Les fondamentaux du Contrôle d'Accès

R&S et Sécurité

Christophe Sarrazin, Technical Solution Architect Cybersecurity

Mardi 7 Mars 2023

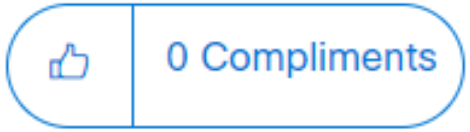
Connectez, Engagez, Collaborez !

Solutions

Acceptez les solutions qui sont correctes et complimentez ceux qui vous ont aidé ! Aidez autres utilisateurs à trouver les réponses correctes dans la fenêtre de recherche.

Compliments

Mettez en évidence les autres membres. Les votes utiles motivent les membres enthousiastes en leur offrant un signe de reconnaissance !



Spotlight Awards

De nouveaux lauréats tous les mois !

Démarquez-vous par vos efforts et votre engagement à améliorer la communauté et à aider les autres membres. Les Spotlight Awards sont distribués chaque mois pour mettre en valeur les membres les plus remarquables.

Maintenant vous pouvez aussi désigner un candidat ! Cliquez ici

Community Spotlight awards

Christophe SARRAZIN

Technical Solution Architect Cybersecurity

Présent chez Cisco depuis début 2000, il a débuté sa carrière comme avant-vente réseau chez Alcatel puis Bay Network/Nortel Network.

Christophe Sarrazin occupe aujourd'hui un poste d'Architecte en Cybersécurité chez Cisco et à ce titre il est titulaire du CCIE Security depuis 2005.

La sécurité est un domaine transversal aux autres technologies, l'expérience acquise entre le networking et la sécurité font de lui un de nos meilleurs spécialistes du NAC avec une expérience de plus de 20 ans sur les déploiements 802.1x

Télécharger la présentation

https://bit.ly/WEBsld-mar23

Les fondamentaux du Contrôle d'Accès

Christophe Sarrazin

Technical Solution Architect Cybersecurity

7 Mars 2023

Agenda

- Introduction to NAC & 802.1x
- Authentication
- Authorization
- Guest Access
- Profiling
- Posture
- Threat centric NAC with Third party integration

NAC End to End solution

Enterprise

Security

Endpoints

- Users
- Devices
- Things

Network Devices

- Switches
- WLCs / APs
- VPN

Radius Server

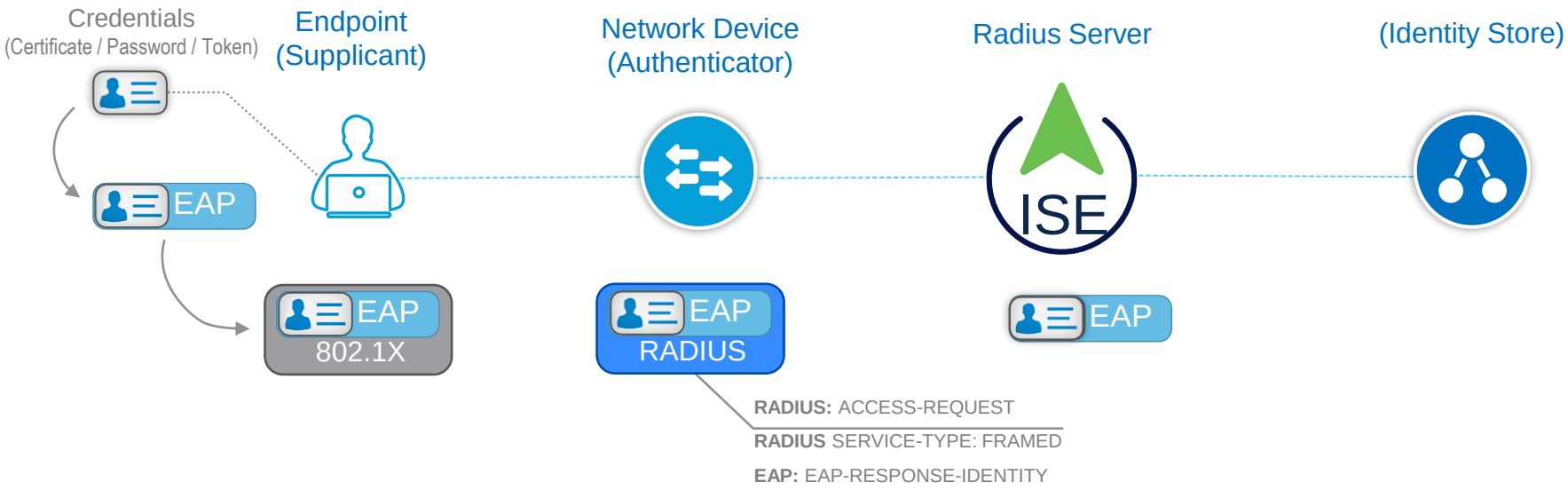
Identity Services

- Azure/AD/LDAP
- MDM
- SAML/MFA

Security Integration

- Cloud Analytics
- Secure Firewall
- Third party security products

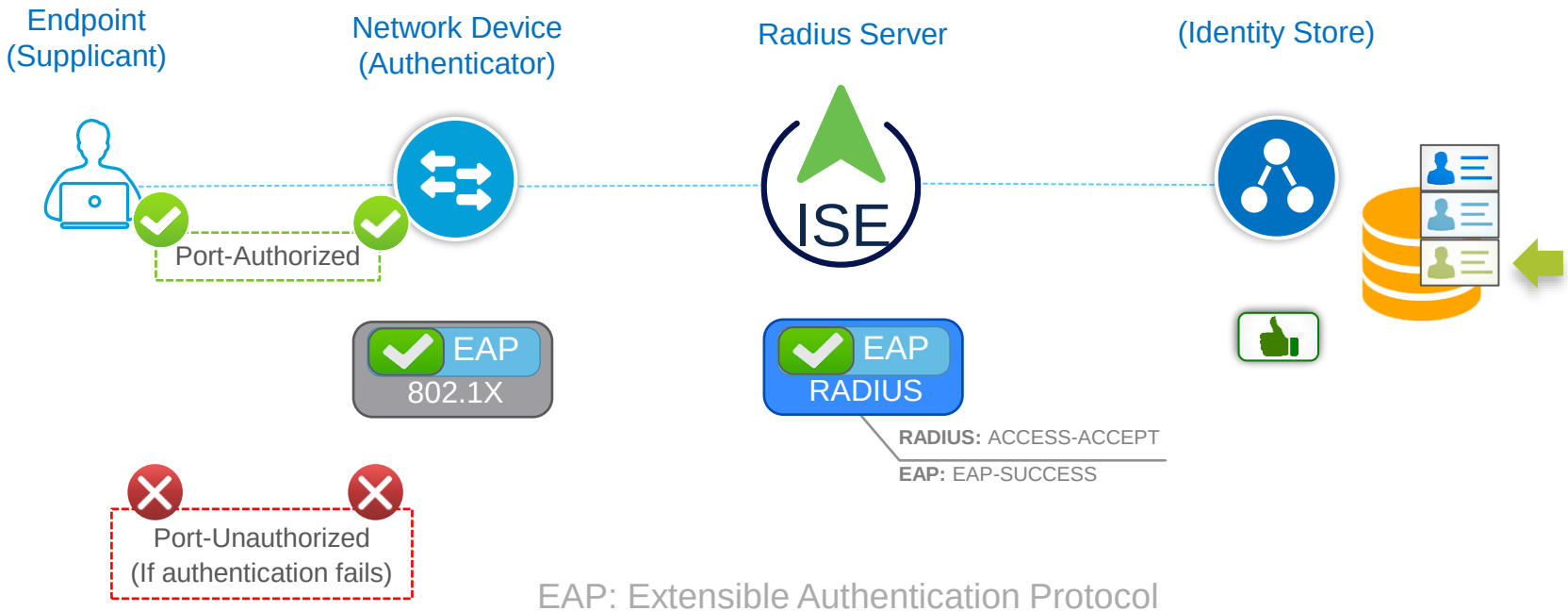
Fundamentals of 802.1X



EAP: Extensible Authentication Protocol

Supplicant: Software running on the client that provides credentials to the authenticator (Network Device).

Fundamentals of 802.1X



EAP: Extensible Authentication Protocol

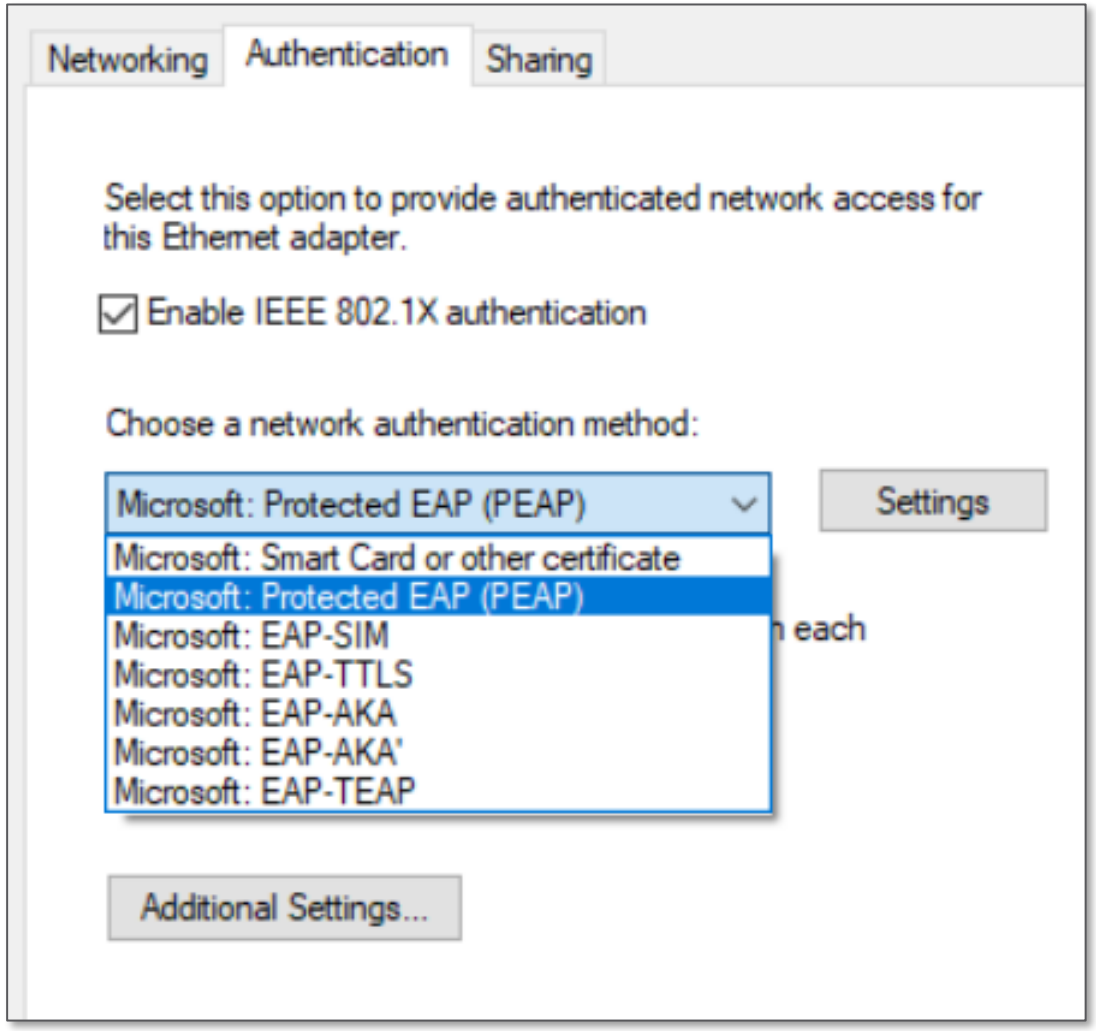
Supplicant: Software running on the client that provides credentials to the authenticator (Network Device).

Agenda

- Introduction to NAC & 802.1x
- Authentication
- Authorization
- Guest Access
- Profiling
- Posture
- Threat centric NAC with Third party integration

What type of authentication

- Multiple EAP
  - PEAP-MSCHAPv2
  - EAP-TLS
  - EAP-TTLS
  - EAP-GTC
  - EAP-AKA
  - EAP-TEAP
  - EAP-SIM
  - PEAP
  - ……



Authentication How and who

Machine authentication

And / Or

User authentication

Certificates

EAP-TLS

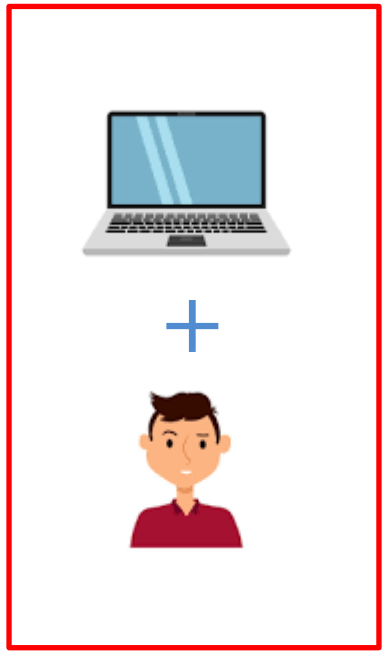
MAC-ID

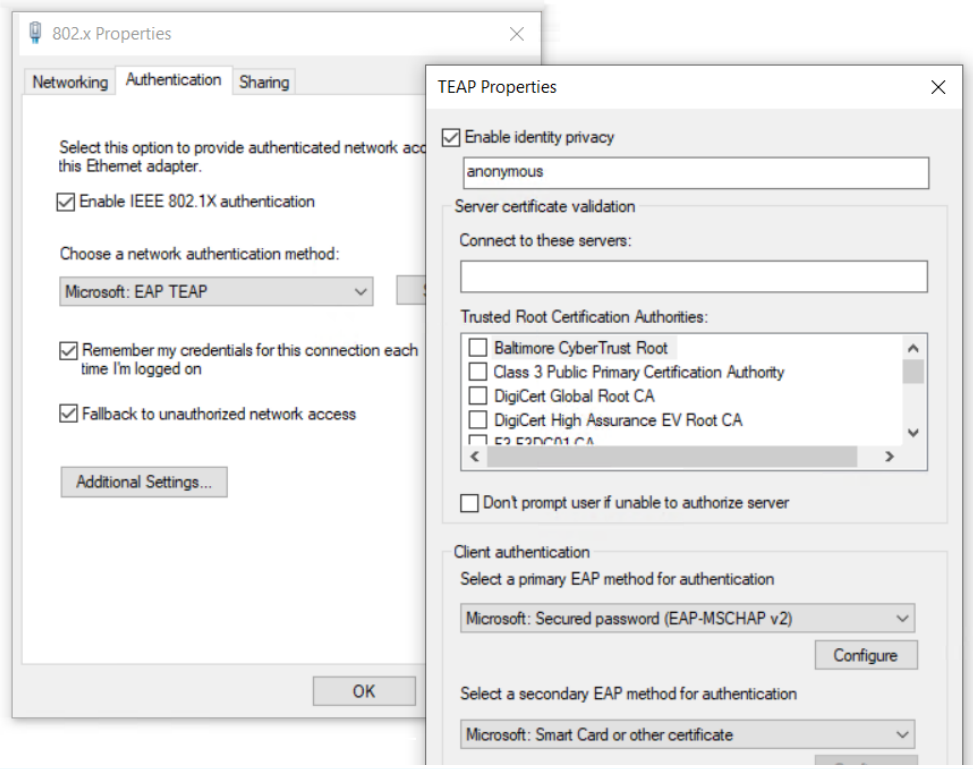
Passwords

PEAP-MSCHAPv2

Token / OTP

Trust User and Machine authentication with TEAP

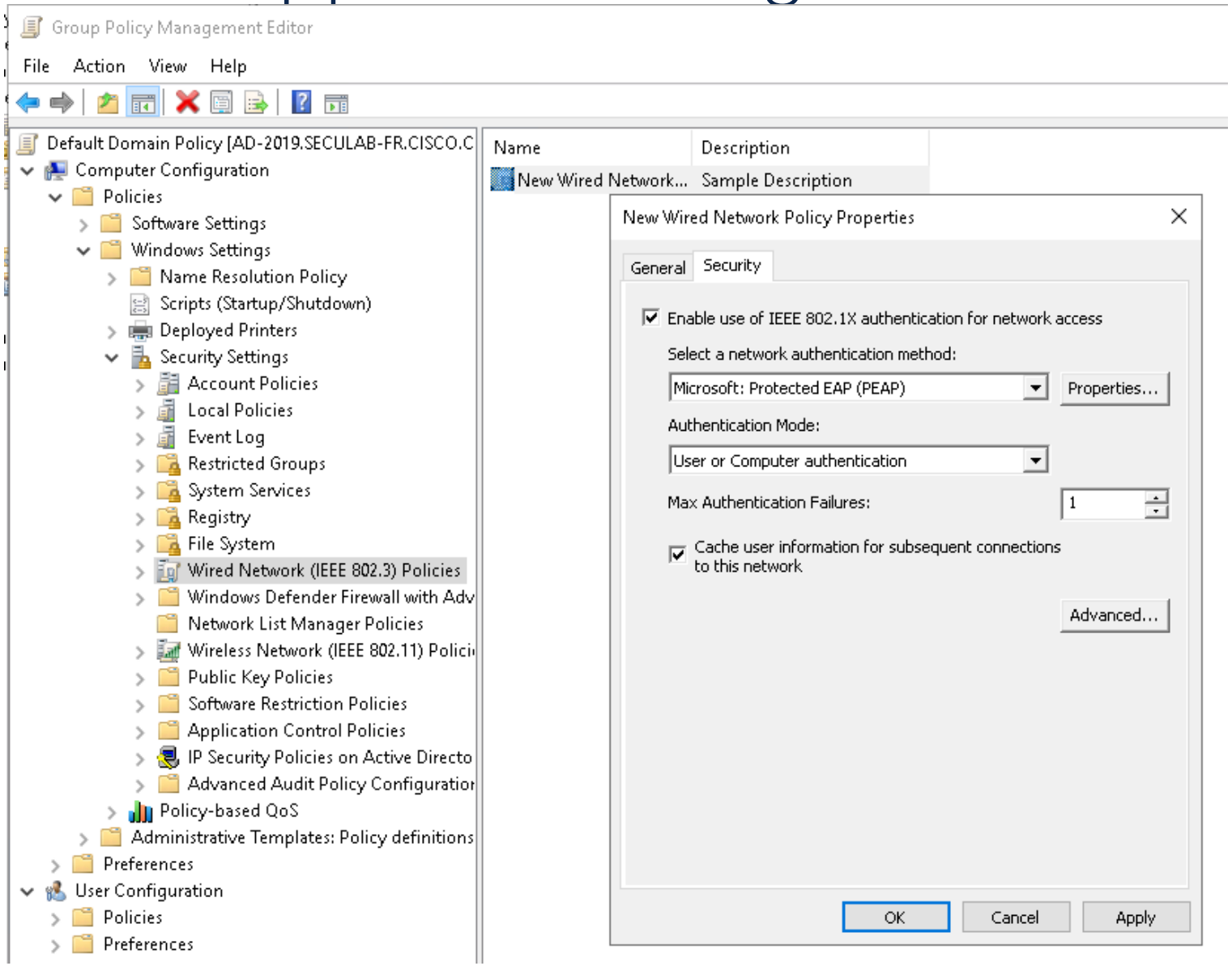




TEAP : Machine & User authentication

TEAP_Machine	AND	Network Access:EAP Tunnel EQUALS TEAP demo.local:ExternalGroups EQUALS demo.local/Users/Domain Computers Network Access EapChainingResult EQUALS **User failed and machine succeeded**	MachineAuth	Domain_Computers
TEAP_Chaining	AND	Network Access:EAP Tunnel EQUALS TEAP demo.local:ExternalGroups EQUALS demo.local/Users/Domain Users Network Access EapChainingResult EQUALS **User and machine both succeeded**	Permit Access	Employees

802.1x supplicant configuration from AD GPO



By default, TEAP is not configurable from AD Group Policy management

GPO need to be updated to support TEAP :

https://community.cisco.com/t5/security-knowledge-base/teap-for-windows-10-using-group-policy-and-ise-teap/ta-p/4134289

