

# Automating Access with ISE



# Agenda

1. Introduction to ISE
2. Network Access Control
3. Profiling Endpoints
4. Posturing for Compliance
5. Segmentation
6. Integrations to Automate Policy

# Introduction to ISE

# A little about me



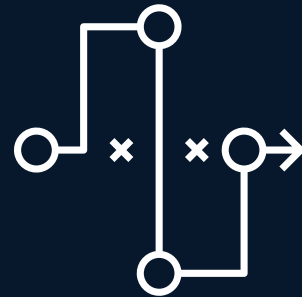
- Started as an early ISE 1.1 customer
- 15+ years of networking & security experience
- Lots of paper: BS and MS in IT Security, 2x CCIE (Data Center + Security), CISSP, and various other industry certifications
- Co-authored recent CiscoPress SISE book
- Co-organize for the largest Cisco Meetup study group – Router gods and owner of network-node blog

# The Foundations of Zero Trust in Your Workplace



## Visibility

Identify your trusted endpoints, users, and applications.



## Segmentation

Grant access to trusted subjects based on principle of least privilege



## Containment

Continuously verify behavior and automate containment of with a change of authorization

# ISE Capabilities for Zero Trust



## Establish Trust

- User & Endpoint Authentication
- MFA with Duo
- pxGrid Context-In
- Profiling
- Posture
- Guest
- BYOD



## Enforce Trust-Based Access

- Network based Authorization Policies
- Micro-segmentation
- pxGrid Context Out
- Device Administration with TACACS+



## Continuously Verify Trust

- Integrations for Threat Detection
- Behavior Analysis
- Vulnerability Assessment



## Respond to Change in Trust

- Rapid Thread Containment (RTC)
- Threat-Centric NAC (TC-NAC)
- Orchestrated Remediation (CoA)

# The Swiss Army Knife of Network Access Control



Device Administration	 <p><b>TACACS+</b> Migrating from Cisco Secure ACS or building a new Device Administration Policy Server, this allows for secure, identity-based access to the network devices</p>
Secure Access	 <p>Allow wired, wireless, or VPN access to network resources based upon the identity of the user and/or endpoint. Use <b>RADIUS</b> with <b>802.1X</b>, <b>MAB</b>, <b>Easy Connect</b>, or <b>Passive ID</b></p>
Guest Access	 <p>Differentiate between <b>Corporate and Guest</b> users and devices. Choose from Hotspot, Self-Registered Guest, and Sponsored Guest access options</p>
Asset Visibility	 <p>Use the probes in ISE and Cisco network devices to classify endpoints and authorize them appropriately with <b>Device Profiling</b>. Automate access for many different IoT devices</p>
Compliance & Posture	 <p>Use <b>agentless posture</b>, <b>Cisco Secure Client</b>, <b>MDM</b>, or <b>EMM</b> to check endpoints to verify compliance with policies (Patches, AV, AM, USB, etc.) before allowing network access</p>
Context Exchange	 <p><b>pxGrid</b> is an ecosystem that allows any application or vendor to integrate with ISE for endpoint identity and context to increase <b>Network Visibility</b> and facilitate automated Enforcement.</p>
Segmentation	 <p><b>Group-based Policy</b> allows for segmentation of the network through the use of Security Group Tags (SGT) and Security Group ACLs (SGACL) instead of VLAN/ACL segmentation.</p>
Cisco SDA/DNAC	 <p>ISE integrates with <b>DNA Center</b> to automate the network fabric and enforces the policies throughout the entire network infrastructure using Software-Defined Access (SDA)</p>
BYOD	 <p>Allow employees to use their own devices to access network resources by registering their device and downloading certificates for authentication through a simple <b>onboarding</b> process</p>
Threat Containment	 <p>Using a <b>Threat Analysis</b> tool, such as Cisco Cognitive Threat Analytics, to grade an endpoints threat score and allow network access based upon the results</p>

# Network Access Control

# ISE Provides Zero Trust for the Workplace

## Enterprise

### Endpoints

- Users
- Devices
- Things
- 5G



### Network Devices

- Switches
- WLCs / APs
- VPN



### Cisco ISE

- Shared or Distributed
- VM/Appliance/Cloud
- Up to 2M Endpoints
- RADIUS and TACACS



