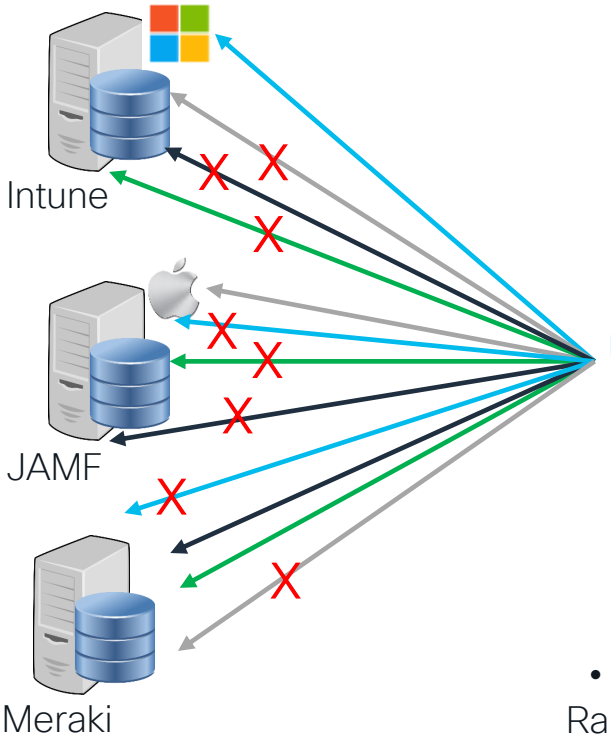
ISE & AnyConnect – Posture Conditions



ISE & AnyConnect – Device Management Integration



Uncertain Identities



Needs to know:
- What device?
  Profiling challenges
- Which DM suite?
  Random mac challenges

- Wired MAC Address
- Wireless MAC Address
- Docking station MAC Address
- Random MAC Address
- VM Shared MAC Address

- Thunderbolt MAC
- Spoofed MAC Address
- **Windows VM**

- Android Device

- Apple Device
- iPhone
- iPad

Desktop Posture with UDID & ISE External Datasource Condition

- Wired MAC Address
- Wireless MAC Address
- Docking station MAC Address
- Random MAC Address