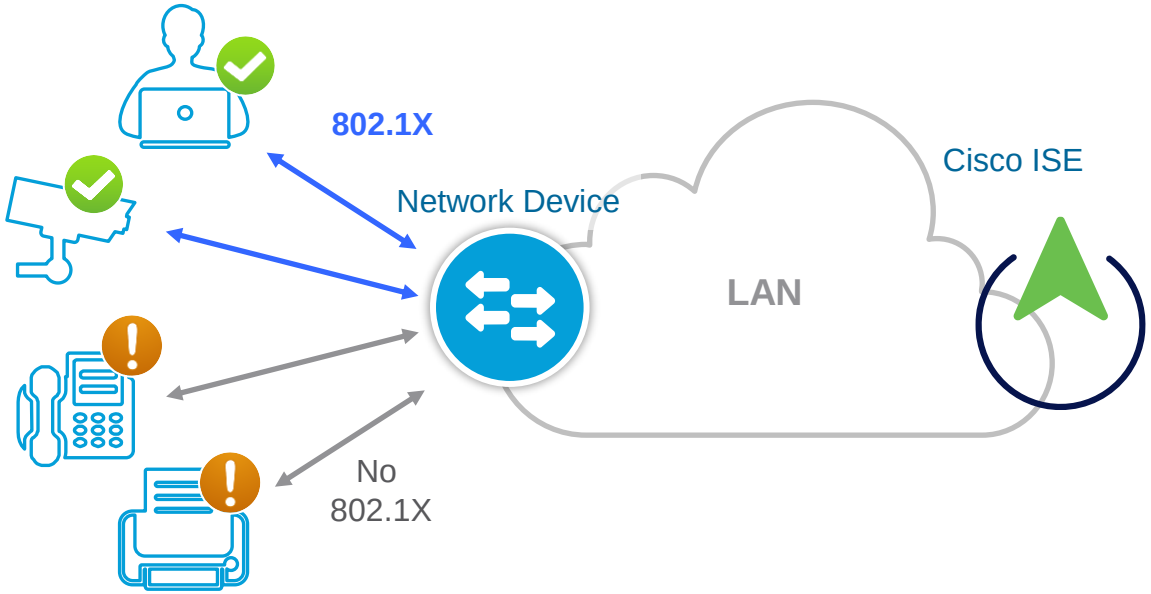
802.1X with EAP-TLS or TEAP to Azure AD

ISE separates Authentication from Authorization :

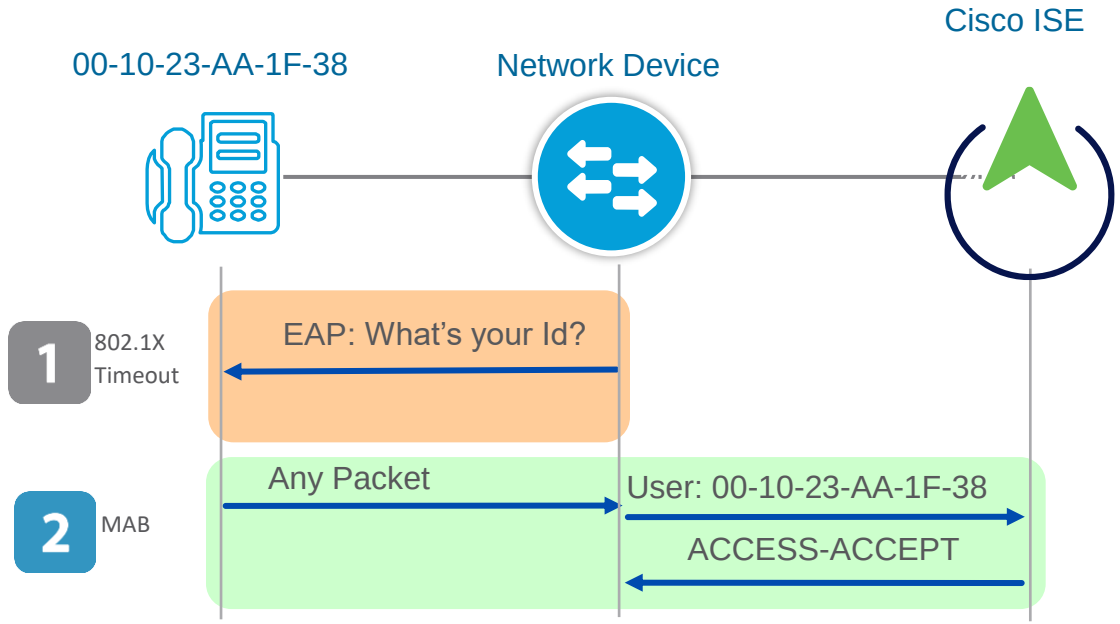
1. Authentication Using Certificate (user OR machine (EAP-TLS)| user AND machine (TEAP))
2. ISE fetches groups & attributes for certificate CN using Azure Graph API
3. Authorization based on Azure AD group membership and attributes

MAC Authentication Bypass (MAB)

Endpoints without supplicant will fail 802.1X authentication!



Bypassing “Known” MAC Addresses

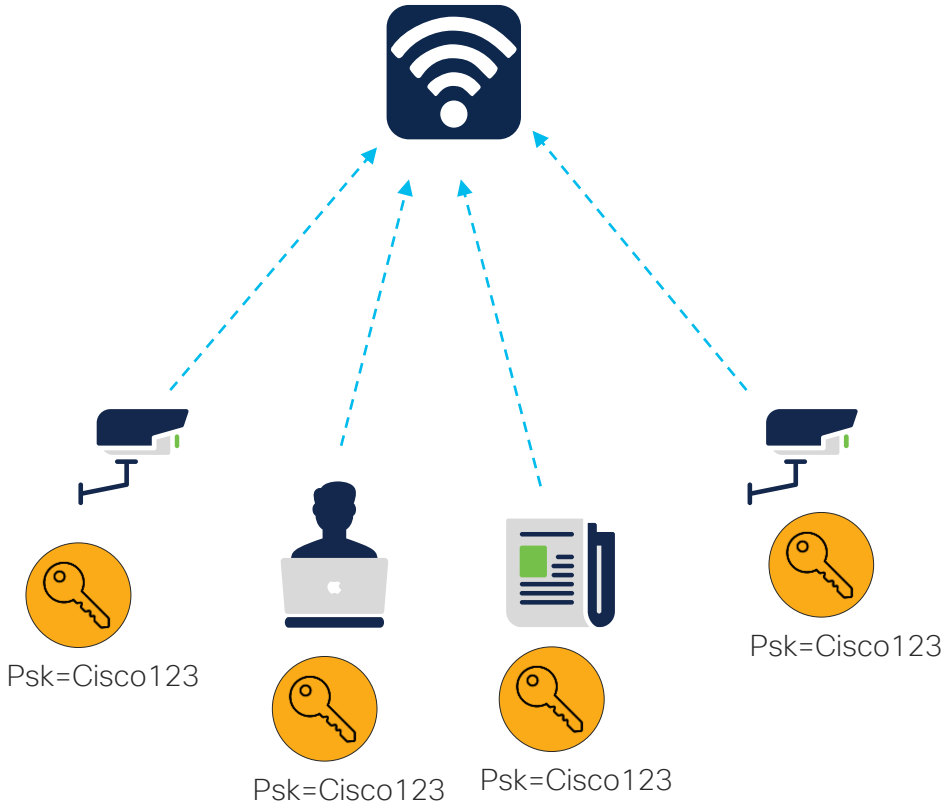


MAB requires a MAC database | ISE can build this database dynamically

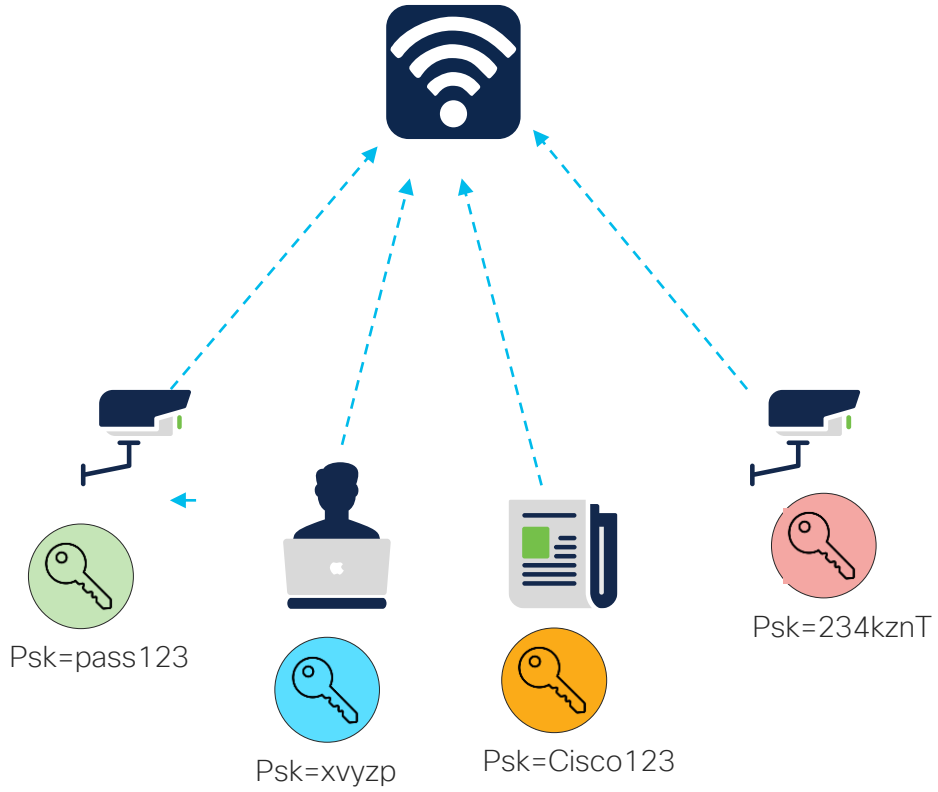
Wireless PSK & iPSK

Internal or external DB

Traditional PSK



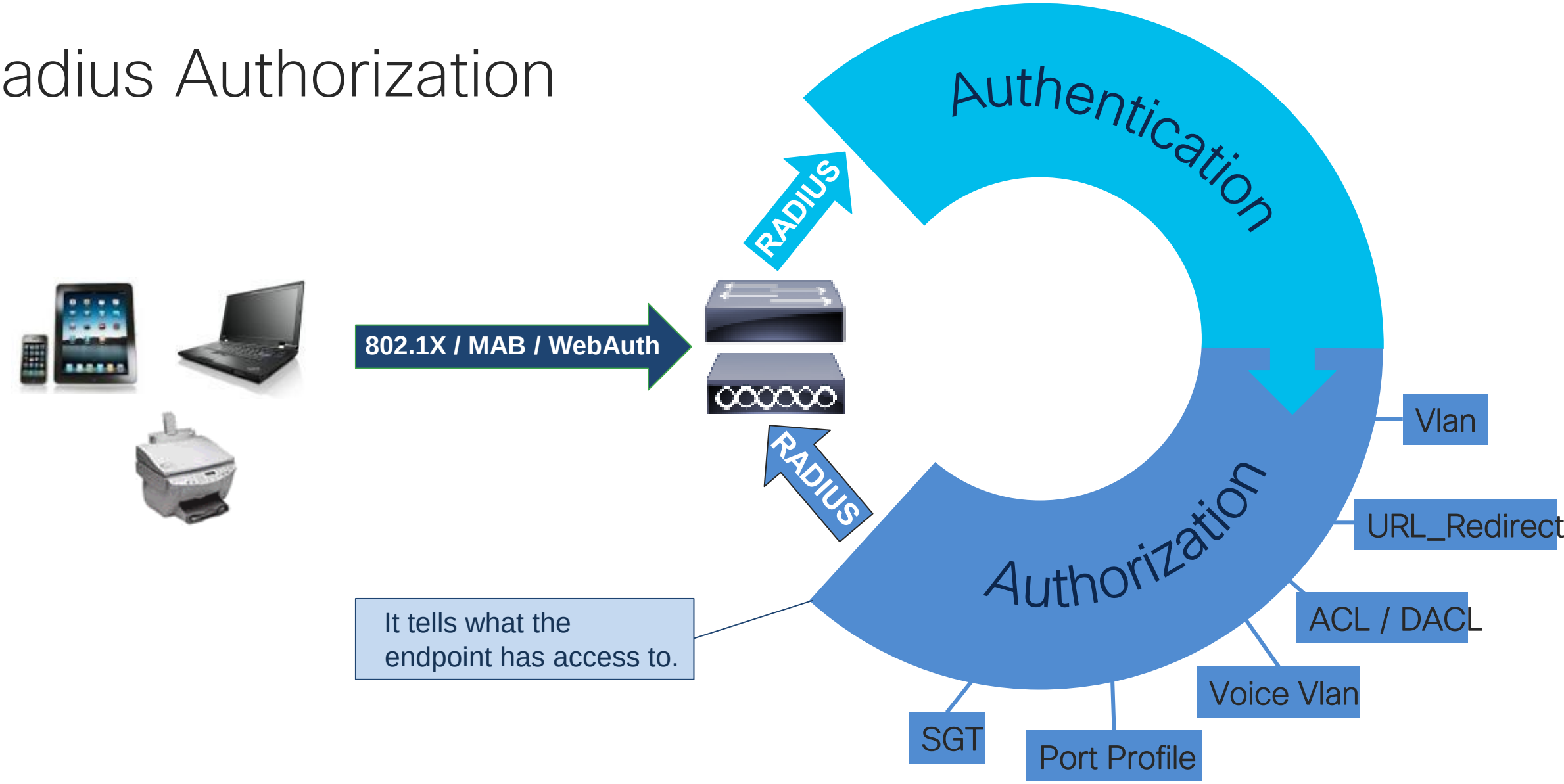
Identity PSK



Agenda

- Introduction to NAC & 802.1x
- Authentication
- Authorization
- Guest Access
- Profiling
- Posture
- Threat centric NAC with Third party integration

Radius Authorization



18

Radius Attribute

IETF

Dictionaries > RADIUS > IETF

Dictionary | Dictionary Attributes

Dictionary Attributes

Edit

Name	Number	Type	Direction	Description	Predefi...
Delegated-IPv6-Prefix	123	IPV6PREFIX	BOTH	DelegatedIPv6Prefix	YES
Delegated-IPv6-Pre...	171	STRING	BOTH	DelegatedIPv6PrefixPool	YES
Digest-Attributes	207	STRING	BOTH	DigestAttributes	YES
Digest-Response	206	STRING	BOTH	DigestResponse	YES
EAP-Key-Name	102	STRING	NONE	EapKeyName	YES
EAP-Message	79	STRING	BOTH	EapMessage	YES
Egress-VLAN-Name	58	STRING	BOTH	Egress-VLAN-Name	YES
Egress-VLANID	56	INT	BOTH	Egress-VLANID	YES
Error-Cause	101	INT	BOTH	ErrorCause	YES
Event-Timestamp	55	INT	IN	EventTimestamp	YES
Filter-ID	11	STRING	BOTH	FilterID	YES
Framed-AppleTalk-L...	37	INT	OUT	FramedAppleTalkLink	YES
Framed-AppleTalk-...	38	INT	OUT	FramedAppleTalkNetwork	YES
Framed-AppleTalk-Z...	39	STRING	OUT	FramedAppleTalkZone	YES
Framed-Compression	13	INT	BOTH	FramedCompression	YES

Vendor Specific Attribute

Dictionaries > ... > RADIUS Vendors > Microsoft

Dictionary | Dictionary Attributes

Dictionary Attributes

Add | Edit | Delete

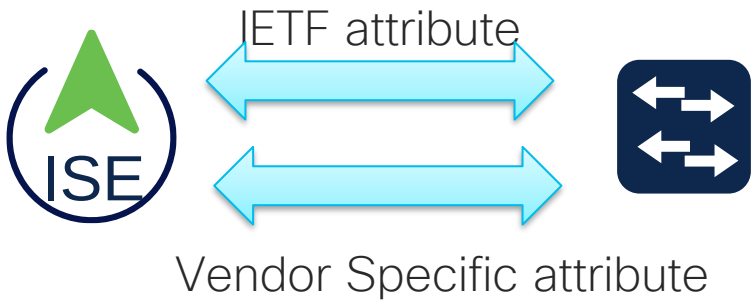
Name	Number	Type	Direction	Description	Predefi...
MS-AFW-Protection...	49	UINT32	BOTH	Attribute MS-AFW-Prote...	NO
MS-AFW-Zone	48	UINT32	BOTH	Attribute MS-AFW-Zone	NO
MS-ARAP-PW-Chan...	21	UINT32	BOTH	Attribute MS-ARAP-PW-...	NO
MS-Acct-Auth-Type	23	UINT32	BOTH	Attribute MS-Acct-Auth-...	NO
MS-Acct-EAP-Type	24	UINT32	BOTH	Attribute MS-Acct-EAP-...	NO
MS-BAP-Usage	13	UINT32	BOTH	Attribute MS-BAP-Usage	NO
MS-CHAP-CPW-1	3	OCTET_STRI...	BOTH	Attribute MS-CHAP-CP...	NO
MS-CHAP-CPW-2	4	OCTET_STRI...	BOTH	Attribute MS-CHAP-CP...	NO
MS-CHAP-Challenge	11	OCTET_STRI...	BOTH	Attribute MS-CHAP-Cha...	NO
MS-CHAP-Domain	10	STRING	BOTH	Attribute MS-CHAP-Do...	NO
MS-CHAP-Error	2	STRING	BOTH	Attribute MS-CHAP-Error	NO
MS-CHAP-LM-Enc-...	5	OCTET_STRI...	BOTH	Attribute MS-CHAP-LM-...	NO
MS-CHAP-MPPE-Ke...	12	OCTET_STRI...	BOTH		NO
MS-CHAP-NT-Enc-...	6	OCTET_STRI...	BOTH	Attribute MS-CHAP-NT-...	NO
MS-CHAP-Response	1	OCTET_STRI...	BOTH	Attribute MS-CHAP-Res...	NO