## Security

### Identity Services

- Entra, AD
- LDAP, ODBC
- MDM
- SAML/MFA



### Security Services

- Cloud Analytics
- Secure Firewall
- Partners

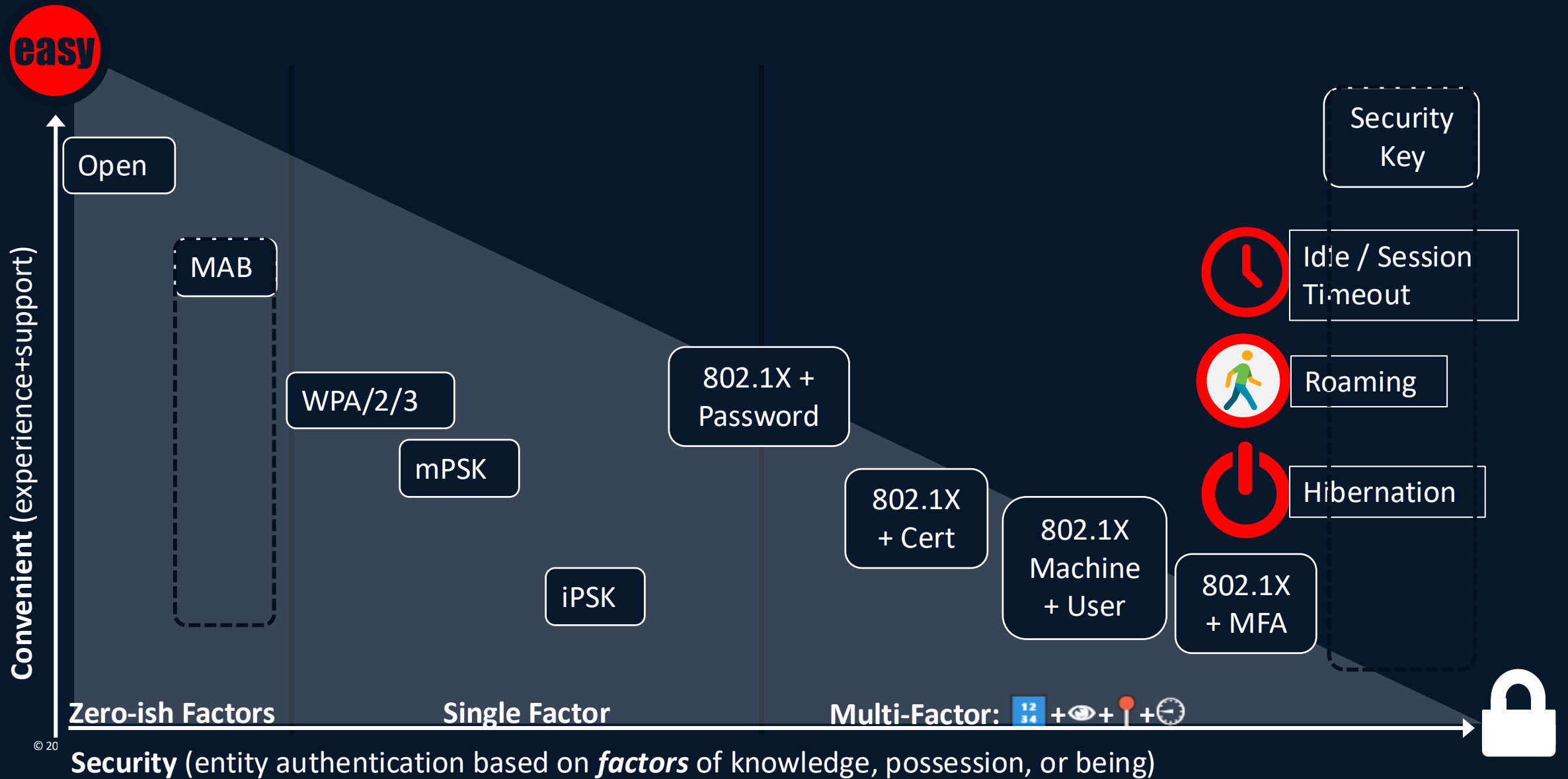