UDID consistent

- VM Shared MAC Address

Separate UDID

- Thunderbolt MAC
- Spoofed MAC Address

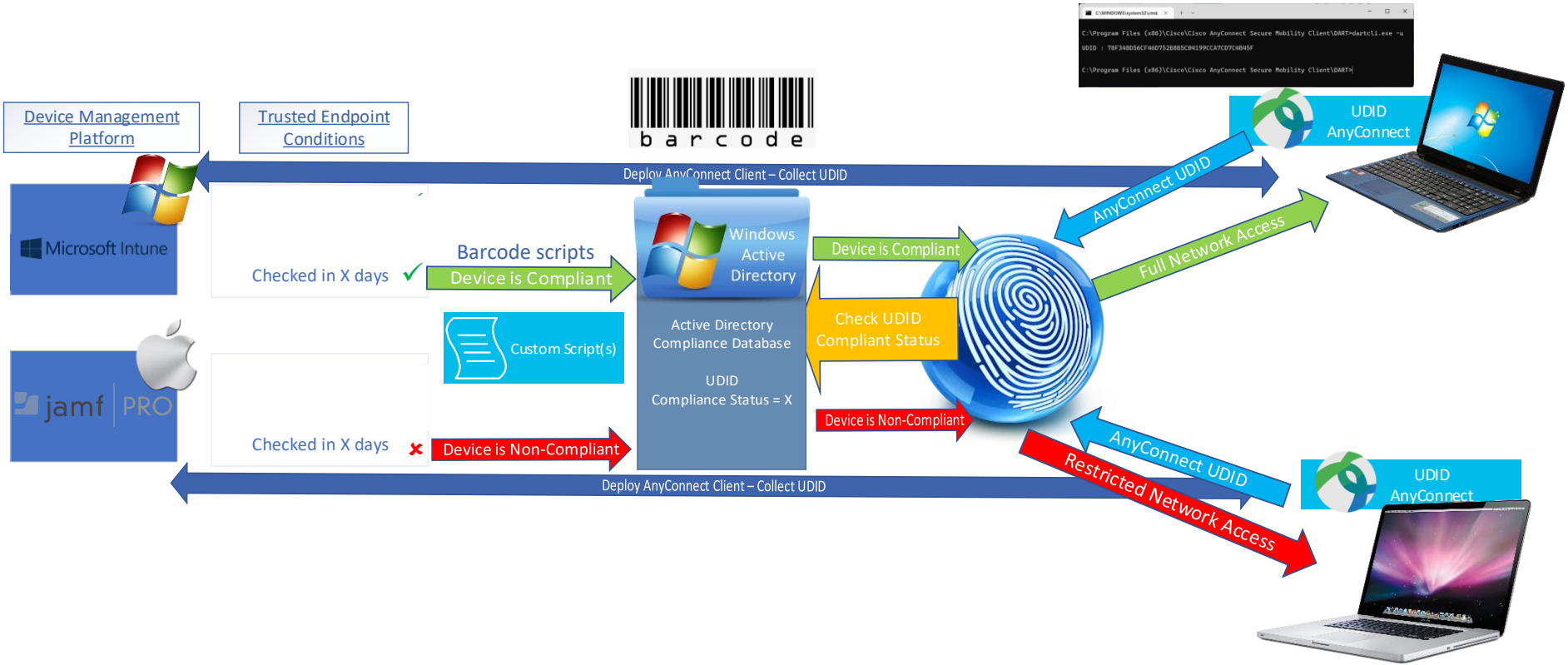
UDID consistent

- Windows VM

Separate UDID

Desktop Posture VPN/Wireless/Wired

ISE External Datasource Condition & AnyConnect Posture Module



Network Access Controls

The Future

ISE and Device Management Integration (2023)
Cert based Authentication and URI in certificates

TrustSec

Cisco TrustSec? A Quick Refresher..

The Three Pillars of TrustSec

Classification

- User or device connects
- Assignment of specific Scalable Group Tag (SGT)

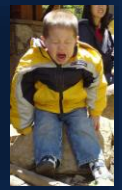
Propagation

- SGT must be propagated from where classification took place
- Inline Tagging or SXP

Enforcement

- Propagation leads to where enforcement action is invoked
- Determination of an allow or deny