Radius Server should support Third party Libraries

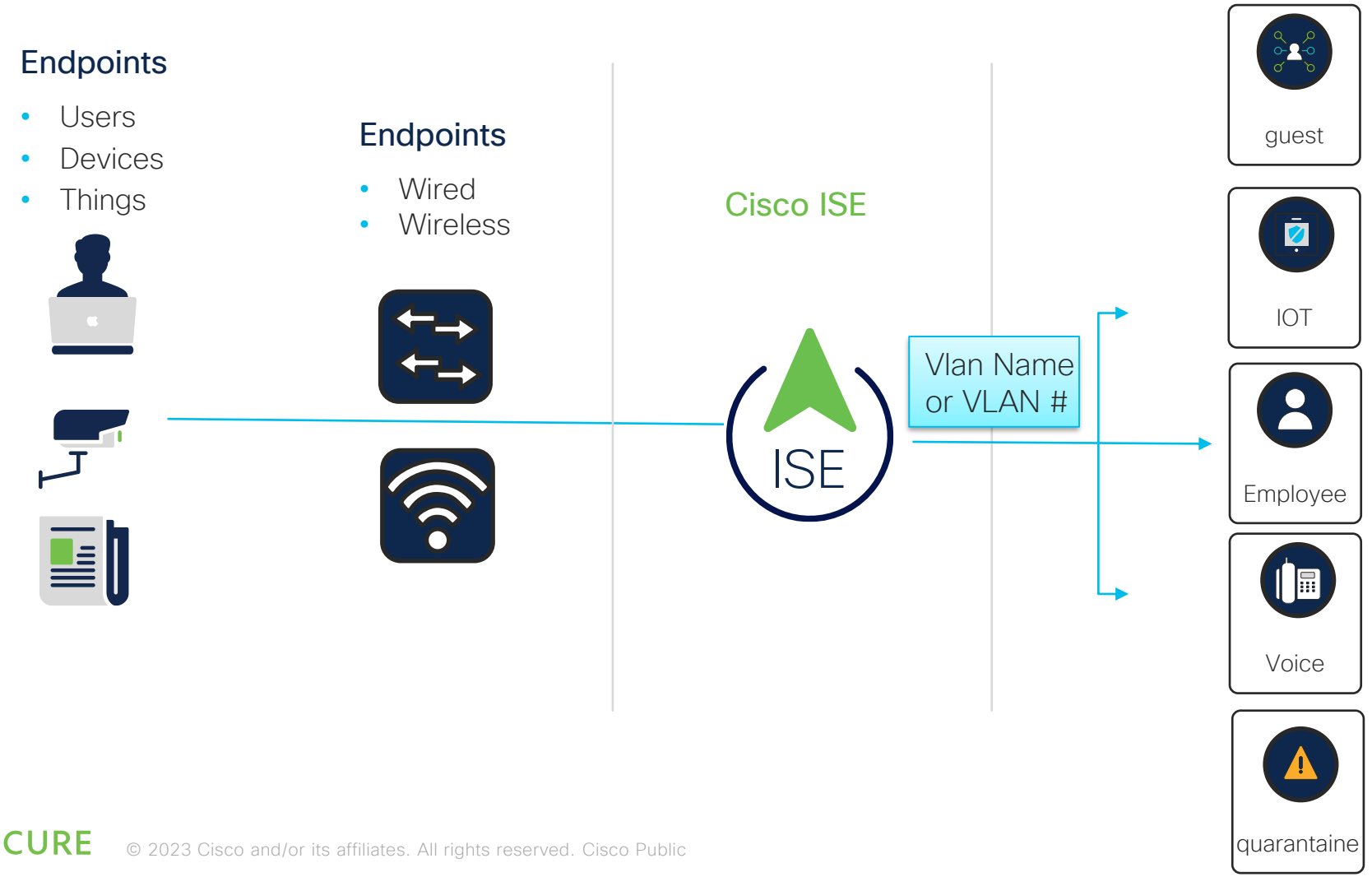
RADIUS Vendors

Edit | Add | Delete | Import | Export

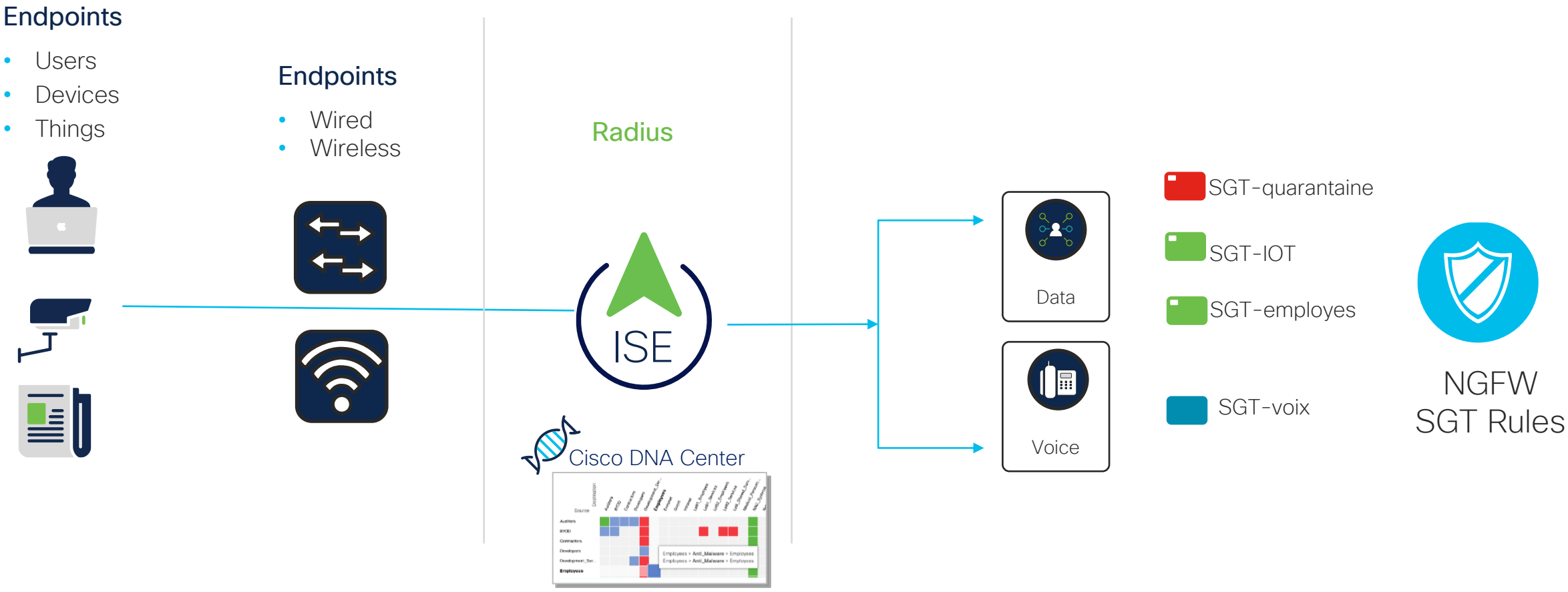
Name	Vendor ID	Description
3gpp	10415	Dictionary for Vendor 3gpp
Airespace	14179	Dictionary for Vendor Airespace
Alcatel-Lucent	800	Dictionary for Vendor Alcatel-Lucent
Aruba	14823	Dictionary for Vendor Aruba
Brocade	1588	Dictionary for Vendor Brocade
Cisco	9	Dictionary for Vendor Cisco
Cisco-BBSM	5263	Dictionary for Vendor Cisco-BBSM
Cisco-VPN3000	3076	Dictionary for Vendor Cisco-VPN3000
H3C	25506	Dictionary for Vendor H3C
HP	11	Dictionary for Vendor HP
Juniper	2636	Dictionary for Vendor Juniper
Microsoft	311	Dictionary for Vendor Microsoft
Motorola-Symbol	388	Dictionary for Vendor Motorola-Symbol
Ruckus	25053	Dictionary for Vendor Ruckus
WISPr	14122	Dictionary for Vendor WISPr



USE case 1 : vlan assignment



USE case 2: Micro-Segmentation, SGT

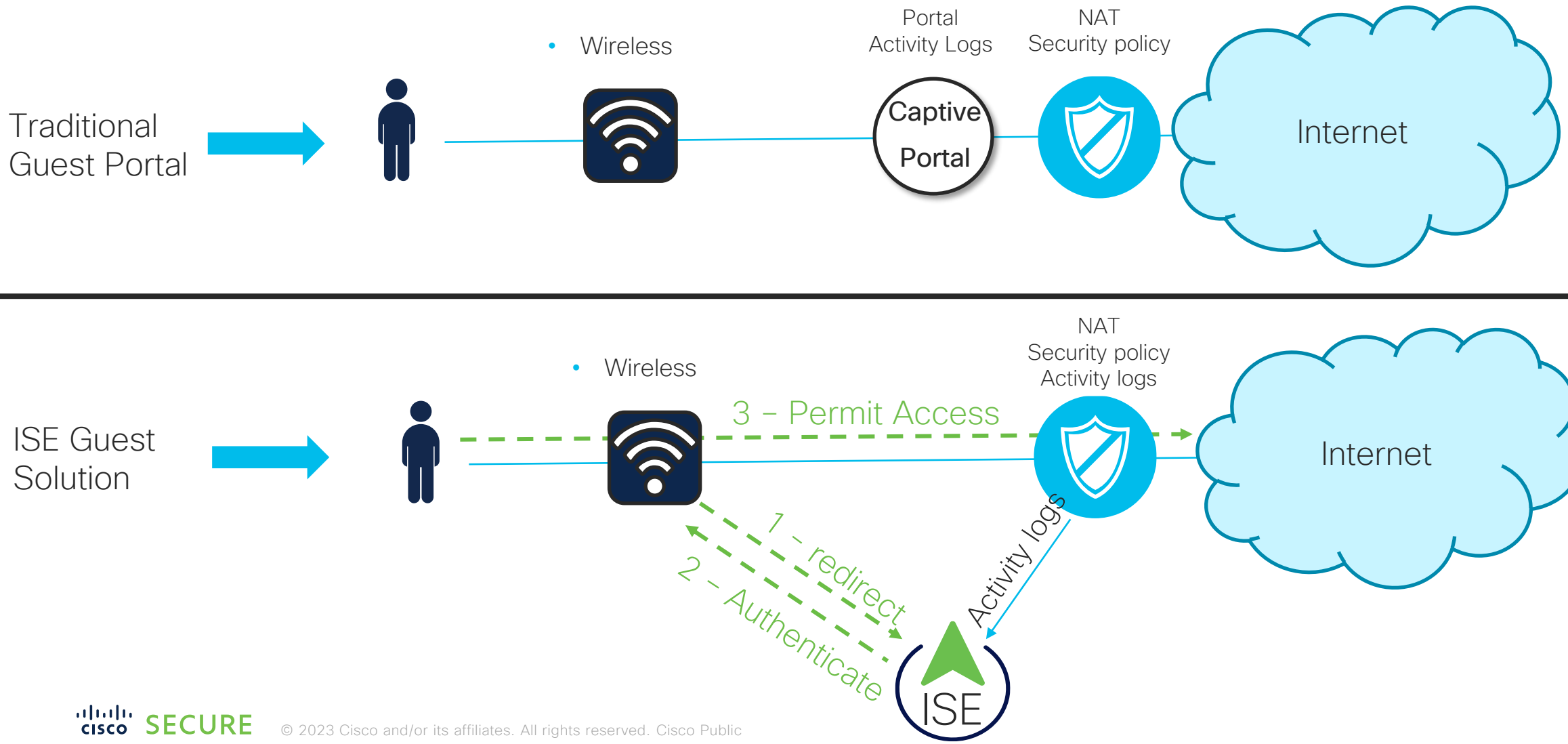


Agenda

- Introduction to NAC & 802.1x
- Authentication
- Authorization
- Guest Access
- Profiling
- Posture
- Threat centric NAC with Third party integration

USE case 3: Guest Access

Guest solutions : traditional vs ISE



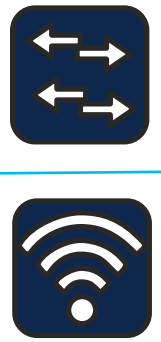
Agenda

- Introduction to NAC & 802.1x
- Authentication
- Authorization
- Guest Access
- Profiling
- Posture
- Threat centric NAC with Third party integration

USE case 4: asset identifications, profiling

Endpoints

- Wired
- Wireless



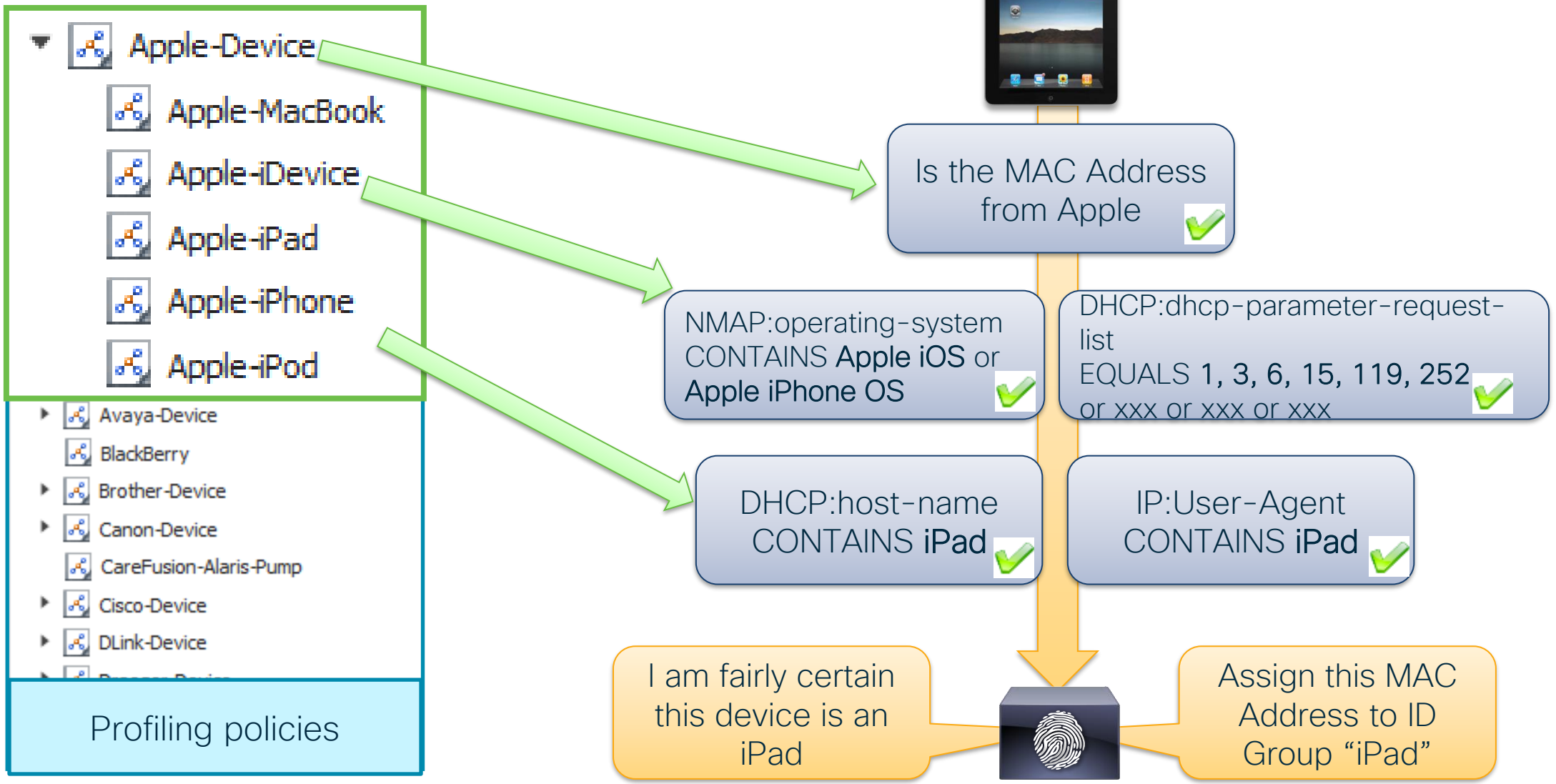
ACTIVE PROBES	Netflow	DHCP	DNS	HTTP	RADIUS	NMAP	SNMP	AD
DEVICE SENSOR	CDP	LLDP	DHCP	HTTP	H323	SIP	MDNS	
ANYCONNECT	ACIDex							

ISE data collection methods for Device profiling

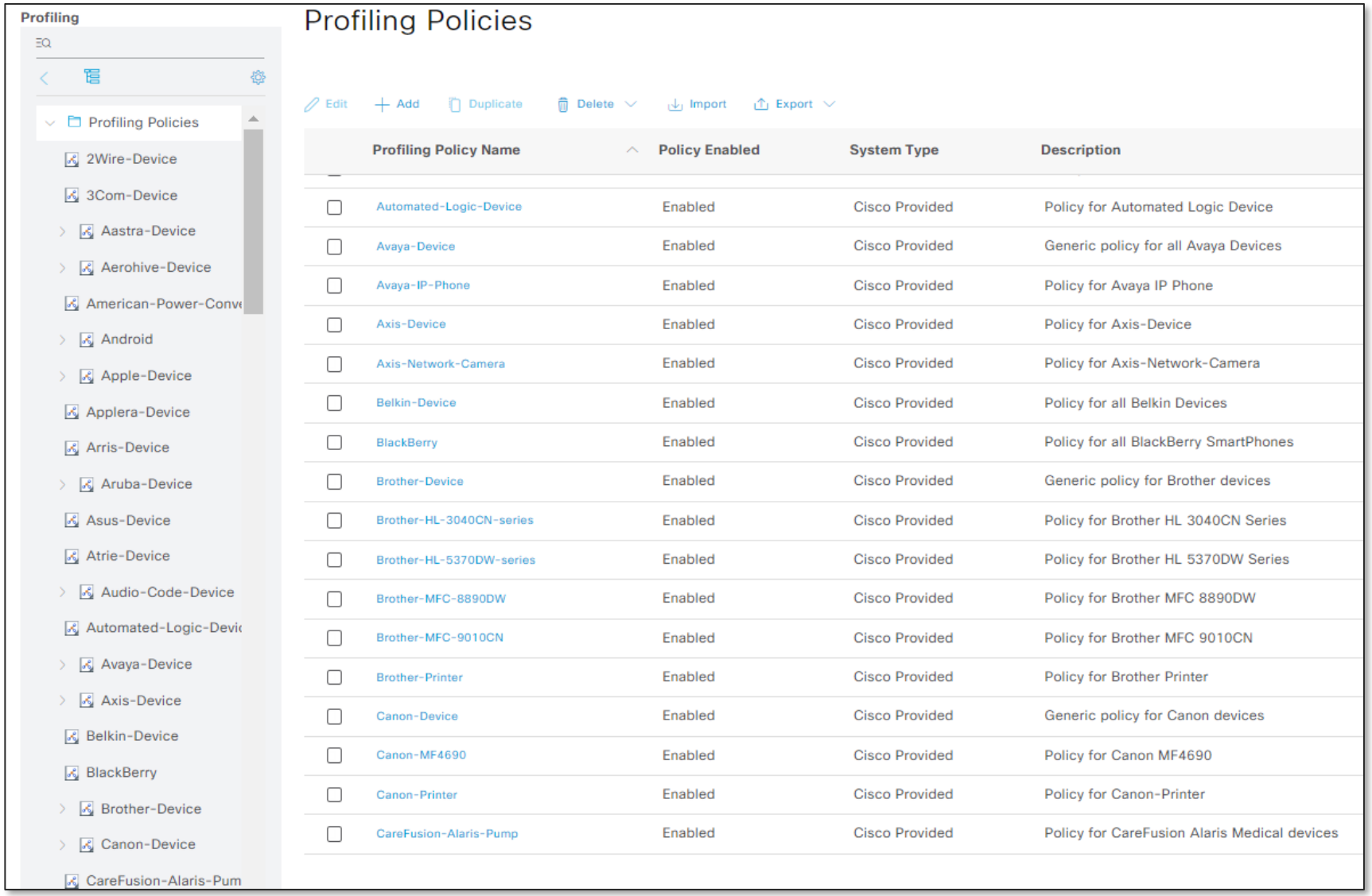
Cisco ISE

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

Example : IPAD profiling



Radius server Profiling policies



Profiling Packages and Integrations

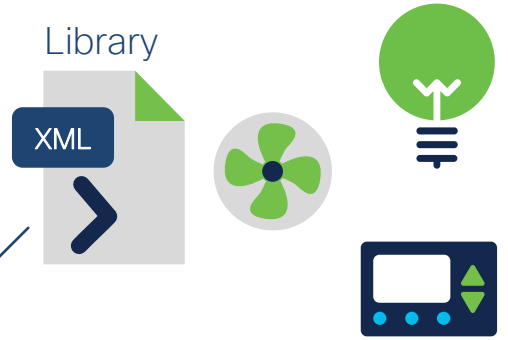
Medical Devices

Hospital

250+ Medical device profiles

- Pharma-Smart-Device
- Philips-Analytical-X-Ray-Device
- Philips-CareServant-Device
- Philips-Healthcare-PCCI-Device
- Philips-Medical-Systems-Device
- Philips-Oral-Healthcare-Device
- Philips-Patient-Monitoring-Device
- Philips-Personal-Health-Device
- Philips-Respironics-Device
- Phonak-Communications-Device

IOT Building & Automation



pxGrid

Factory

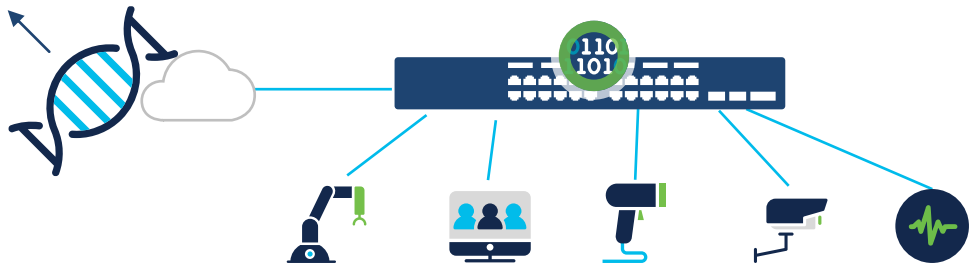
pxGrid

Cisco CyberVision

Industrial Devices

Cisco AI Endpoint Analytics

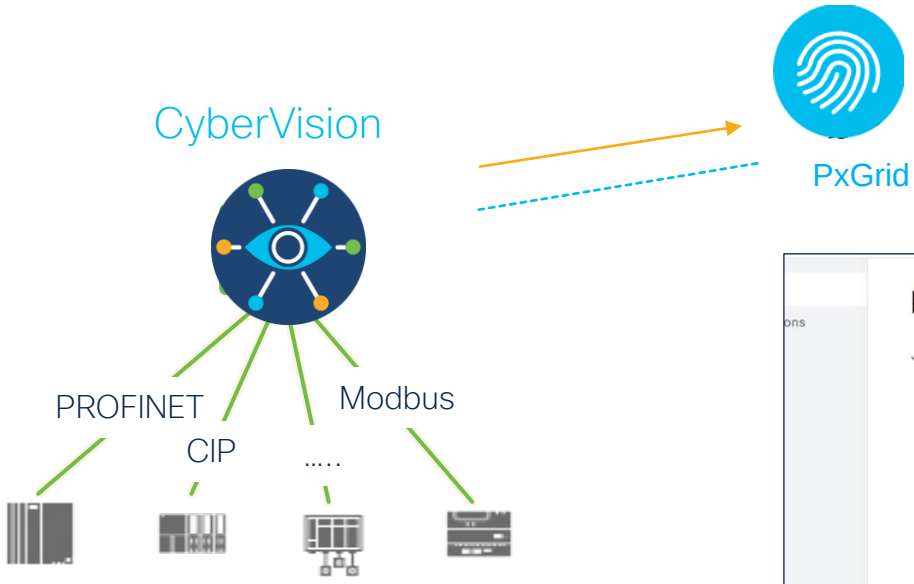
Profiles IOT devices and sends endpoint labels via pxGrid to ISE for authorization