Visibility

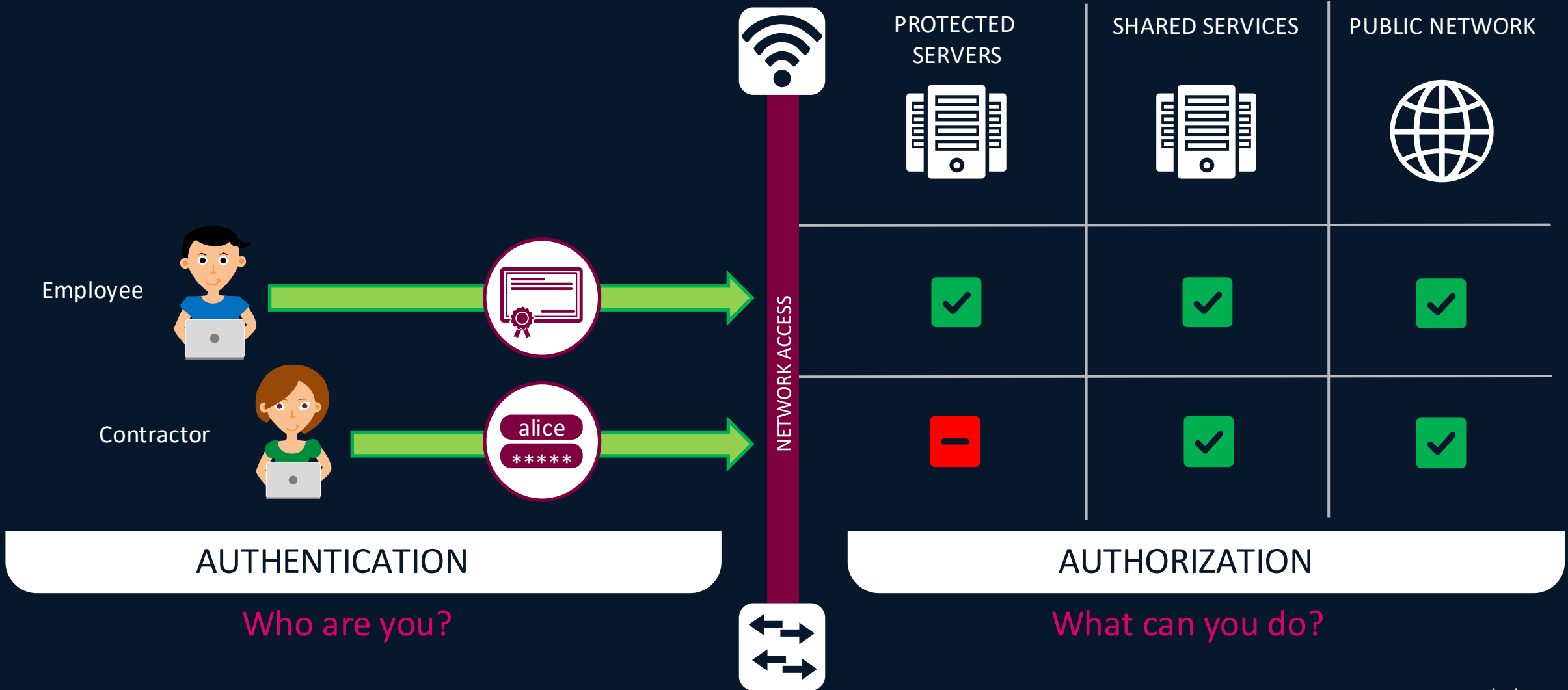
Segmentation

Containment

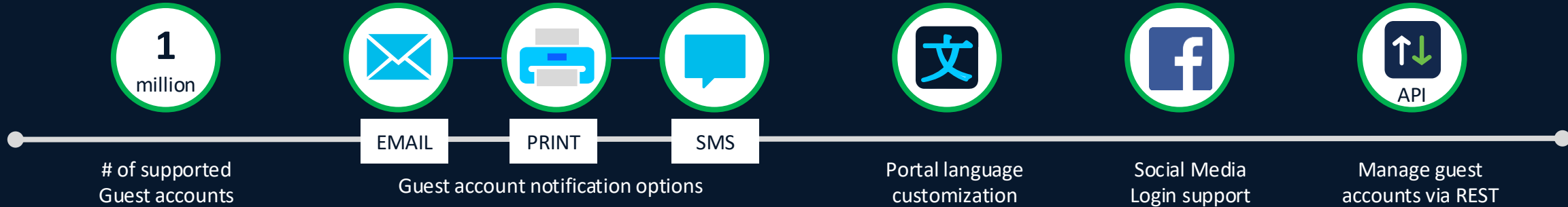
# Network Access Authentication is a Spectrum