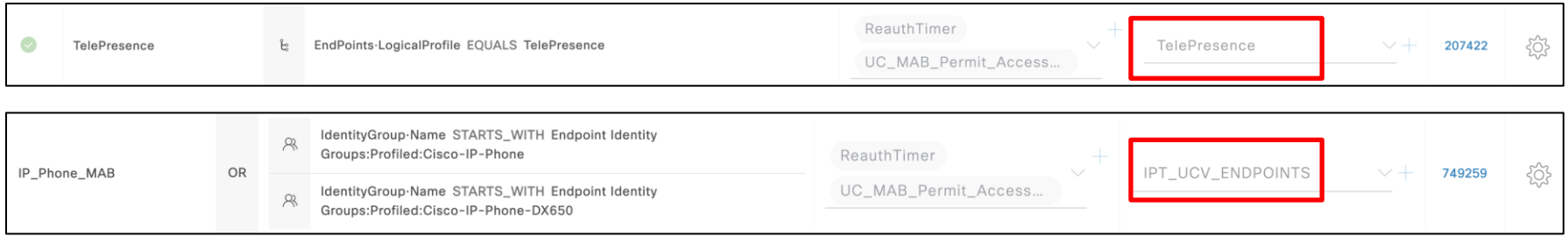
The Theme Park Analogy



DENIED PERMITTED

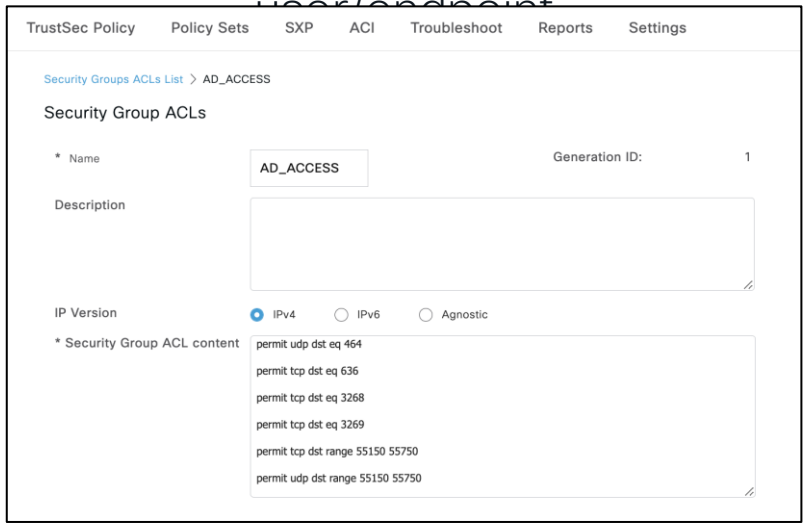
So, what's an SGT?

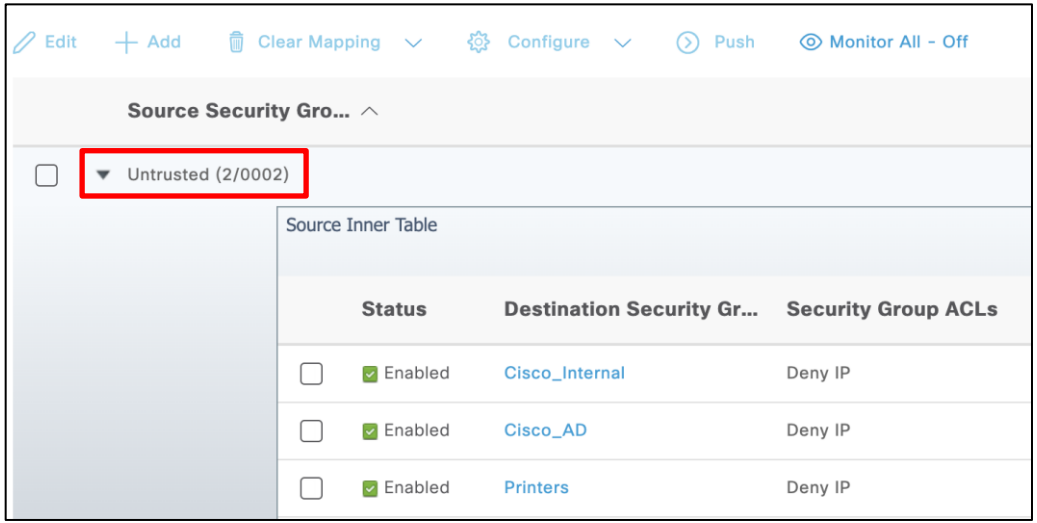
1. A Scalable Group Tag (SGT) is a 16-bit value Cisco ISE assigns to the user or endpoint upon login (Classification stage)
2. Upon the propagation of said SGT (Inline or SXP) – decisions for enforcement can be made at destination based off of the Source SGT/IP
3. Inline Tagging allows for packets send/received to have the SGT embedded (carried via the CMD header) under EtherType 0x8909



And what's an SGACL?

1. Security Group Access Control Lists (SGACLs) allow control over the operations a user can perform, whilst also stripping the requirement for IP addressing
2. SGACLs are defined within ISE / associated to SGTs resulting in agnostic 'role-based permissions' based upon the SGT assigned to a user/endpoint