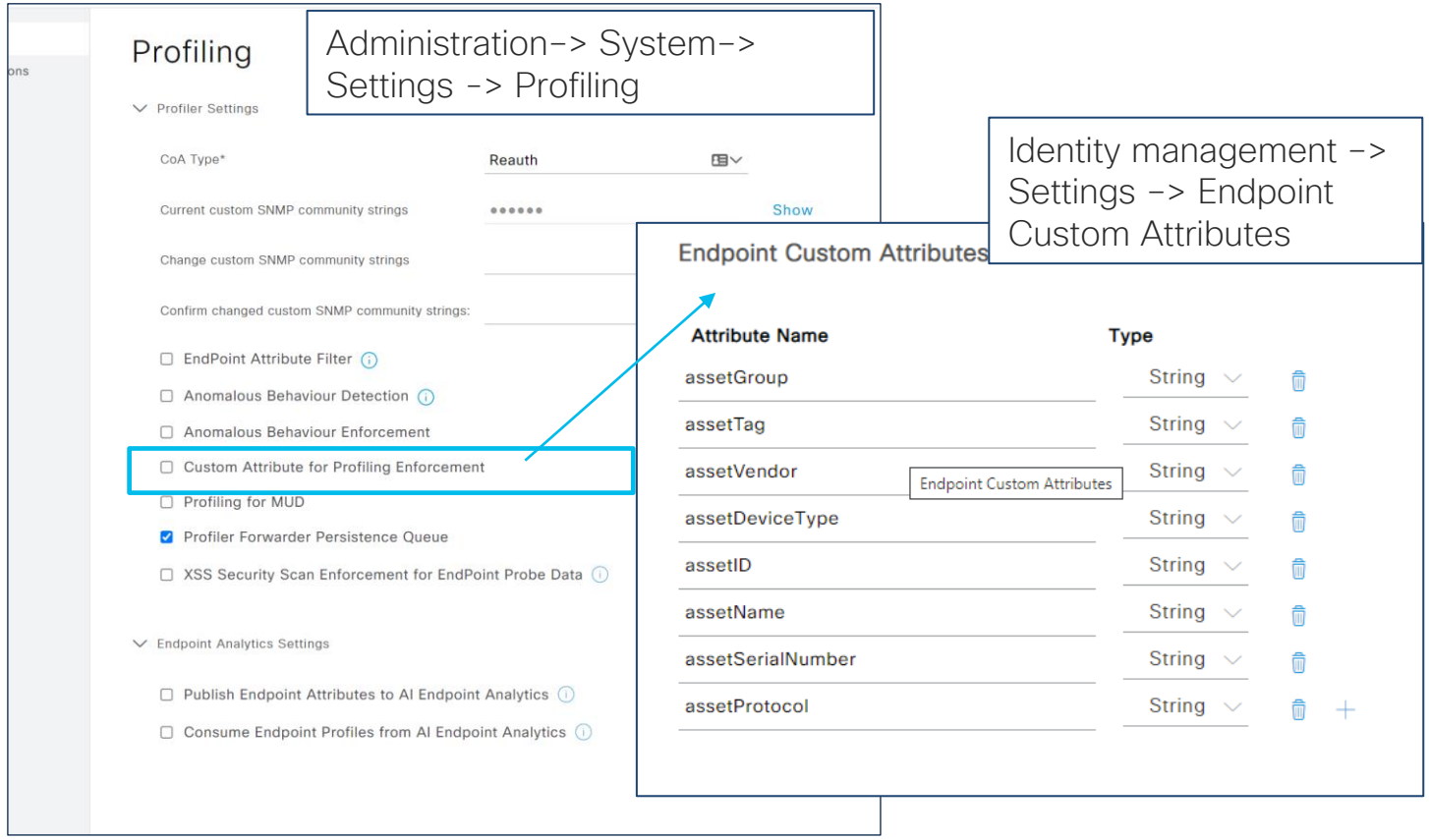
MEDIGATE · CYBER MDX · CLAROTY · NOZOMI NETWORKS · SECURITY MATTERS · Zingbox · Cynerio · armis · CloudPost

https://community.cisco.com/t5/tag/ise-endpoint-profile/tg-p/board-id/4561-docs-security

Example : Cybervision integration

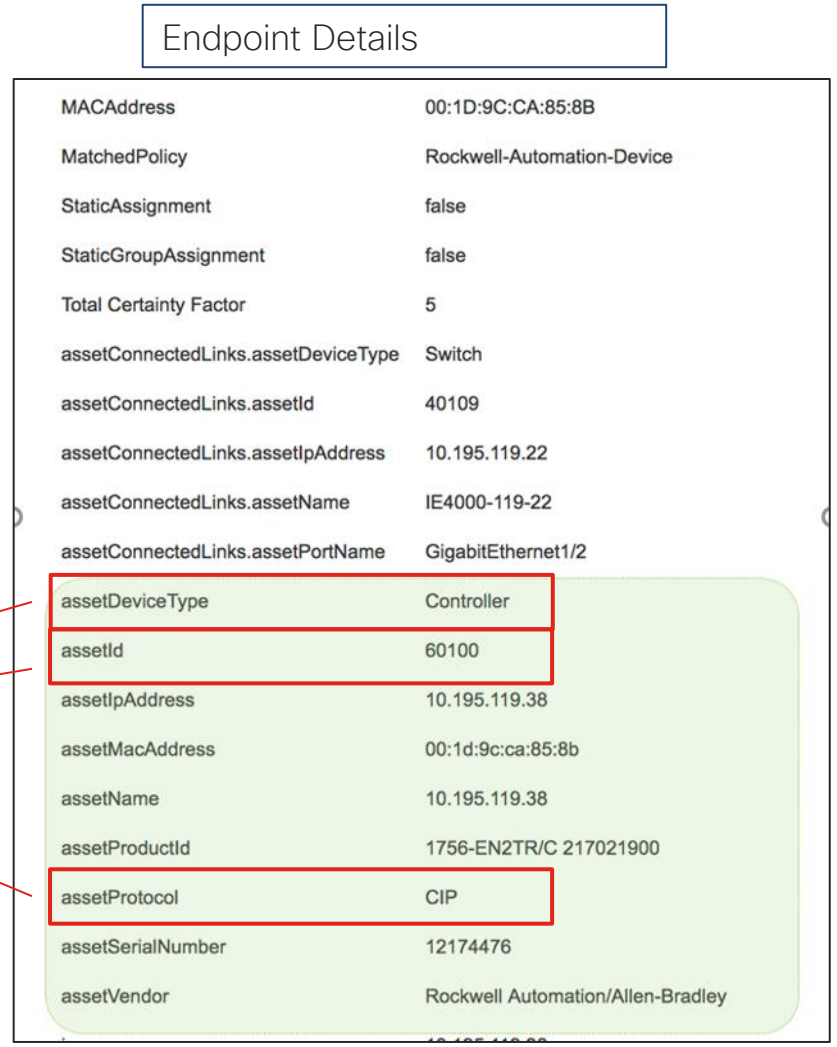


- CyberVision classifies the OT devices based on the results of Deep Packet Inspection.
- The attributes are then sent up to ISE via pxGrid
- ISE populates the custom attributes with the ones received via profiling pxGrid probe

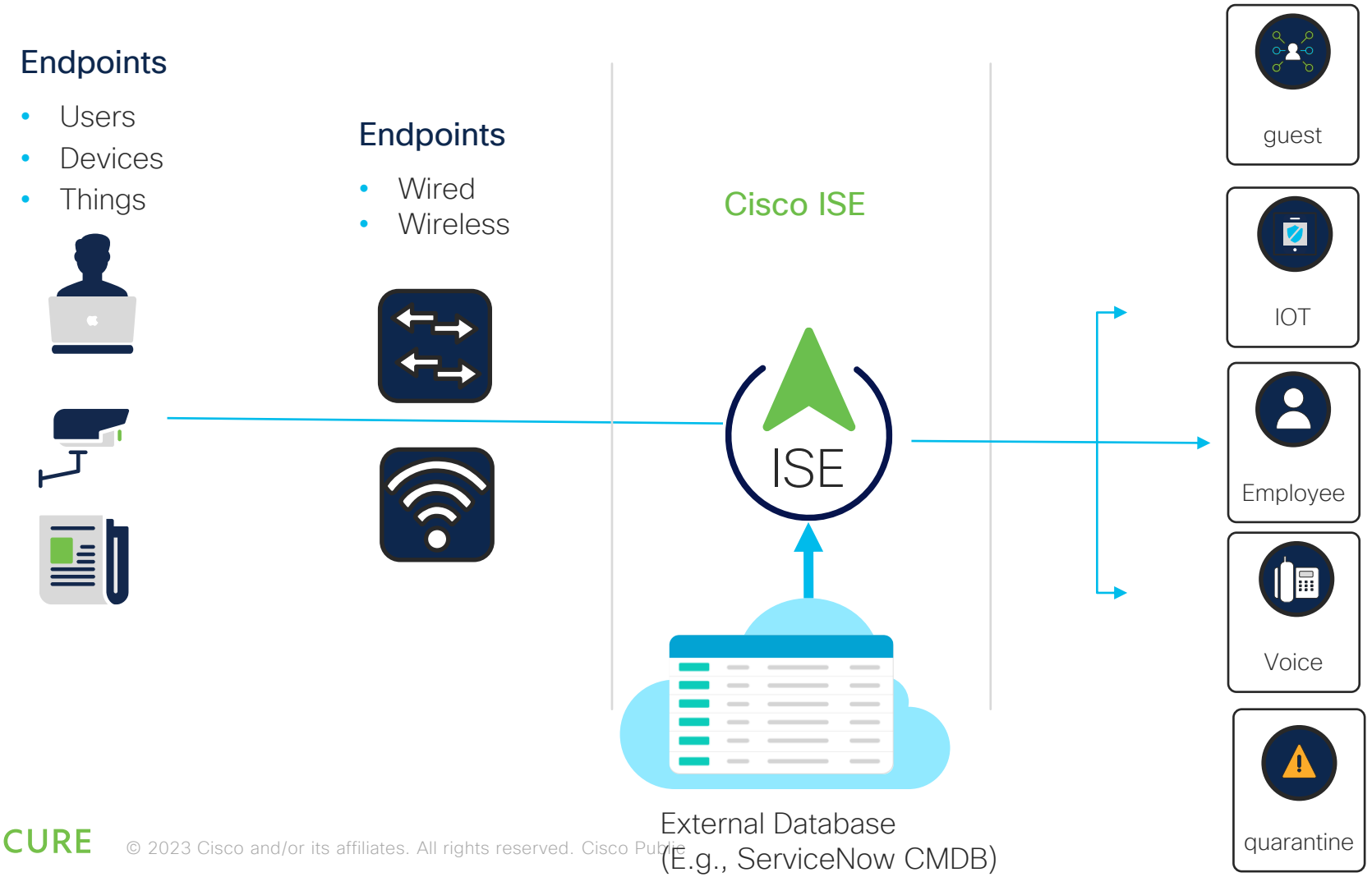


PxGrid Probe

Custom attributes populated from form CyberVision



CMDB integration



Cisco ISE

Add pxGrid Direct Connector

Welcome | Connector Definition | URL | Schedule | Parent Object | 6 Att

Select Attributes Configure Dictionary Items

Add the attributes that Cisco ISE must retrieve from the pxGrid Direct connector. Choose attributes that should be included to the Cisco ISE Dictionary by clicking the toggle switch next to an attribute. Enter the attribute name that you want displayed in the Cisco ISE Dictionary. All the attributes that are retrieved from the pxGrid Direct connector persist in Cisco ISE even if they are not included in the Cisco ISE Dictionary.

Add Attribute | Delete | Include all in Dictionary

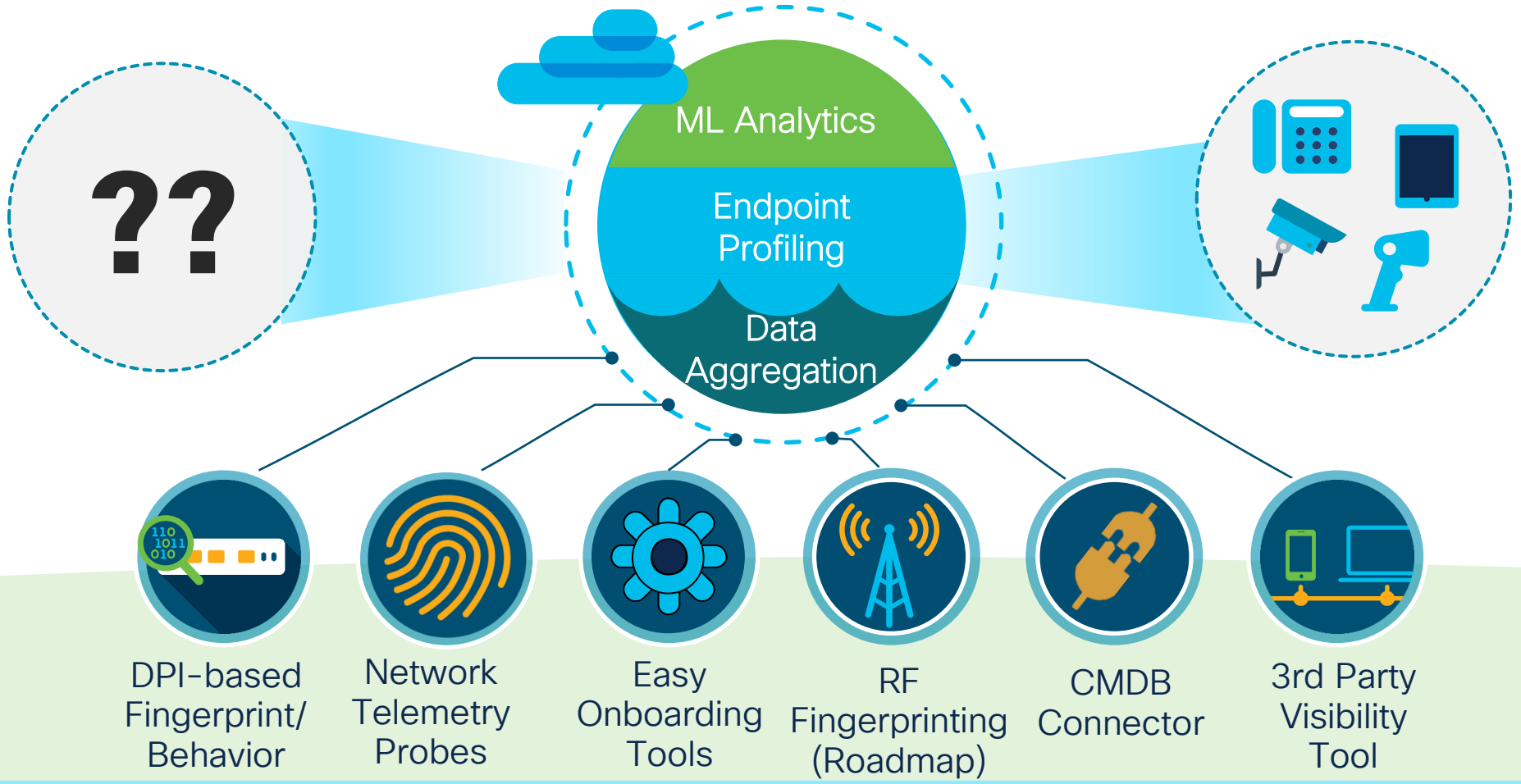
External Name	Include in Dictionary	Name in Dictionary
$.created	on	created
$.department	off	department
$.description	off	description
$.expires	on	expires
$.ipsk	on	ipsk
$.mac_address	on	mac_address
$.owner	on	owner
$.status	on	status

Exit Wizard

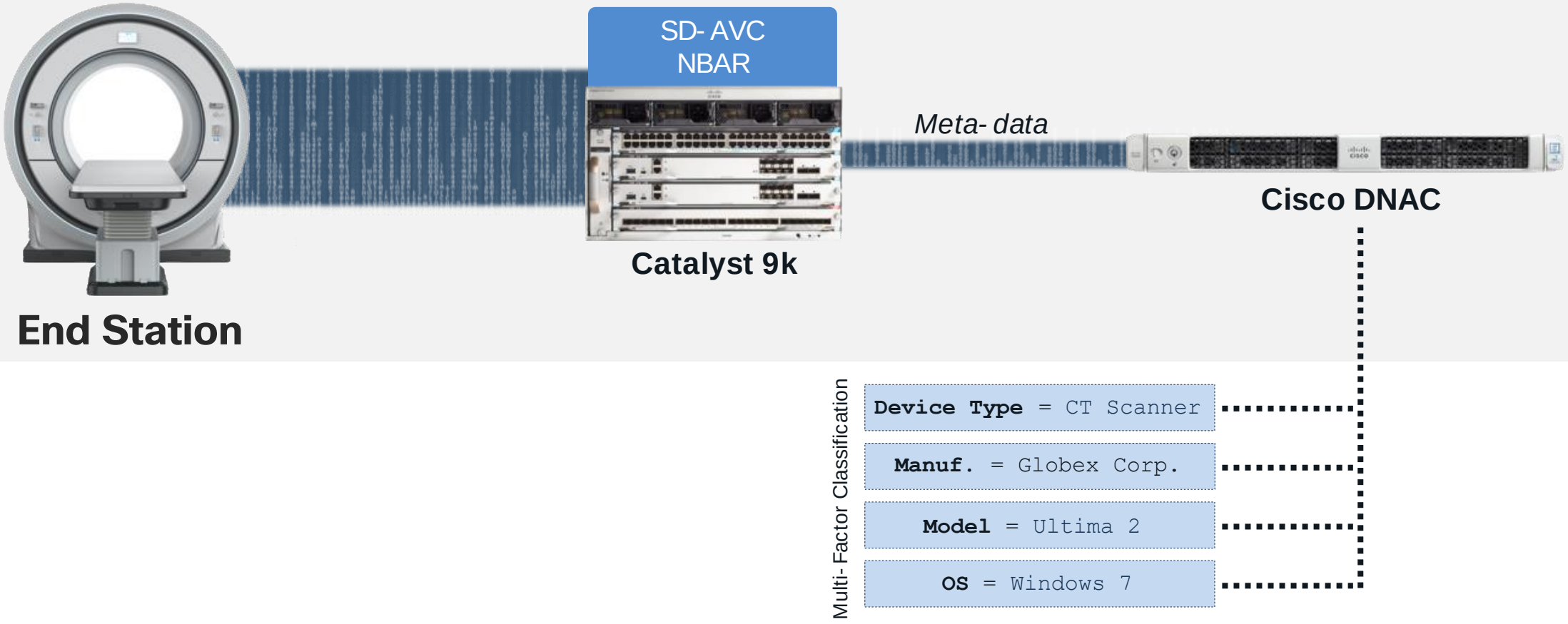

```
{
 "results":[
    {
        "mac_address":"DC:A6:32:6D:A3:BB",
        "ipsk":"Ktghmo9M",
        "created":"20220819T113319",
        "expires":"20230819T113319",
        "owner":"thomas@cisco.com",
        "status":"Operational",
        "department":"Facilities",
        "description":"rpi-1 | Raspberry Pi
    },
    {
        "mac_address":"DC:A6:32:1A:C5:F8",
        "ipsk":"Cisco123",
        "created":"20220819T113319",
        "expires":"20230819T113319",
        "owner":"thomas@cisco.com",
        "status":"Operational",
        "department":"Signage",
        "description":"rpi-2 | Raspberry Pi
    },
...
```