# Authentication and Authorization



# Guest Solution Overview



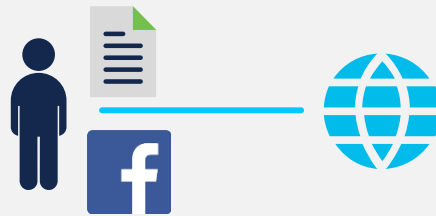
## The 3 types of guest access

### Hotspot



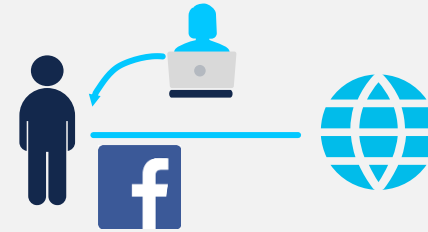
Immediate, un-credentialed Internet access

### Self Registered



Self-registration by guests, Sponsors may approve access

### Sponsored Guest Access



Authorized sponsors create account and share credentials

# ISE BYOD / EMM / MDM Solutions

EMM: Enterprise Mobility Management | MDM: Mobile Device Management

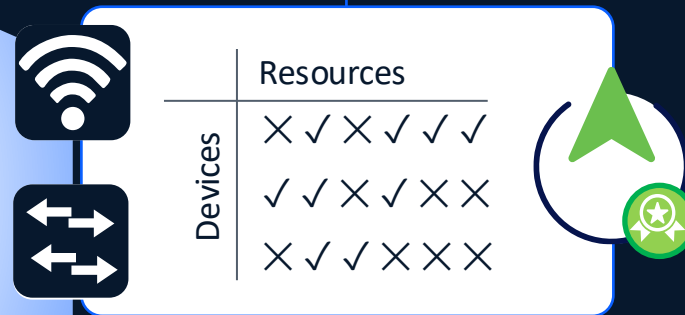
## Device Support

-  iDevice
-  Android
-  macOS
-  Windows
-  ChromeOS

Public

Single / Dual SSID provisioning

MDM policy-based Access



Native supplicant & cert provisioning

Corporate

ISE internal CA for BYOD certificates

 [cisco.com/go/csta](https://cisco.com/go/csta)