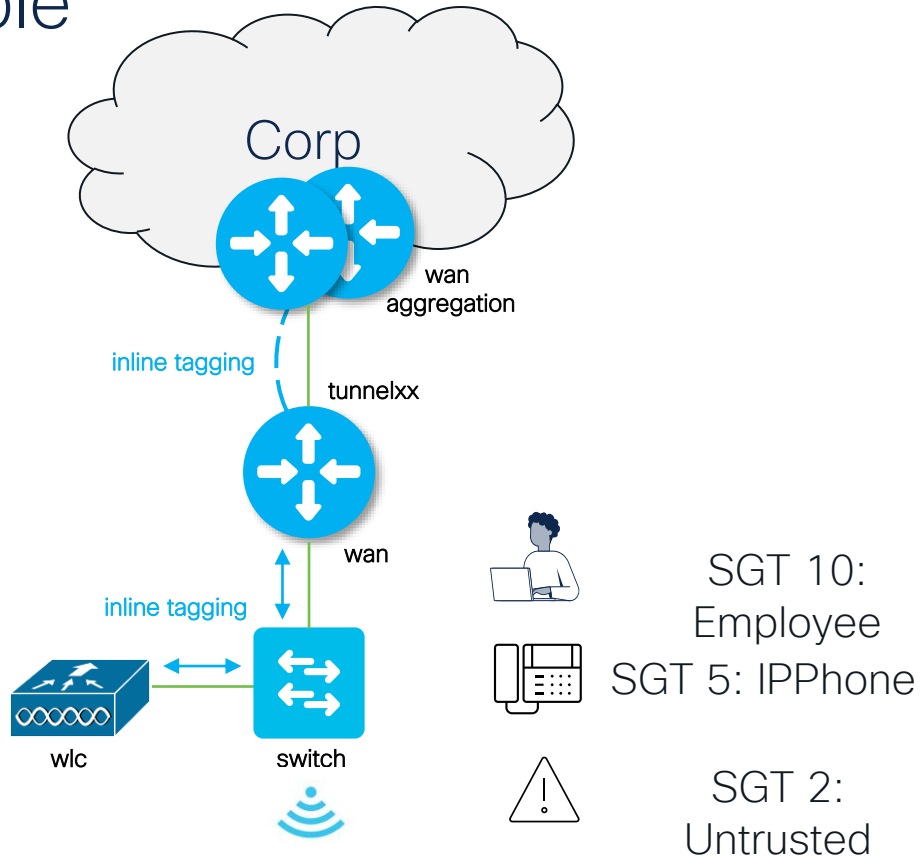
Our Small Office Example

Device-sw1 #show cts role-based sgt-map all
Active IPv4-SGT Bindings Information

IP Address	SGT	Source
10.2.32.0/22	3193	SXP
10.16.0.0/12	3000	SXP
10.22.27.17	3123	SXP
10.22.31.64	3123	SXP
10.22.31.65	3123	SXP
10.28.21.224/27	3026	SXP
10.28.24.0/21	3026	SXP
10.28.25.43	3014	SXP
10.10.10.1	2	LOCAL
10.10.10.2	5	LOCAL
10.10.10.3	5	LOCAL
10.10.10.4	5	LOCAL
10.10.10.5	17	LOCAL
10.10.10.6	17	LOCAL
10.10.10.7	10	LOCAL
10.10.10.8	10	LOCAL
10.10.10.9	10	LOCAL
10.10.10.10	10	LOCAL
10.10.10.11	10	LOCAL

SXP IP-SGT mappings

Local Site Mappings present / sent



Production Example of TrustSec

User Access Session (Classified via ISE)

```
Device-xxx# show access-session interface gig1/0/4 det

Interface:  GigabitEthernet1/0/4
MAC Address:  xxxx.xxxx.xxxx
IPv4 Address:  xx.xx.xx.xx
User-Name:  xxxxxx
Status:  Authorized
...
<output omitted>
...
Server Policies:
ACS ACL: xACSACLx-IP-PERMIT_ALL_TRAFFIC
SGT Value:  10

Method status list:
Method          State
dot1x           Authc Success
mab             Stopped
```

Role-Based Permissions

```
Device-xxx# show cts role-based permissions

IPv4 Role-based permissions from group 2:Untrusted to group
10:Employee: Deny IP-00

IPv4 Role-based permissions from group 5016:Quarantine to
group 10:Employee: Deny IP-00

IPv4 Role-based permissions from group 2:Untrusted to group
3:Trusted: Deny IP-00

IPv4 Role-based permissions from group 5016:Quarantine to
group 3:Trusted: Deny IP-00

IPv4 Role-based permissions from group 2:Untrusted to group
4:CTS_Device: Deny IP-00

IPv4 Role-based permissions from group 20:Camera to group
15:Video_Recorder: TCP_9000 Deny IP-00
```