Continuous Trust with DNA Center Endpoint Analytics

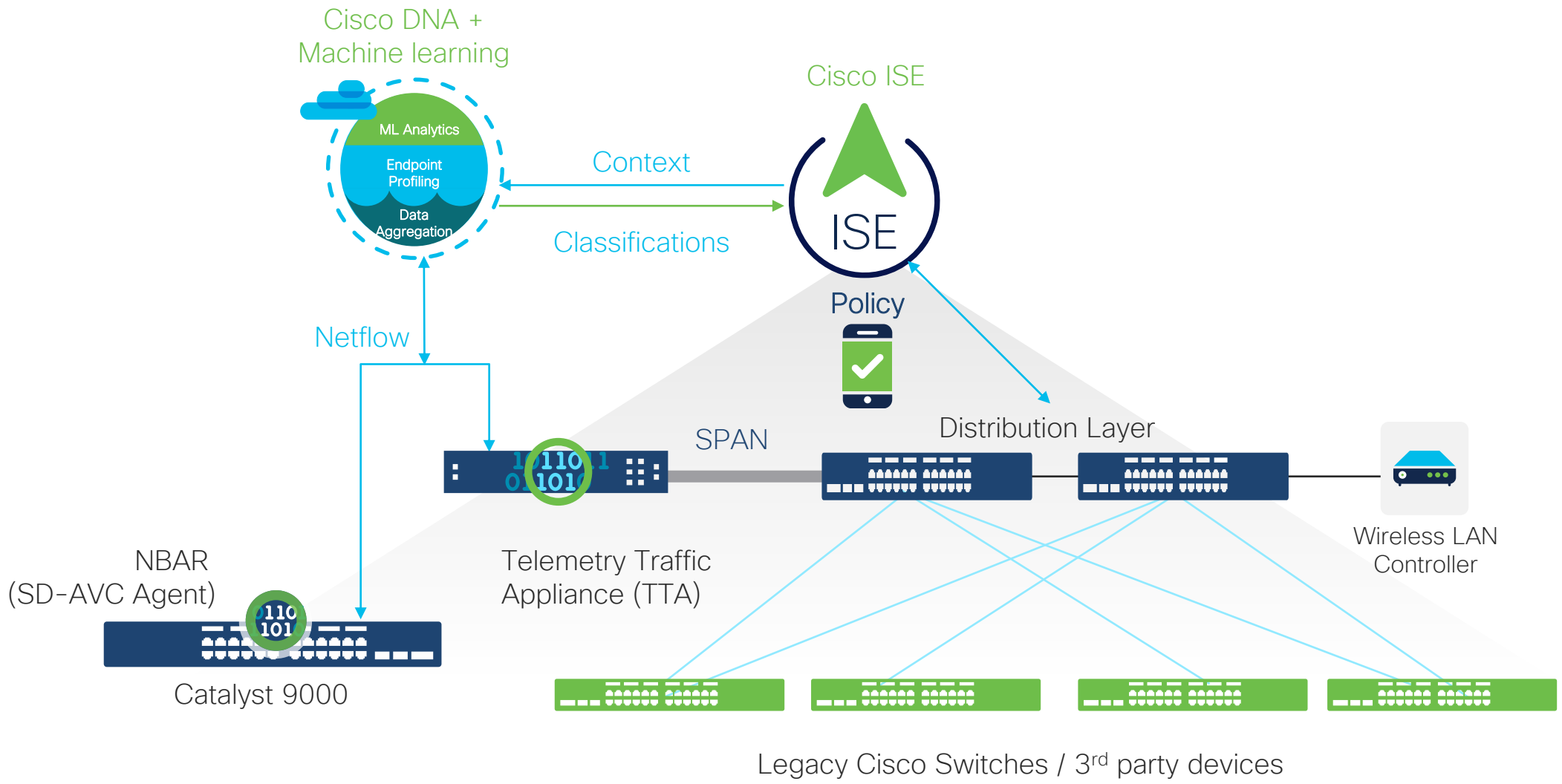
Rapidly reducing the unknowns to gain visibility



AI Endpoint Analytics for enhanced profiling

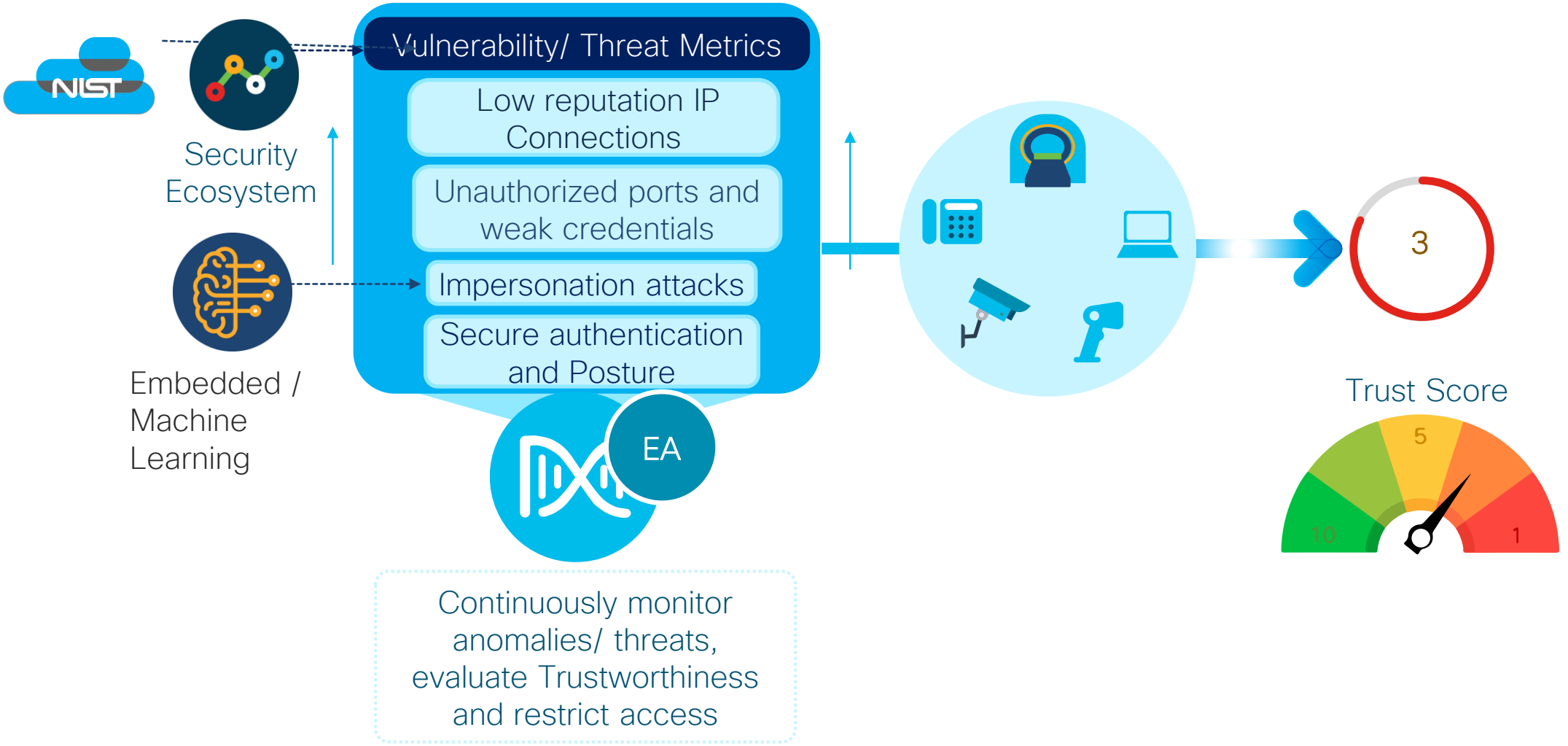


DNA Center Endpoint Analytics and ISE

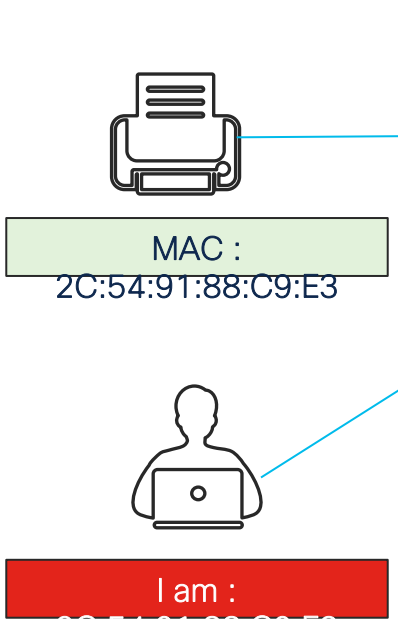


Continuous Trust with DNAC Trust Analytics:

Continuous evaluation of endpoint security posture for Trusted Access

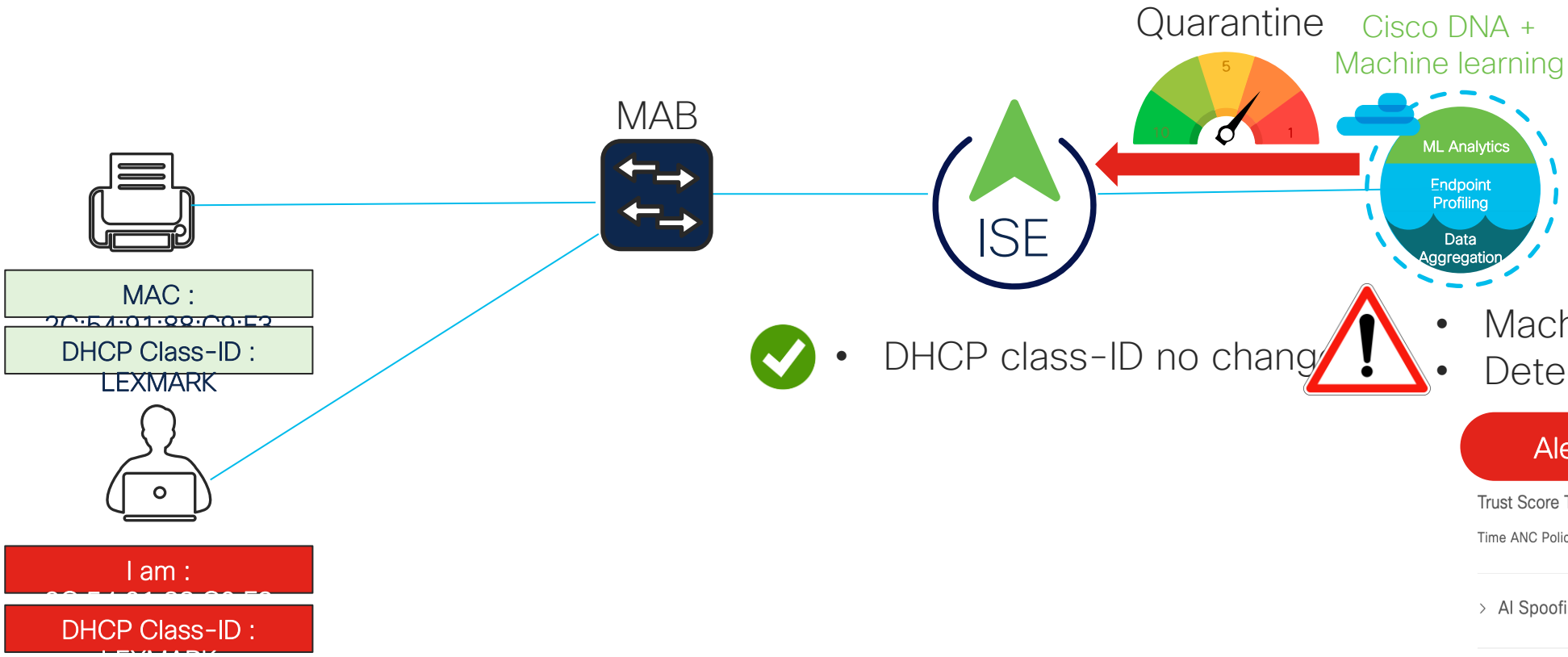


Mac Spoofing

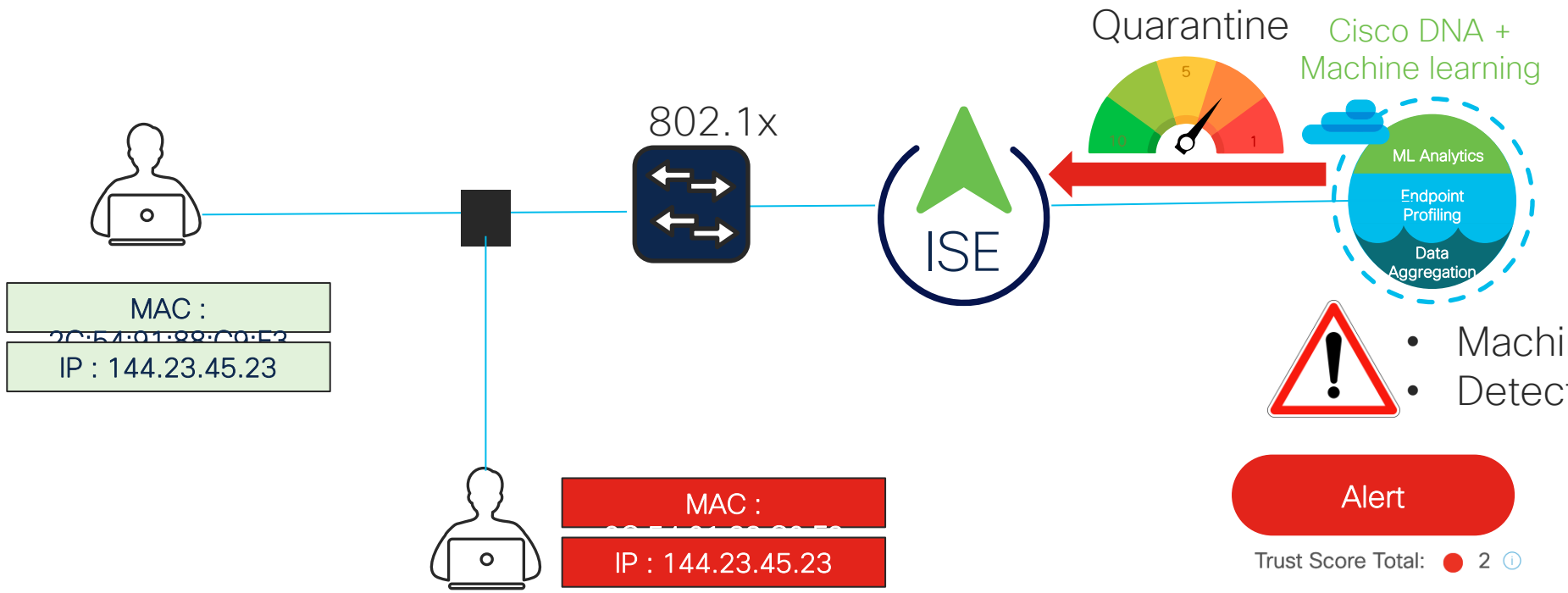


- DHCP class-ID change
- OS change

Mac & Attribute Spoofing



Men in the Middle Attack



- Machine learning
- Detect behavior change

Alert

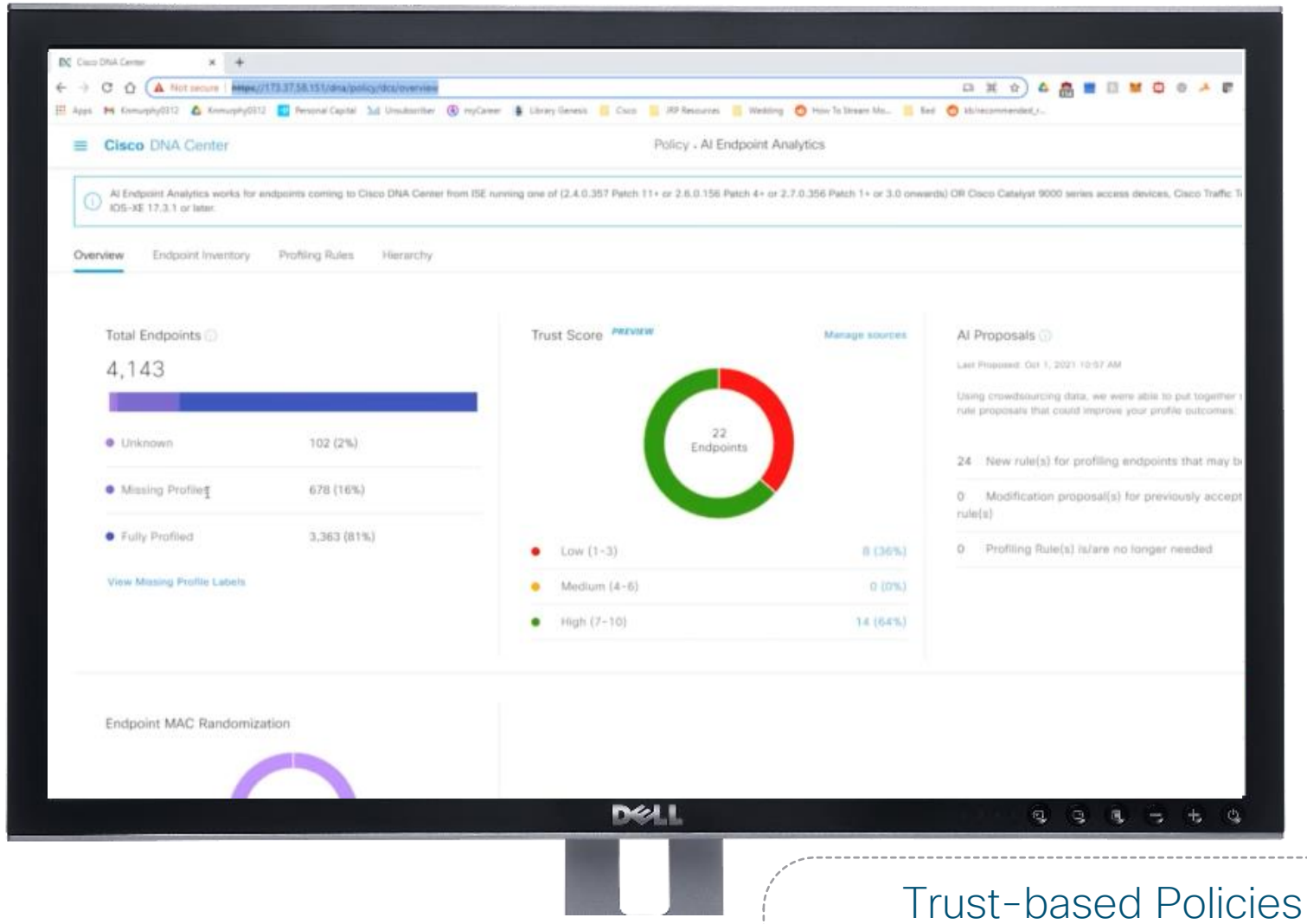
Trust Score Total: 2

Time ANC Policy Applied Sep 15, 2021 04:15 PM

> AI Spoofing Detection: 1

> Changed Profile Labels

> Concurrent MAC Address 3



High Trust (7-10)

Medium Trust (4-6)

Low Trust (1-3)

Trust-based Policies

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

TALOS integration: Detecting endpoint connections to low reputation sites.