Absolute Software

SOPHOS

GLOBO

IBM Security

Microsoft

SOTI

tangoe

CISCO Meraki

CITRIX XenMobile

jamf

SAP

MobileIron

Symantec

airwatch by vmware

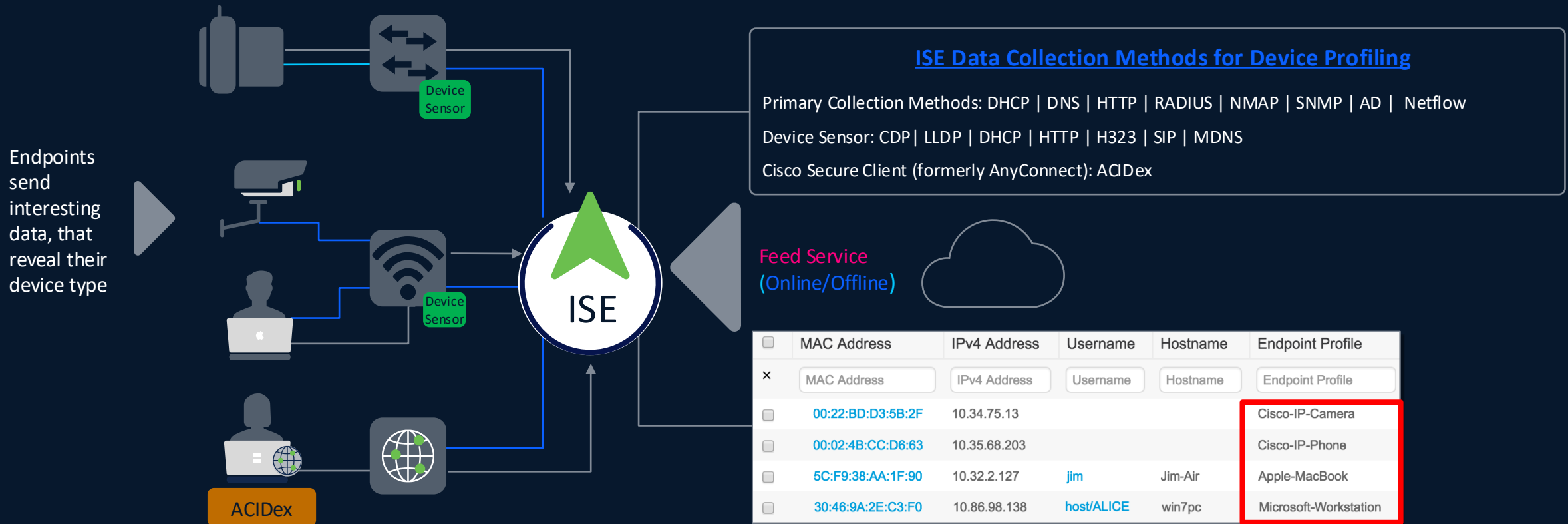
## MDM Attributes

- 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

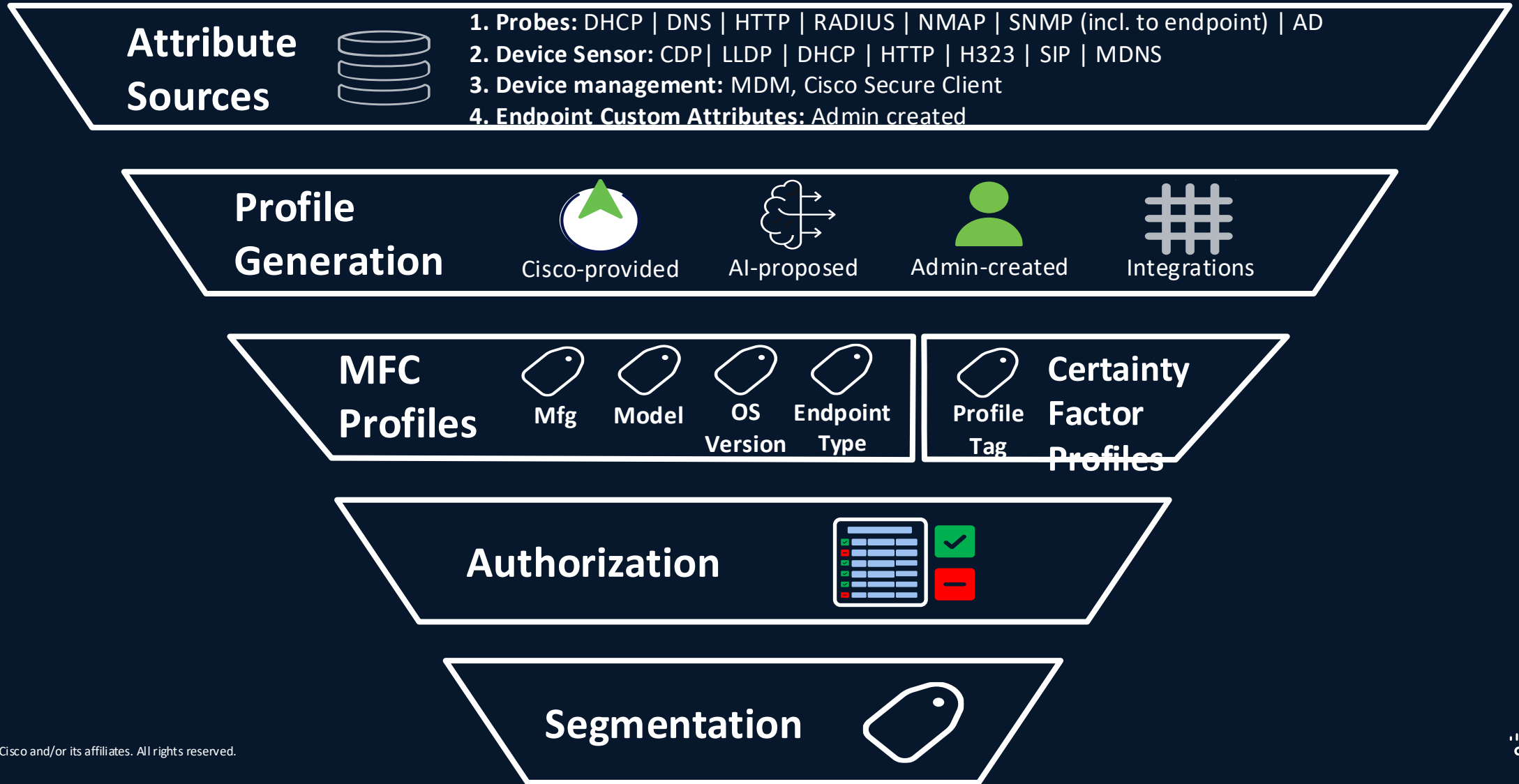
# Profiling Endpoints

# Endpoint Profiling

The profiling service in Cisco ISE identifies the devices that connect to your network



# Turing Attributes into Profiles, Profiles into Protection




# Cisco AI Analytics

Identity Services Engine Work Centers / Profiler Evaluation Mode 89 Days

Overview Ext Id Sources Network Devices Endpoint Classification Node Config Feeds Manual Scans Policy Elements More

Profiler Settings  
NMAP Scan Subnet Exclusions  
Cisco AI Analytics

 To configure Cisco AI Analytics, you must enable pxGrid Services on at least one node in your Cisco ISE deployment. Click [here](#) to see the nodes in your deployment enable pxGrid Services. Come back here to refresh.


## Cisco AI Analytics <sup>BETA</sup>


### ENDPOINT SMART GROUPING


Using AI and machine learning, Endpoint Smart Grouping reduces the number of unknown endpoints in the network by providing AI-based endpoint groupings, automated custom profiling rules, and suggested endpoint labels.


See the [AI Analytics Privacy Data Sheet](#) for details on how Cisco AI Network Analytics stores and processes data.

AI Analytics is governed by the [Cisco End User License Agreement](#). Check [Cisco Privacy Statement](#).