Shameless Plug – Inside Cisco IT Presentations

Date	Start	End	Duration	Session Title	Speaker	Technology	Session ID
Tuesday, February 7th	8:45	9:45	1:00	Hybrid Workplace - The Future of Work	Ifeoma Nembhardt	Collaboration, Webex	BRKCOC-2738
Tuesday, February 7th	15:00	16:30	1:30	Inside Cisco IT: Powering the Next Generation Hybrid Workspace with SASE	Roel Bernaerts	SD-WAN, SASE	BRKCOC-2014
Tuesday, February 7th	17:00	18:30	1:30	Inside Cisco IT: Zero Trust Workplace with Trustsec and Posture	Adam Cobbsky Callum Corneille Maria Dede	Security, Switching	BRKCOC-2778
Wednesday, February 8th	8:45	10:15	1:30	Cisco Zero Trust: Device-Focused Deep-Dive	Laurent Sellin Shyam Chudasama Sukhbir Singh	Security, Hybrid Work	BRKCOC-2620
Wednesday, February 8th	13:30	14:30	1:00	Deploying Smart Building Technologies to Enable the Office of the Future	John Moe Ifeoma Nembhardt	Internet of Things (IoT), Switching	BRKCOC-1014
Wednesday, February 8th	14:45	16:15	1:30	Inside Cisco IT - Cisco DNA Center and Automation Value Cases	Callum Corneille Jamie Mcgregor	Network Management, Automation & Orchestration, Cisco DNA Center, Wifi 6	BRKCOC-2465
Thursday, February 9th	8:45	10:15	1:30	Cisco IT: How We Developed the Hybrid Worker Network Solution for Cisco Employees	David Laban Dipesh Patel	Meraki, ThousandEyes, Hybrid Work	BRKCOC-2120
Thursday, February 9th	14:30	15:30	1:00	Lessons Learnt from Cisco IT's Wifi 6E Deployment	Dean Sanders Marianna Pittokopiti	Wifi 6	BRKCOC-2526
Thursday, February 9th	16:00	17:00	1:00	Inside Cisco IT: Enhancing Day 2 Ops in the Data Center Network	John Banner	Data Center	BRKCOC-2030
Friday, February 10th	9:00	10:30	1:30	Redefining Network Assurance, Challenging the Hybrid World with ThousandEyes	Tom Fincher Marianna Pittokopiti	ThousandEyes, Operations	BRKCOC-2545

Cisco Webex App

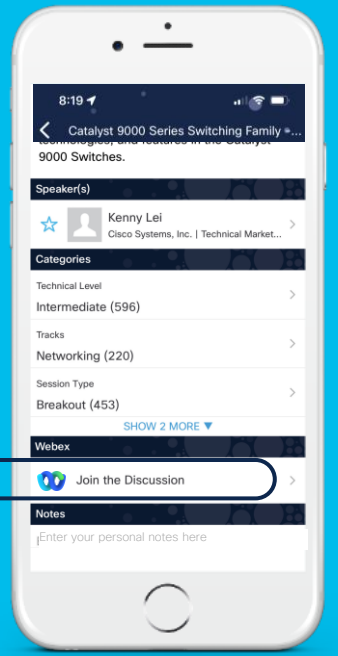
Questions?

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 until February 24, 2023.



Complete your Session Survey

- Please complete your session survey after each session. Your feedback is very important.
- Complete a minimum of 4 session surveys and the Overall Conference survey (open from Thursday) to receive your Cisco Live t-shirt.

- All surveys can be taken in the Cisco Events Mobile App or by logging in to the Session Catalog and clicking the "Attendee Dashboard" at https://www.ciscolive.com/emea/learn/sessions/session-catalog.html

Continue Your Education

Visit the Cisco Showcase for related demos.

Book your one-on-one Meet the Engineer meeting.

Attend any of the related sessions at the DevNet, Capture the Flag, and Walk-in Labs zones.

Visit the On-Demand Library for more sessions at ciscolive.com/on-demand.


cisco
The bridge to possible
Thank you
cisco Live!


CISCO Live!
ALL IN