DNAC 2.3.3

Use case

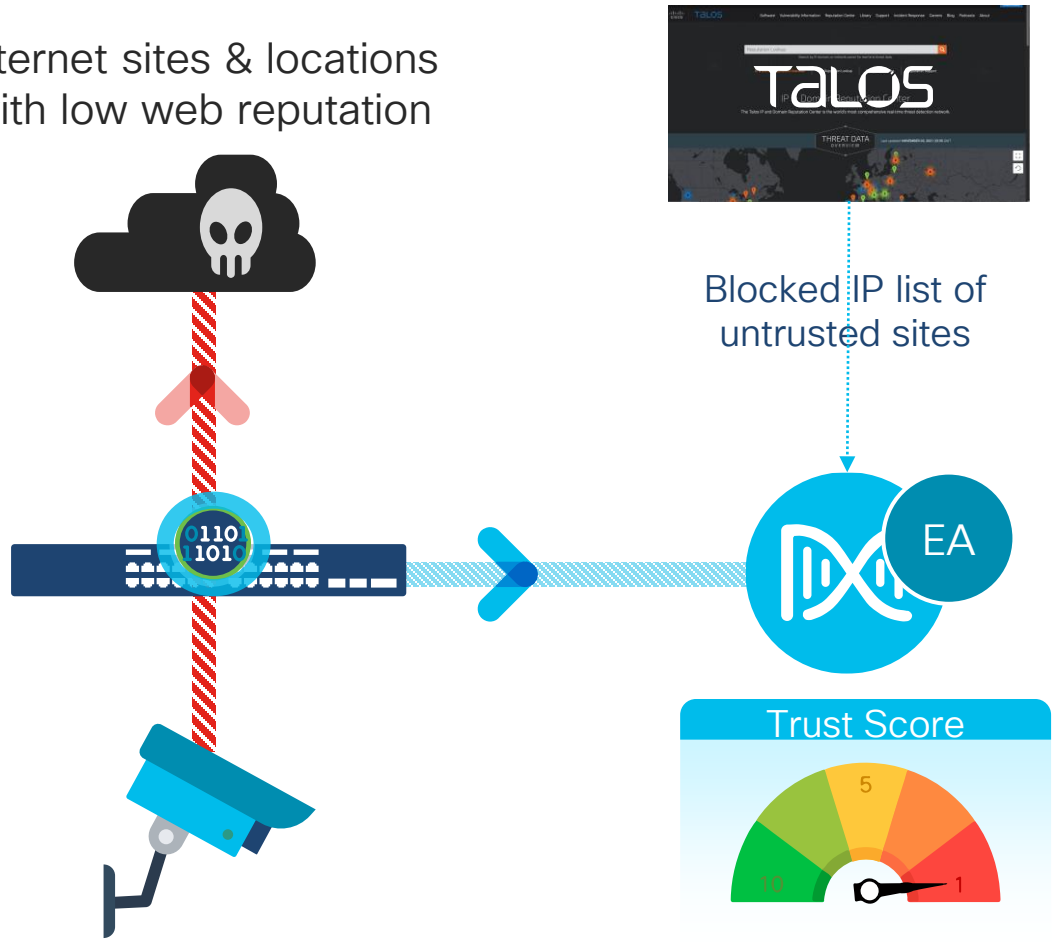
- Endpoints have unauthorized connections to bad reputed sites and and malicious IP's indicating anomalous behavior

Capability

- Cisco TALOS IP Reputation feature gets blocked list from TALOS to Endpoint Analytics to identify and alert admins of this behavior.

Considerations

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



Endpoint Analytics Compatibility Matrix

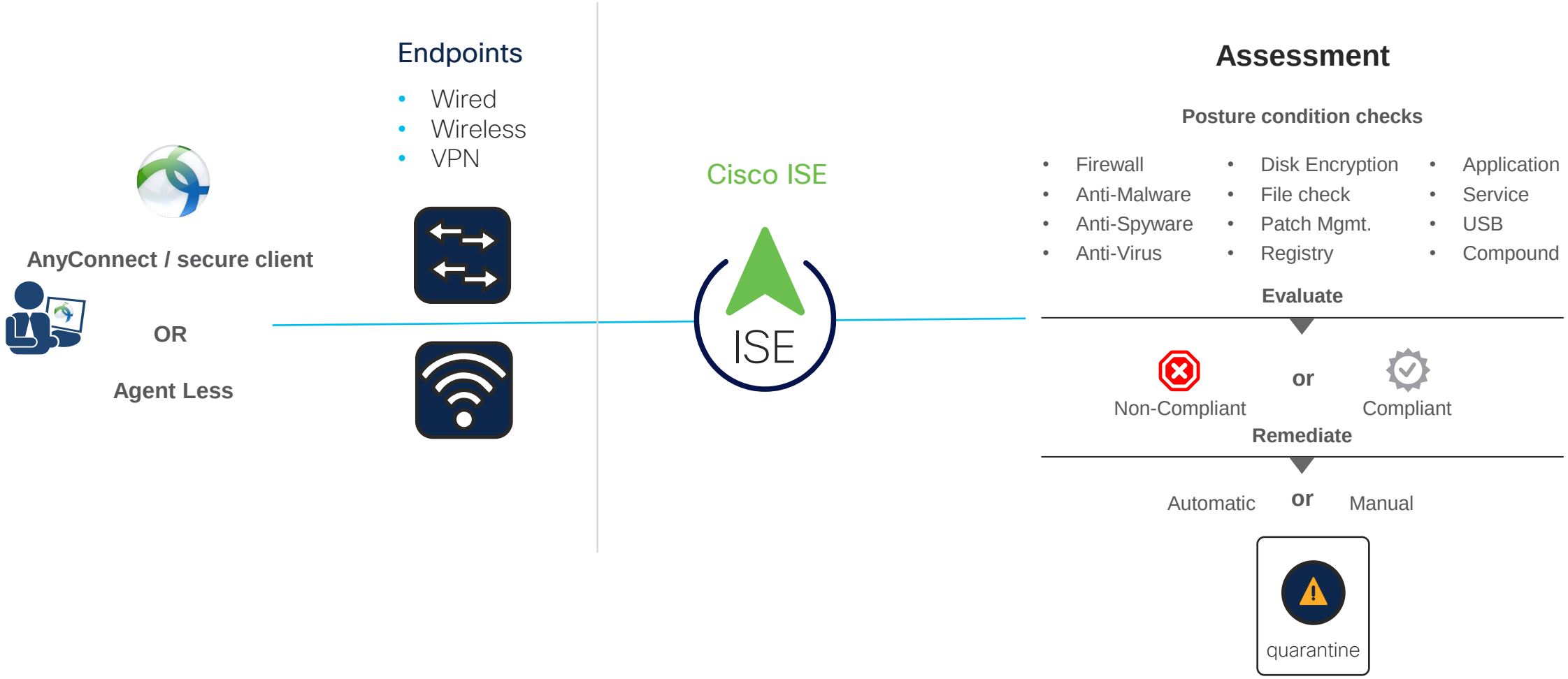
Capability	DNAC	Wired CAT9k		Wireless CAT9800 [4]		Traffic Telemetry Appliance (TTA)
		Fabric	Non-Fabric	Local	Flex	
DPI Based Profiling	2.1.2.x	✓	✓	✓	✓	✓
AI Smart Grouping	2.1.2.x	✓	✓	✓	✓	✓
AI Spoofing Detection[2]	2.2.2.x	✓	✓	✓	✓	✓
Anomalous profile change	2.2.3.x	✓	✓	✓	✓	✓
NAT Detection	2.2.3.x	✓	✓	✓	✓	✓
Concurrent MAC Detection	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

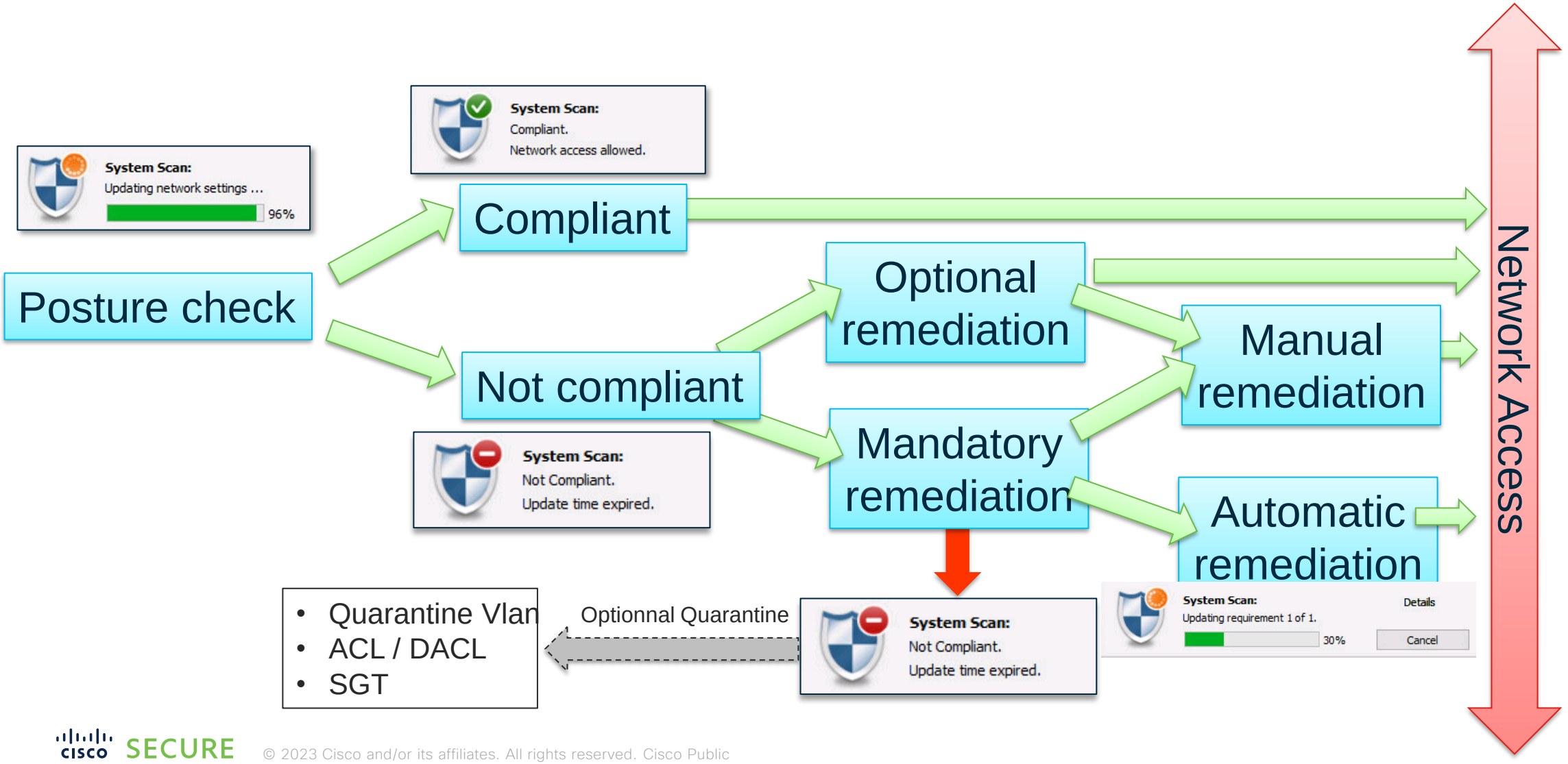
Agenda

- Introduction to NAC & 802.1x
- Authentication
- Authorization
- Guest Access
- Profiling
- Posture
- Threat centric NAC with Third party integration

USE case 5: posture assessment



Posture Flow with anyconnect / Secure Client

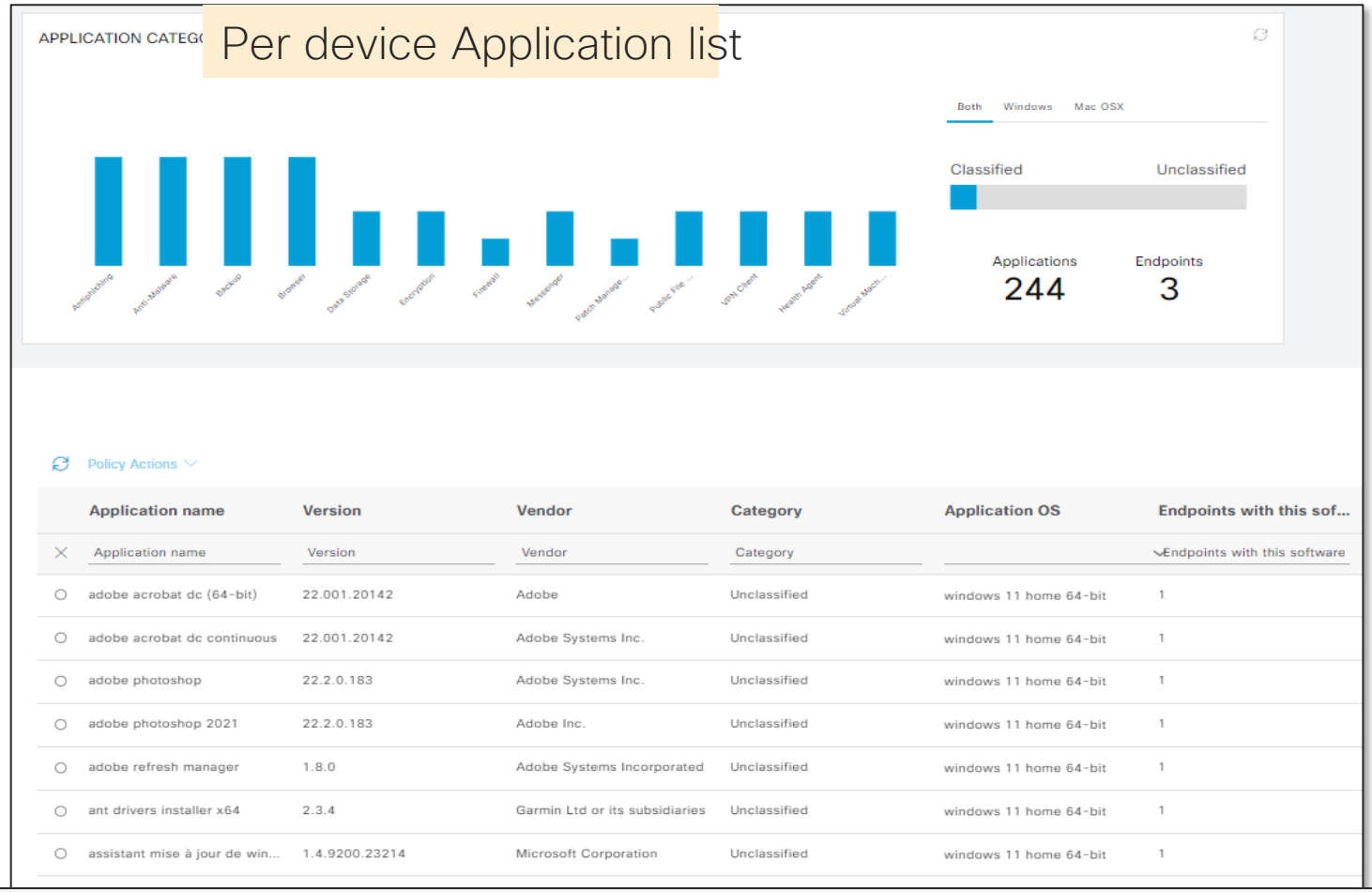


- Quarantine Vlan
- ACL / DACL
- SGT

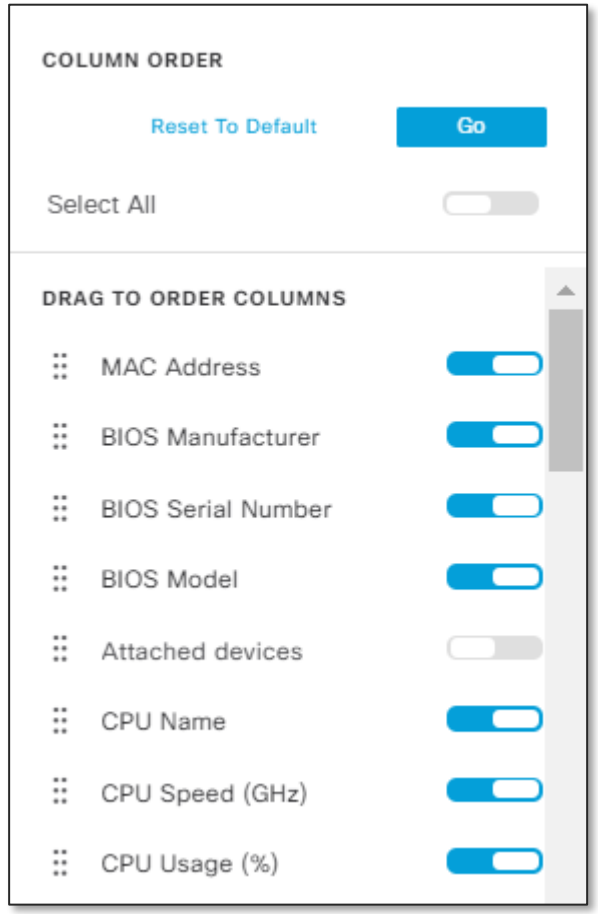
Agentless Posture

Application & HW visibility with posture

Per device Application list



Application name	Version	Vendor	Category	Application OS	Endpoints with this sof...
adobe acrobat dc (64-bit)	22.001.20142	Adobe	Unclassified	windows 11 home 64-bit	1
adobe acrobat dc continuous	22.001.20142	Adobe Systems Inc.	Unclassified	windows 11 home 64-bit	1
adobe photoshop	22.2.0.183	Adobe Systems Inc.	Unclassified	windows 11 home 64-bit	1
adobe photoshop 2021	22.2.0.183	Adobe Inc.	Unclassified	windows 11 home 64-bit	1
adobe refresh manager	1.8.0	Adobe Systems Incorporated	Unclassified	windows 11 home 64-bit	1
ant drivers installer x64	2.3.4	Garmin Ltd or its subsidiaries	Unclassified	windows 11 home 64-bit	1
assistant mise à jour de win...	1.4.9200.23214	Microsoft Corporation	Unclassified	windows 11 home 64-bit	1



MAC Address	BIOS Manufacturer	BIOS Serial Number	BIOS Model	CPU Name	CPU Speed (GHz)	CPU Usage (%)	Memory Usage(%)	Total Internal Disk(s) U...	UDID
00:0D:3A:0B:92:4E	Microsoft Corporation	0000-0006-2160-4329-87...	Virtual Machine	Intel(R) Xeon(R) Platinum 8...	2.594000	62.500540	43.828620	17.35558	509e772b78e26d02b1e656...
00:22:48:BB:B4:16	Microsoft Corporation	0000-0013-2878-7742-86...	Virtual Machine		2.594000	3.109140	60.133322	19.035036	ac019275f2f022f5549180f...
2C:F0:5D:3B:A0:E7	American Megatrends Inc.	MSB926K6S0103110	MEG Z490 Trident X (MS-B...		3.696000	0.356241	28.971839	72.16438	5007443aca3c11e69aac77...