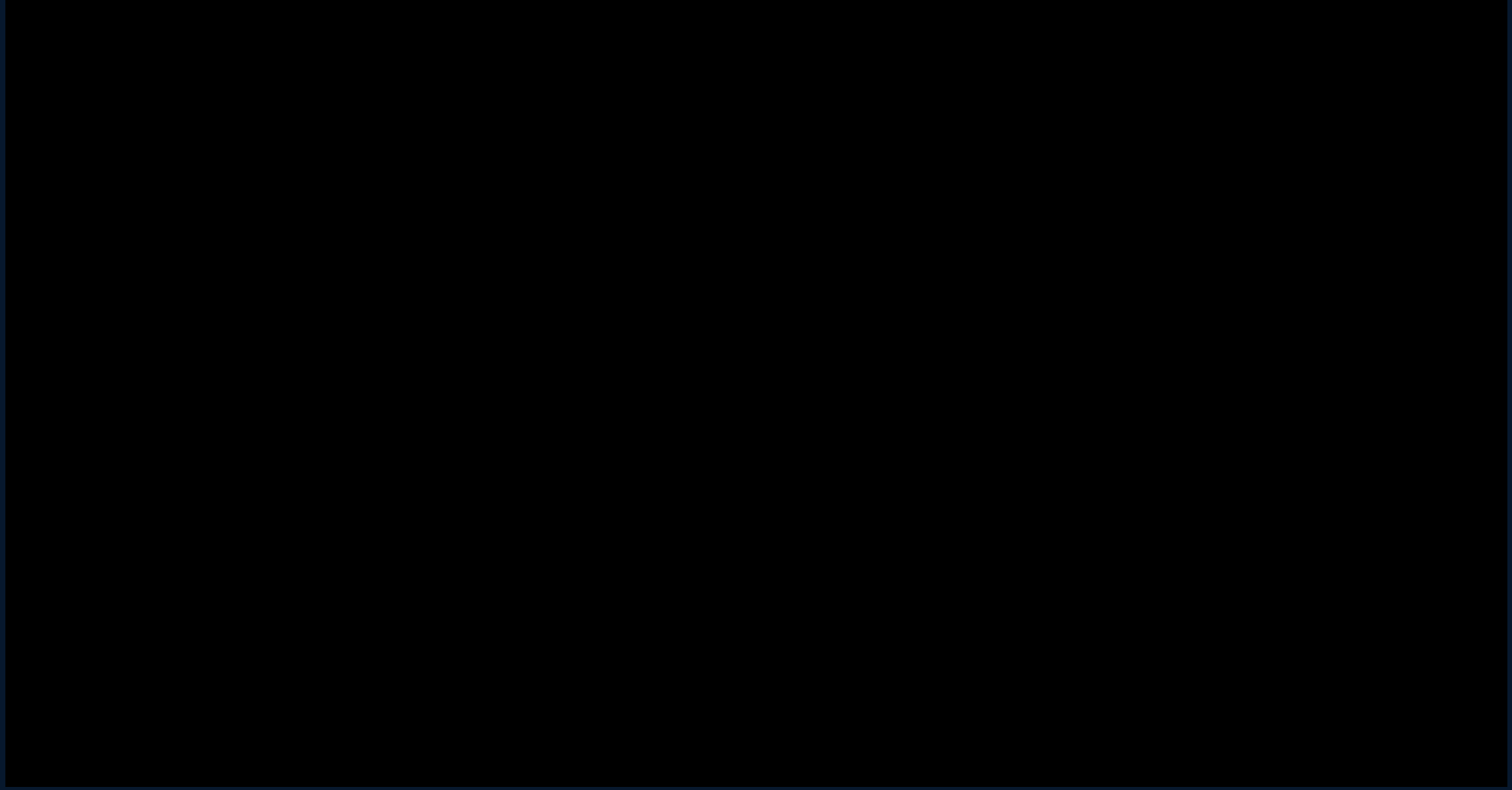
 No PII sent to cloud

 Advantage License Required - No Evaluation Support

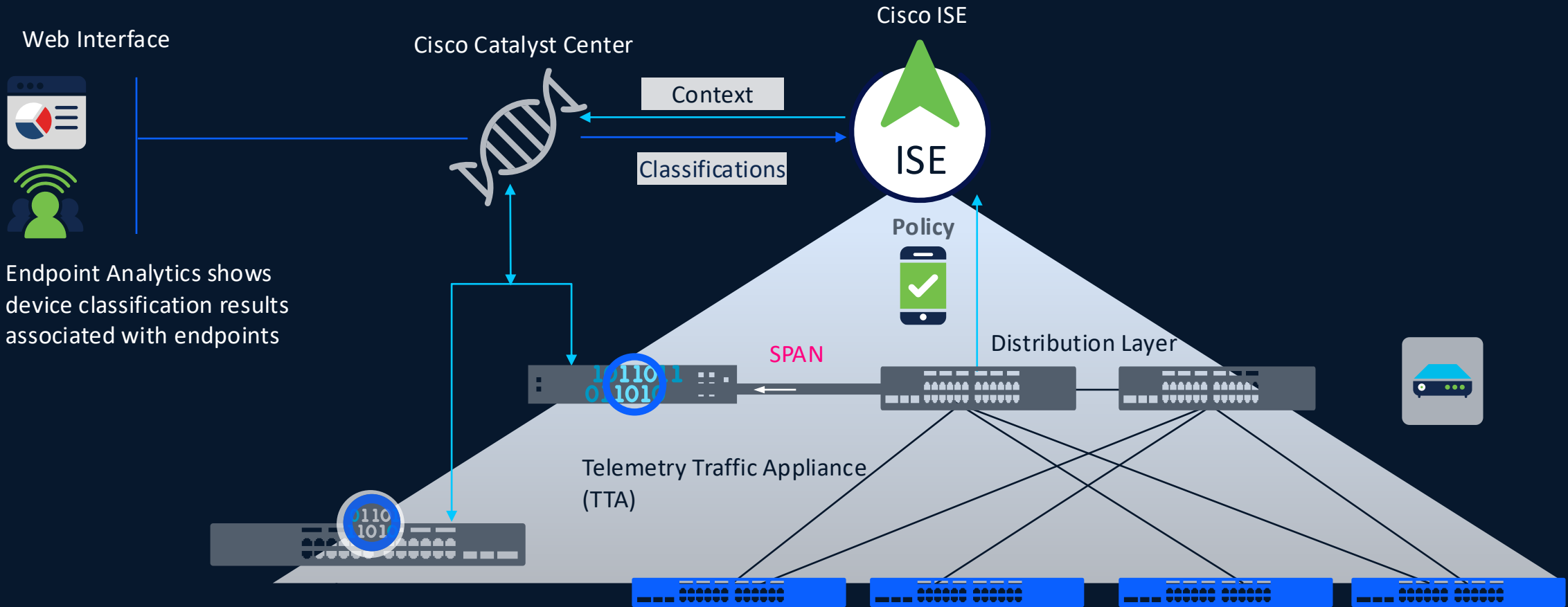
 Cloud Connectivity Required (no air-gapped support)