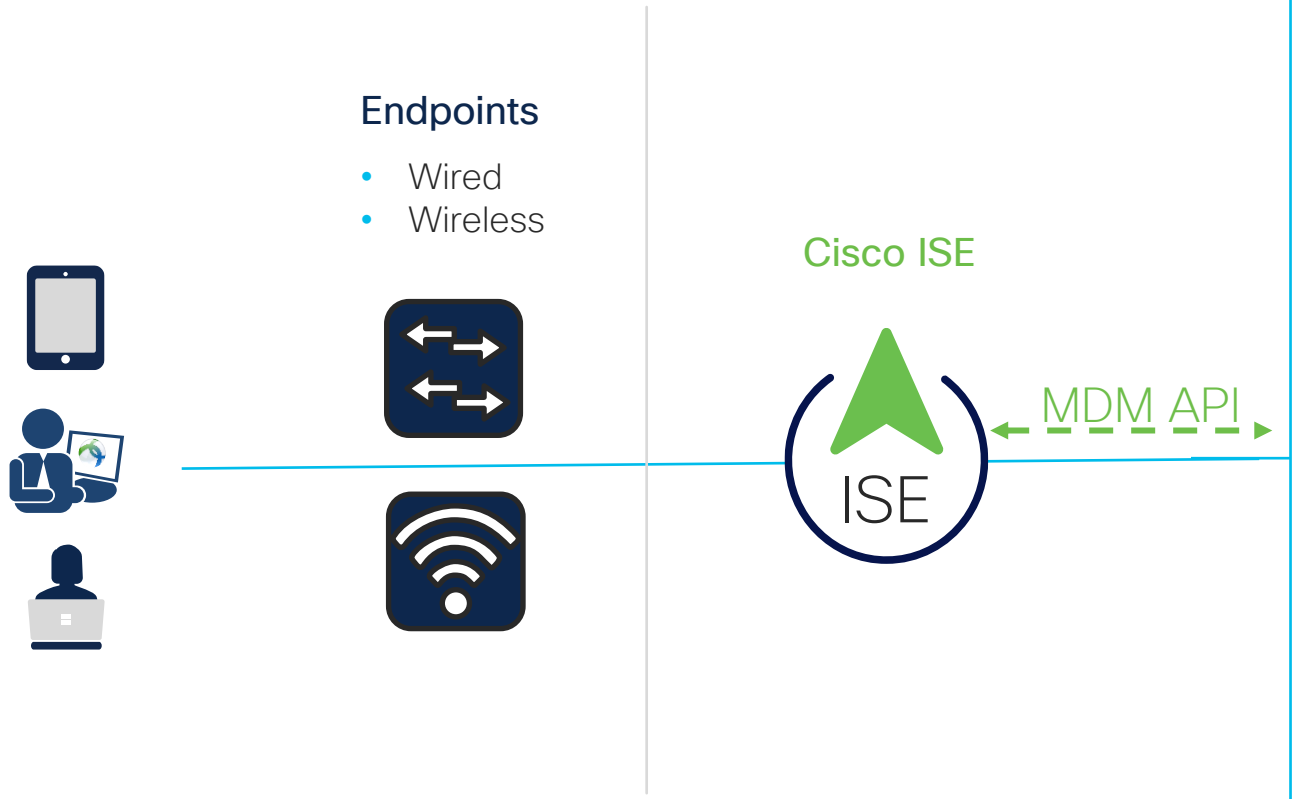
Per device HW detail

Posture Deployment Options

✓ Supported
! Limitations
✗ Not Supported

Capability	AnyConnect secure client			AC/SC Stealth		Temporal		Agentless	
	Windows	macOS	Linux	Windows	macOS	Windows	macOS	Windows	macOS
Anti-Malware Checks	✓	✓	✓	✓	✓	✓	✓	✓	✓
Firewall Installation Checks	✓	✓	!	✓	✓	✓	✓	✓	✓
Application Inventory	✓	✓	✓	✓	✓	✓	✓	✓	✓
Hardware Inventory	✓	✓	✗	✓	✓	✓	✓	✓	✓
Process Checks	✓	✓	✗	✓	✓	✓	✓	✓	✓
Dictionary Conditions	✓	✓	✗	✓	✓	✓	✓	✓	✓
Application Checks	✓	✓	✓	✓	✓	✓	✓	✓	✓
File Checks	✓	✓	✓	✓	✓	✓	✓	!	✓
Service Checks	✓	✓	✓	✓	✓	✓	!	✓	!
Disk Encryption	✓	✓	✗	✓	✓	!	!	!	!
Patch Management	✓	✓	✓	✓	✓	!	!	!	!
Registry Checks	✓	N/A	N/A	✓	N/A	✓	N/A	!	N/A
USB Checks	✓	✗	✗	✓	✗	✓	✗	✓	✗
Custom Posture Script	✓	✓	✓	✓	✓	✗	✗	✗	✗
Custom Remediation Script	✓	✓	✓	✓	✓	✗	✗	✗	✗
Remediation	Auto, Manual	Partial	Auto (script)	Part Auto	Partial	Text	Text	✗	✗
Reassessment	✓	✓	✓	✓	✓	✗	✗	✗	✗

USE case 6: MDM integration



AbsoluteSoftware
SOPHOS
GLOBO
IBM Security
Microsoft
SOTI
tangoe
cisco Meraki
citrix XenMobile
jamf
SAP
MobileIron
Symantec.
airwatch by vmware

MDM Attributes

ActivityType
AdminAction
AdminActionUUID
AnyConnectVersion
DaysSinceLastCheckin
DetailedInfo
DeviceID
DeviceName
DeviceType
DiskEncryption
EndPointMatchedProfile
FailureReason
IdentityGroup
IMEI
IpAddress
JailBroken
LastCheckInTimeStamp
MacAddress
Manufacturer
MDMCompliantStatus
MDMFailureReason
MDMServerName
MEID
Model
OperatingSystem
PhoneNumber
PinLock
PolicyMatched
RegisterStatus
SerialNumber
ServerType
SessionId
UDID
UserName
UserNotified

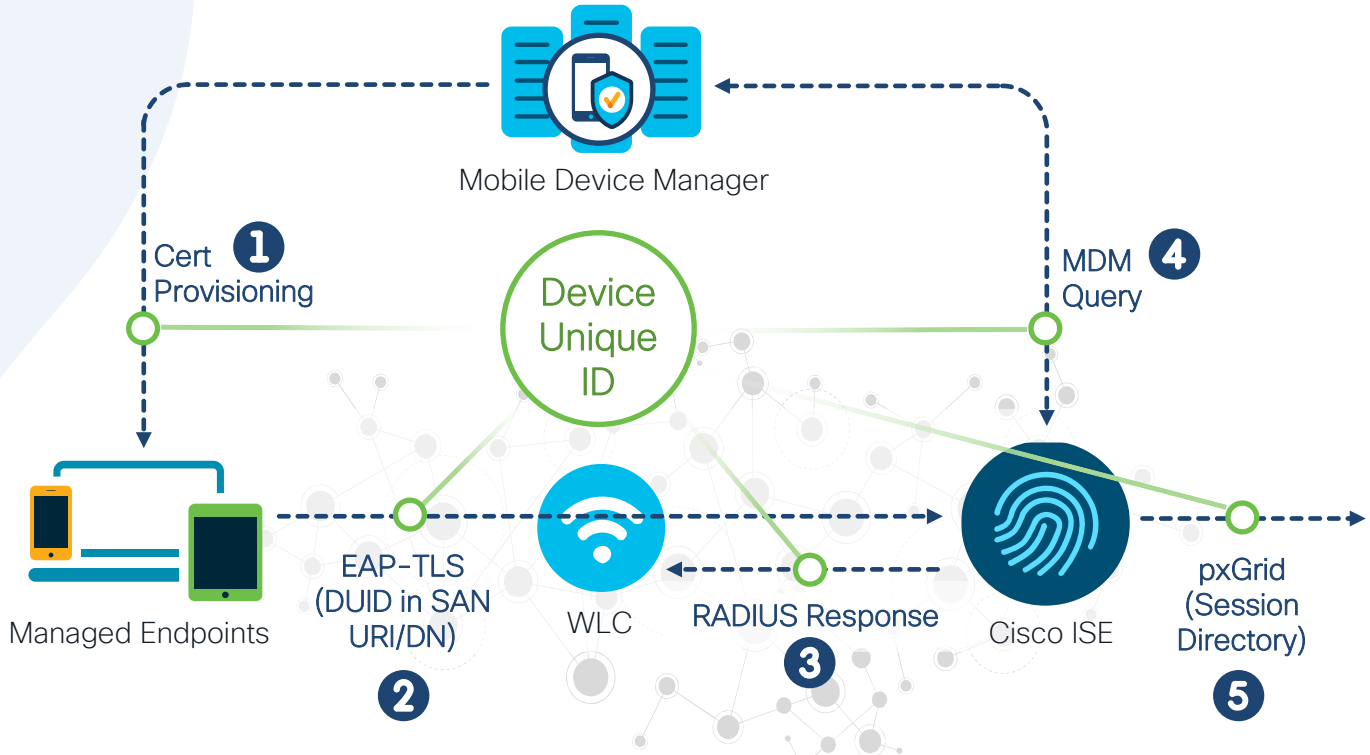
Visibility and compliance for devices with Randomized MAC addresses

Problem

Latest endpoint OSs randomize device MAC address as they connect to the network. As a result, MDM compliance check and other security controls fail because of unrecognized private MAC addresses as device identifiers.

Solution

Managed assets are provisioned with client certificates with unique device identifier which is used for NAC services.



"Device Unique Identifier" (DUID)
as the policy anchoring point instead of MAC addresses

DUID/GUID terms used interchangeably

Agenda

- Introduction to NAC & 802.1x
- Authentication
- Authorization
- Guest Access
- Profiling
- Posture
- Threat centric NAC with Third party integration

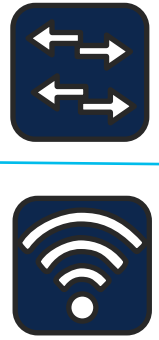
USE case 7: Third Party security solutions integration

Endpoints

- Users
- Devices
- Things

Endpoints

- Wired
- Wireless



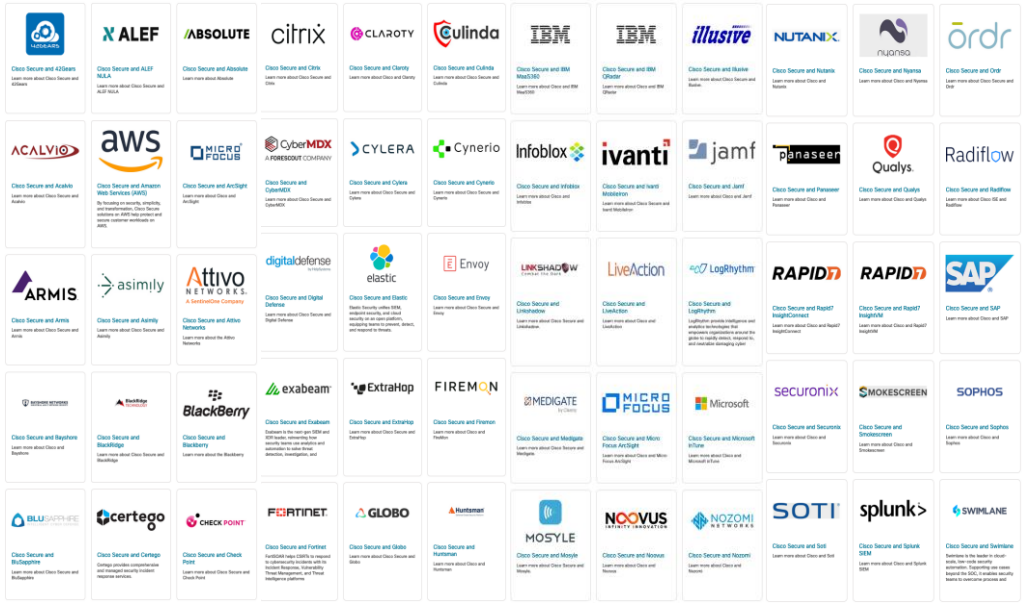
Cisco ISE

Context

- Who
- What
- When
- How
- Where
- Posture
- Threat
- Vulnerability

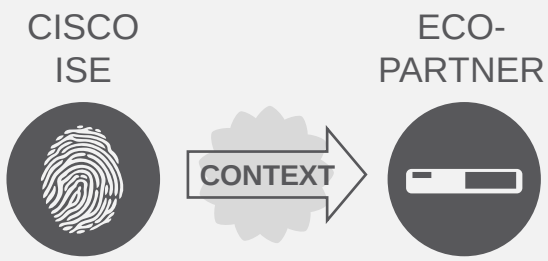
PxGrid API

3rd Party Security solutions



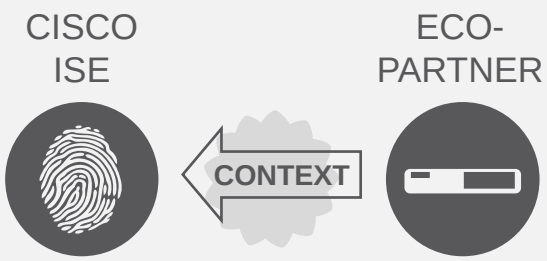
pxGrid enables these 4 scenarios

CONTEXT TO PARTNER



ISE makes Customer IT Platforms User/Identity, Device and Network Aware

ENRICH ISE CONTEXT

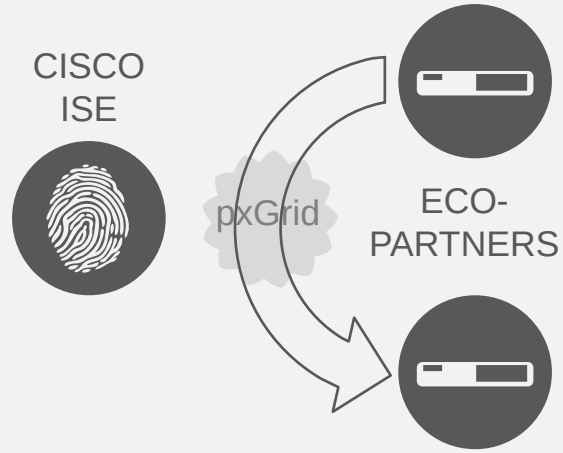


Enrich ISE context. Make ISE a better Policy Enforcement Platform

THREAT MITIGATION

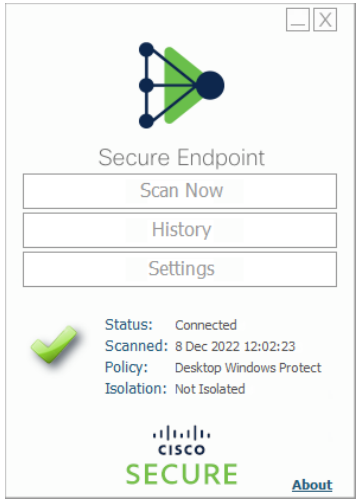
Enforce dynamic policies in to the network based on Partner's request

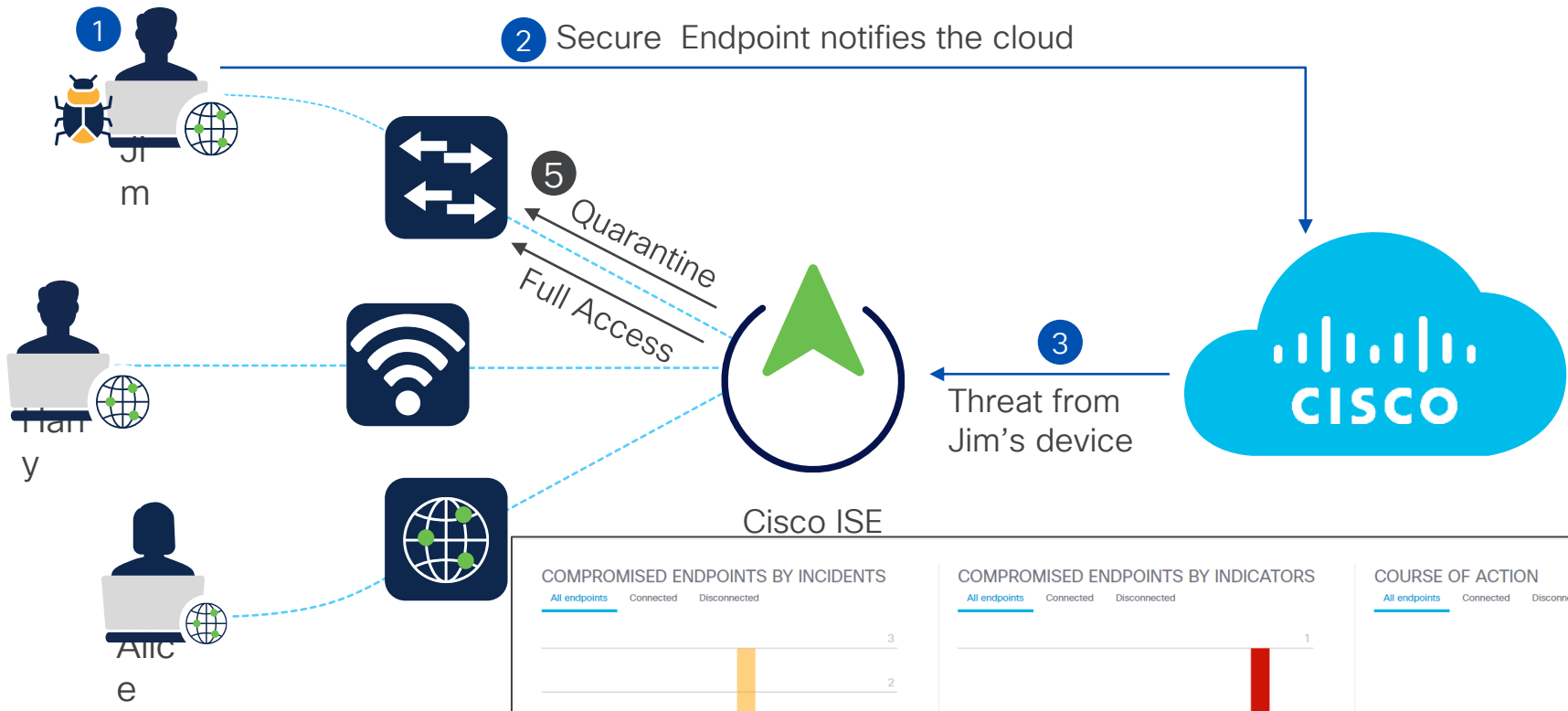
CONTEXT BROKERAGE

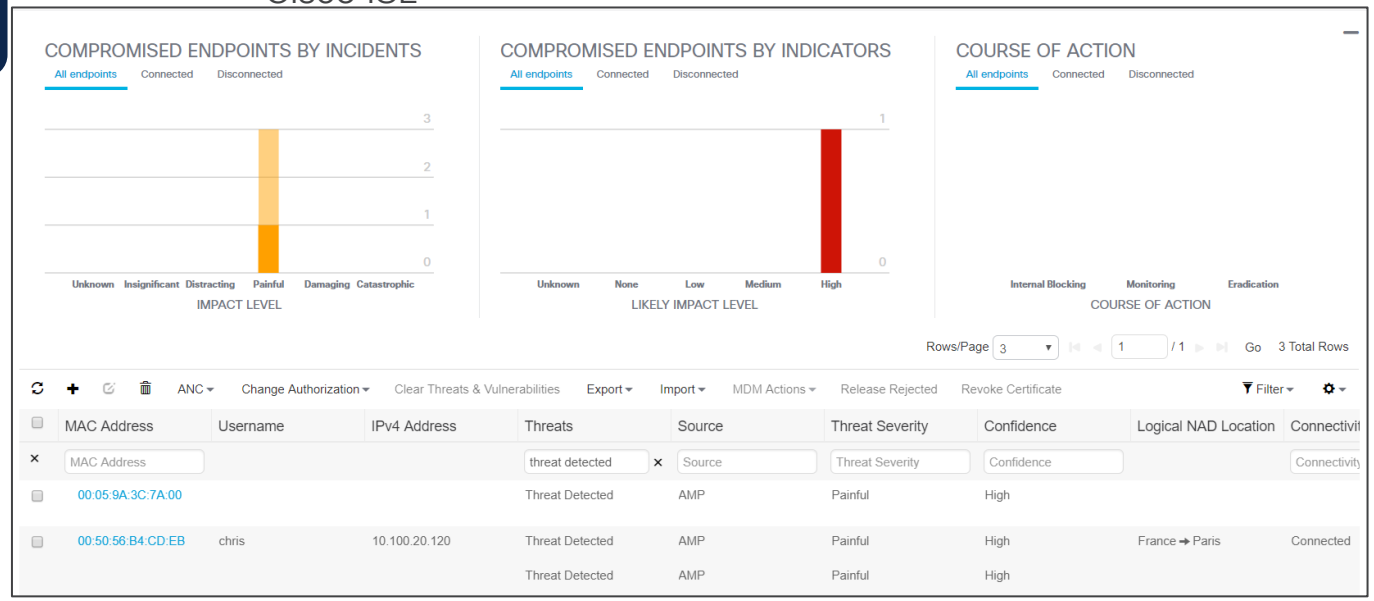


ISE brokers Customer's IT platforms to share data amongst themselves

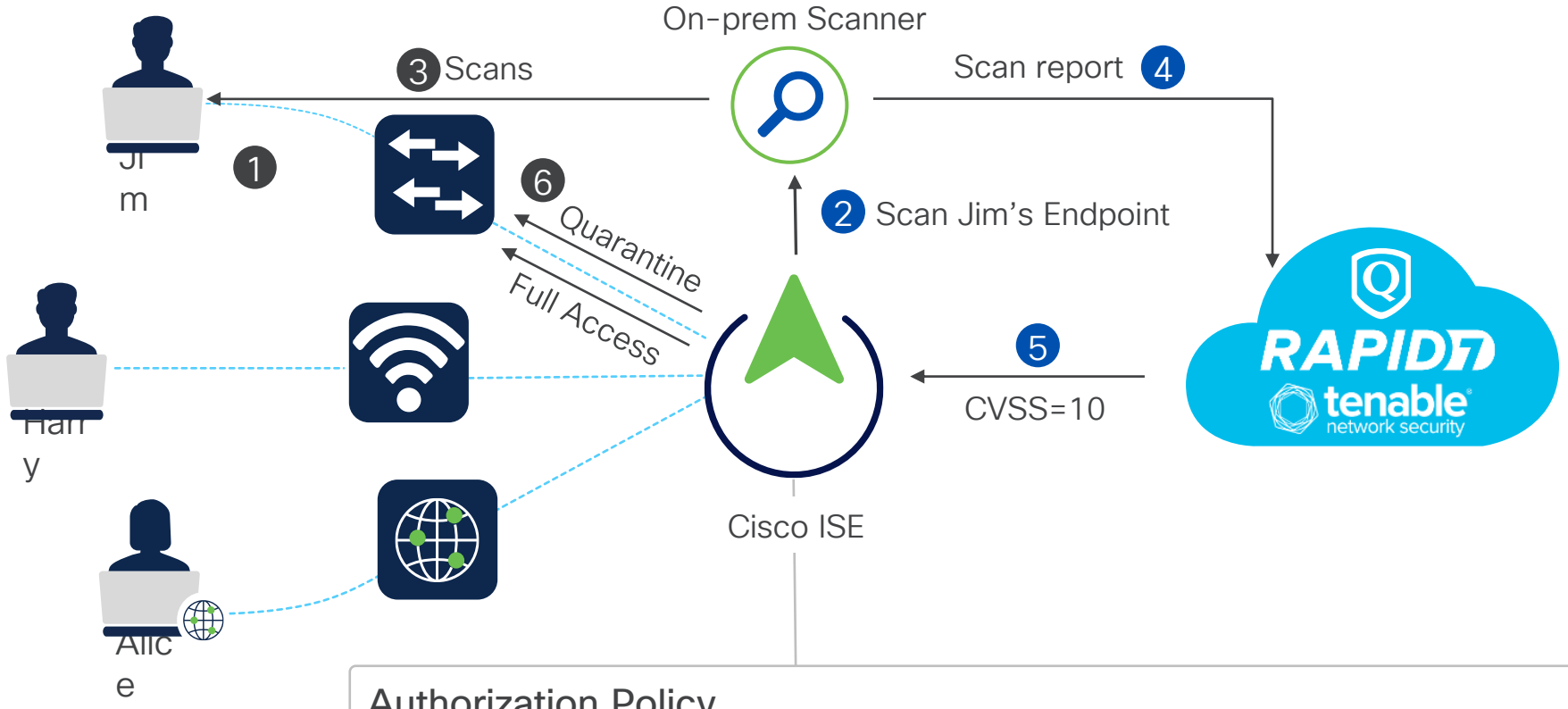
ISE Continuous trust: threat centric with secure endpoint







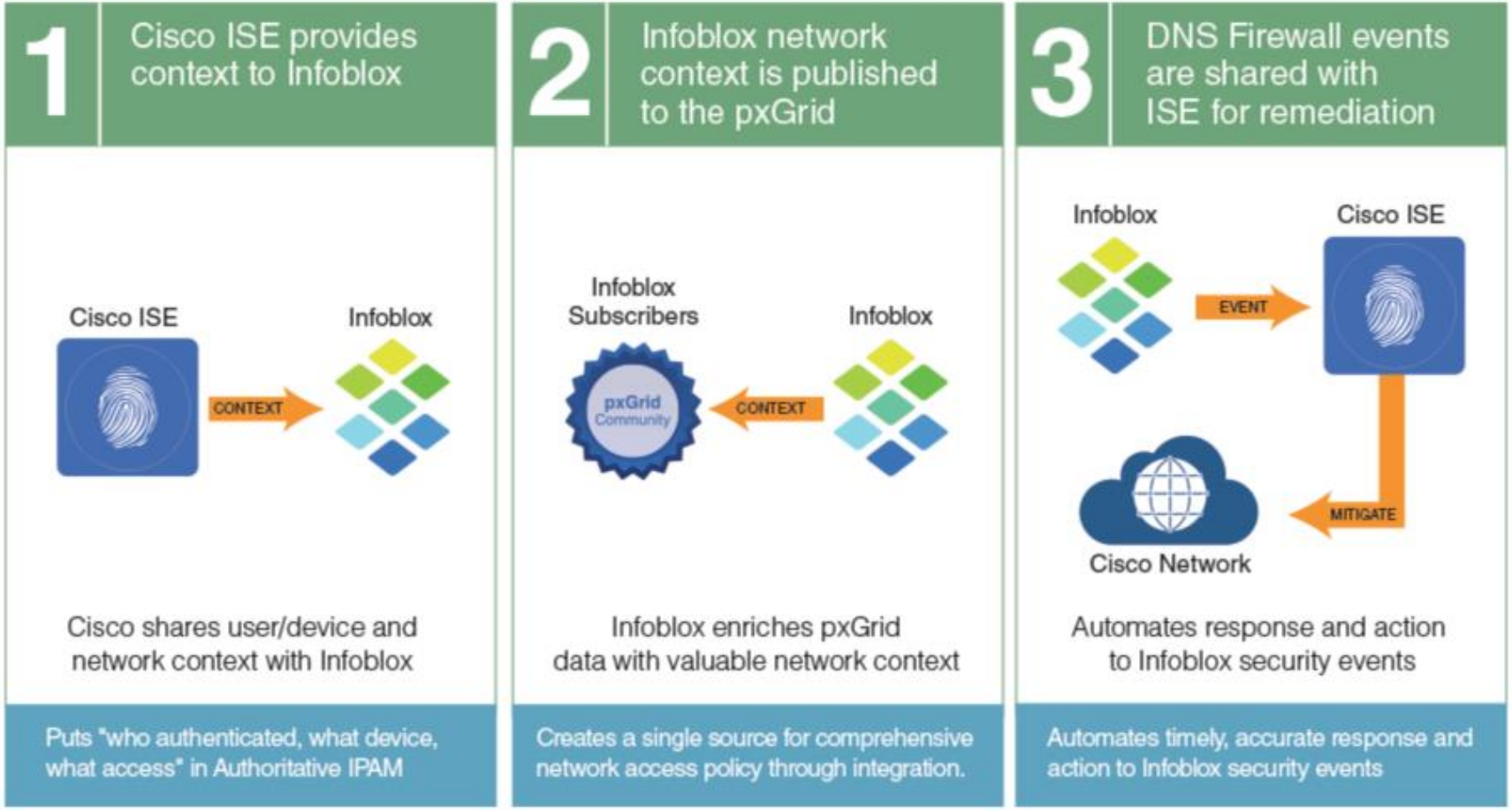
Continuous trust based on Vulnerability Assessment



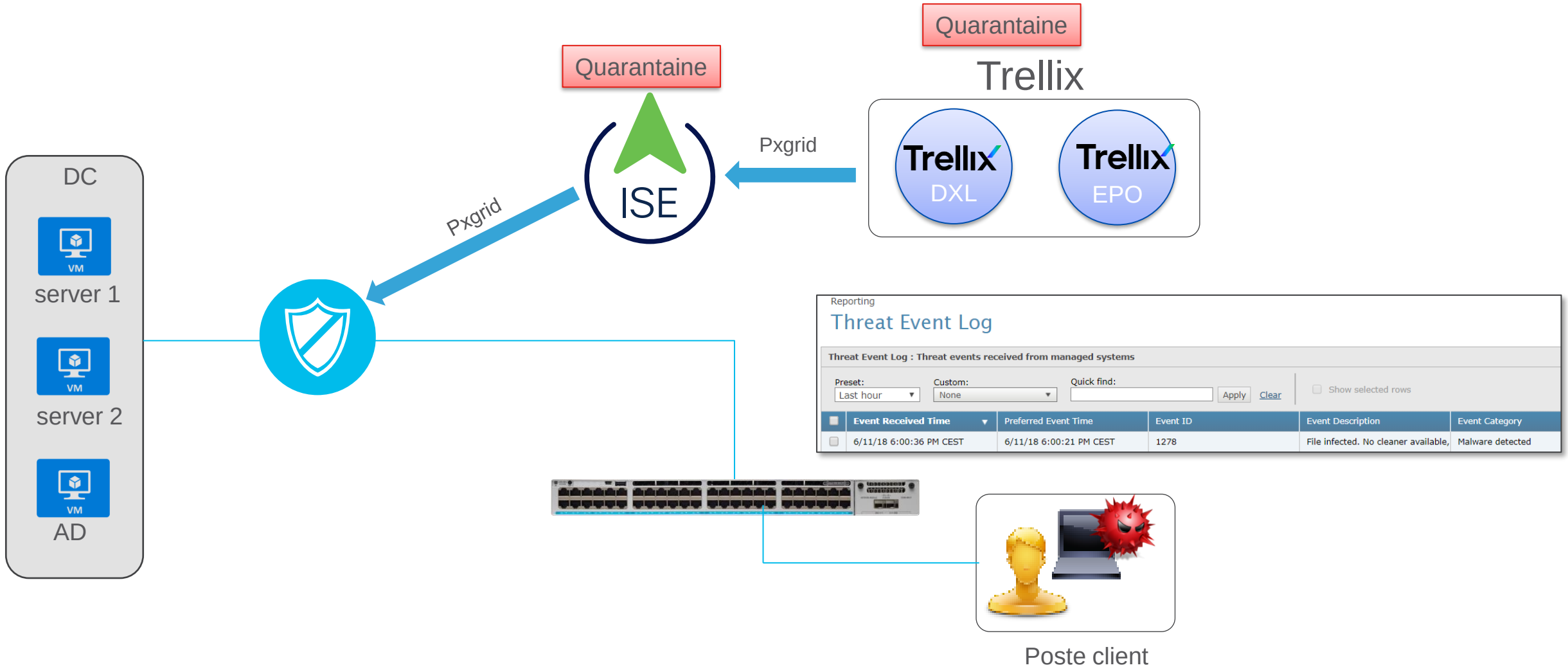
CVSS: Common Vulnerability Scoring System

Example of Infoblox PxGRID integration

- Context based IPAM: IP address management with user and device context.
  "Who has that IP last Tuesday?"
- Threat containment: Infoblox detects suspicious DNS resolutions and requests ISE quarantine over ANC



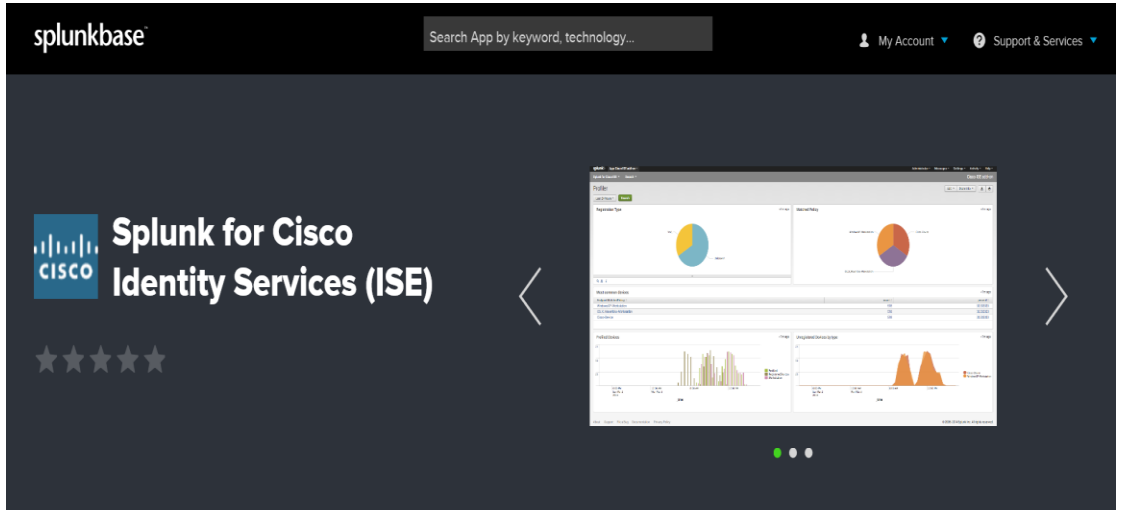
Example of Trellix & third party Firewall integration



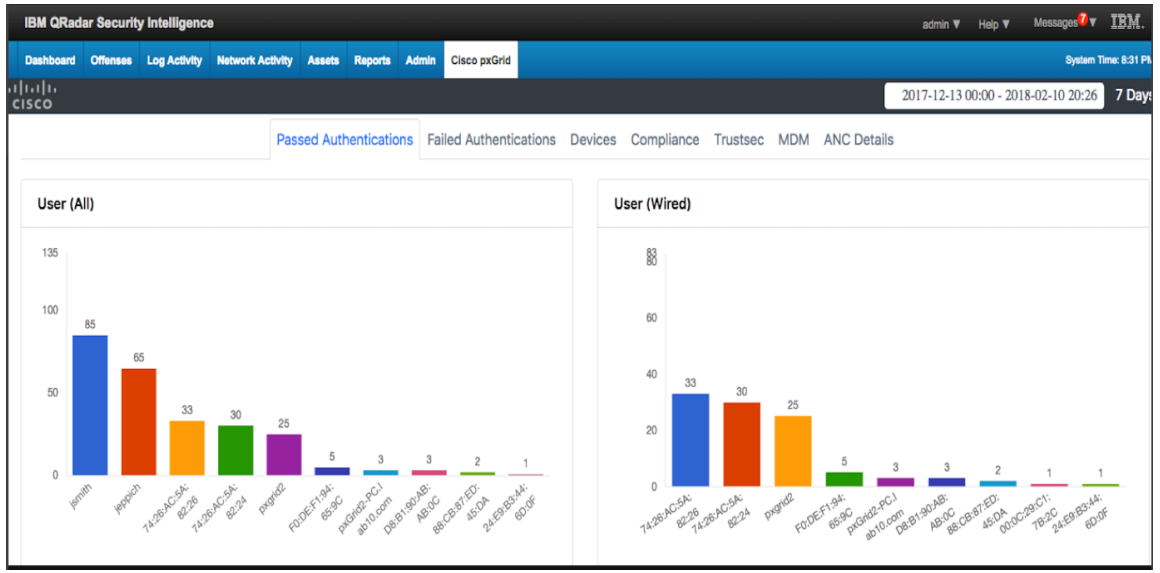
Example of SIEM Integration

SPLUNK & QRADAR

Download from Spluk APP Store : https://splunkbase.splunk.com/app/1589/

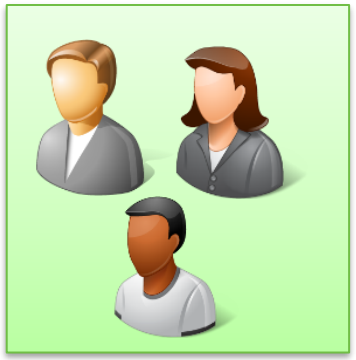


Download from IBM Qradar APP store



https://exchange.xforce.ibmcloud.com/hub/extension/6091fd93042043212fd2494fe97ff5b7

NAC need to trust all context



Users and guests

Localizations

Devices

Applications

Posture

Threats & vulnerability

Network Access Devices

Zero Trust & NAC

Authenticate user and device trust across wired, wireless, & VPN networks

1. User/Device requests network access
2. User/Device is authenticated, role is verified
3. Device posture is checked and verified - User/Device Trust level is established

Strong Security

- **Authenticate seamlessly** - Gain global awareness with both cloud and on-prem identity stores using standard protocols (e.g., EAP-based)
- **Secure BYOD/MDM** with device posture assessment for managed and unmanaged devices
- **Balance risk with flexible access** - Identify devices managed/unmanaged, BYOD/MDM, Guest/Visitors to align access based on need

High Productivity

- **Simplify and automate** guest and contractor access based on business need (e.g., ISE Is a RADIUS, TACACS AAA server)
- **Automatically detect,** identify, and categorize devices connecting to the network including IoT / OT
- **Accelerate and unify** network access policy across the distributed global network with NAC from the cloud

SECURE

Avez-vous des questions ?

Si vous avez posé une question sur le panneau de Q&R (Q&A en anglais) ou que vous revenez sur la communauté dans les jours qui suivent notre webinaire, nos experts peuvent encore vous aider !

Participez dans le forum de Ask Me Anything (AMA) avant le 17 février 2023

https://bit.ly/AMA-mar23

Faites valoir votre opinion

Répondez à notre enquête pour...

- Proposer des nouveaux sujets
- Évaluer nos experts et contenus
- Envoyer vos commentaires ou suggestions

Cliquez sur le lien

https://bit.ly/WEBenq-mar23

Nos réseaux sociaux

LinkedIn

Cisco Community

Twitter

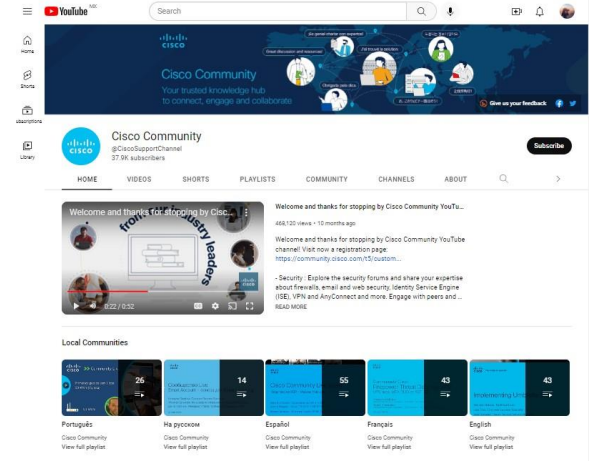
@CiscoCommunity

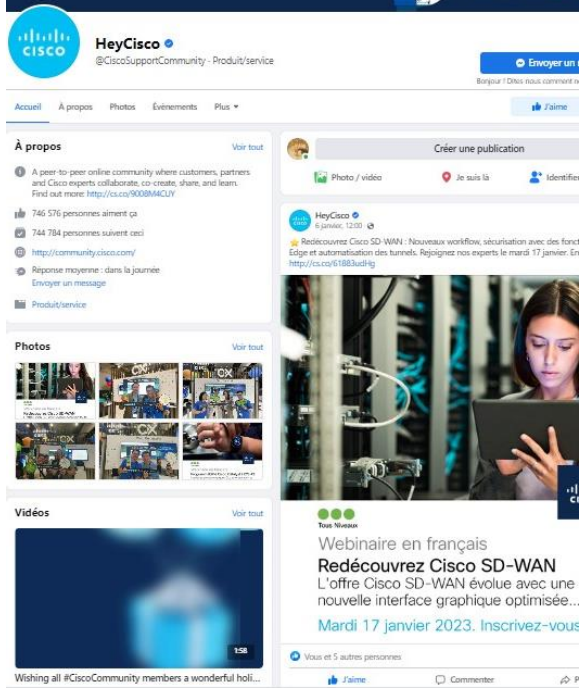
YouTube

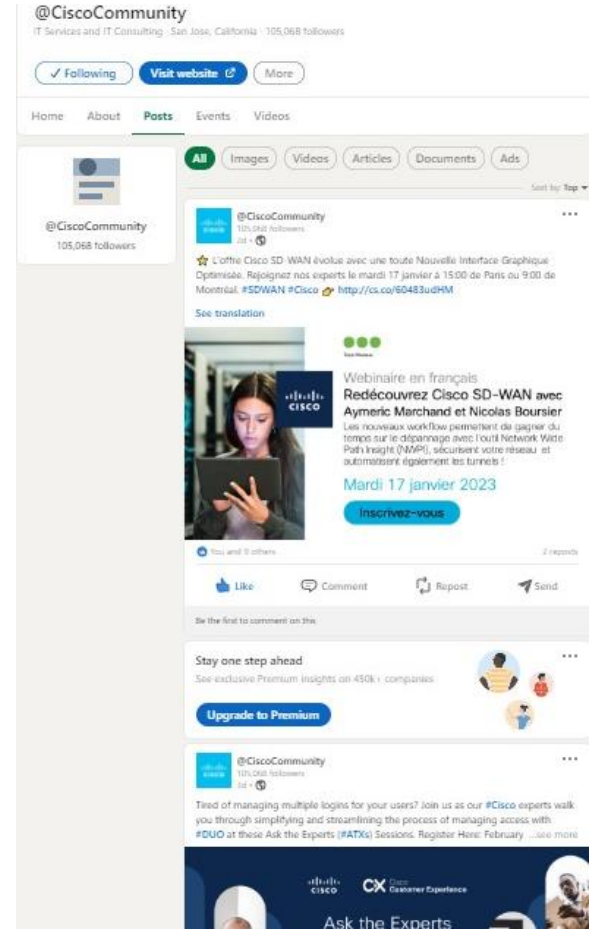
CiscoCommunity

Facebook

CiscoCommunity







The bridge to possible