# AI Endpoint Analytics on ISE



# Cisco AI Analytics



# New Context Visibility UI

Cisco Identity Services Engine
Context visibility

Endpoints pxGrid Direct Users Applications

Endpoints View: Authentication Refresh Last update: July 8, 2024 23:57:47

5000 Total

3900 Connected

1000 Disconnected

100 Rejected

Analytics

**Top failed authentication**

- No respond during PEAP establishment 1400
- Command failed to match permit rule 900
- legend 800
- legend 600
- legend 450

Total failed authentication: 54

**Top authorization profiles**

- Long long long long long legend 1200
- Long long long long long legend 1000
- legend 800
- legend 600
- legend 450

Total authorization profiles: 375

**Top reject reasons**

- Long long long long long long ... long long legend 1400
- Long long long long long legend 900
- legend 800
- legend 600
- legend 450

Total rejected reasons: 46

**Top locations**

- Long long long long long long ... long long legend 900
- Long long long long long long ... long long legend 700
- legend 650
- legend 400
- legend 250

Total locations: 267

Authentication status  Only show 5G endpoints Advanced filters Export Import + Add

MAC address	Auth Status	IP address	Username	Location	Authentication policy	Authorization policy	MFC: Endpoint type
<input type="checkbox"/> 00:00:00:00:00:01	✓	10.0.10.155	john.smith	San Jose - Floor 1	EAP-PEAP Corp	Corp → Employee	Mobile Phone
<input type="checkbox"/> 00:00:00:00:00:02	✓	10.2.20.44	bob.kitches	San Jose - Floor 2	EAP-PEAP Corp	Corp → Employee	Mobile Phone
<input type="checkbox"/> 00:00:00:00:00:03	✓	10.84.15.44	ron.edwards	Sacramento Corp	EAP-PEAP Corp	Corp → Contractor	Mobile Phone
<input type="checkbox"/> 00:00:00:00:00:04	✗	10.84.15.88	david.cooks	Sacramento Corp	Default	—	Mobile Phone
<input type="checkbox"/> 00:00:00:00:00:05	⊖	10.2.10.10	00:00:00:00:00:05	San Jose - Floor 2 Guest	MAB Guest	Guest → Guest Access	Mobile Phone

# Improved Profiling Policy Management

Identity Services Engine Work Center / Profiler

[Bookmarks](#)
[Dashboard](#)
[Context Visibility](#)
[Operations](#)
[Policy](#)
[Administration](#)
[Work Centers](#)

[Overview](#)
[Ext Id Sources](#)
[Network Devices](#)
[Node Config](#)
[Feeds](#)
[Manual Scans](#)
[Policy Elements](#)
[Policy Sets](#)
[Profiling Policies](#)
[More](#)
[More](#)

## Profiling Policies

Last update: July 8, 2024 03:25 [Refresh](#)

[MFC Profiling Policies](#)
Certainty Factor & Logical Profiling Policies

30 Policies enabled
✔

3 Policies disabled
⊘

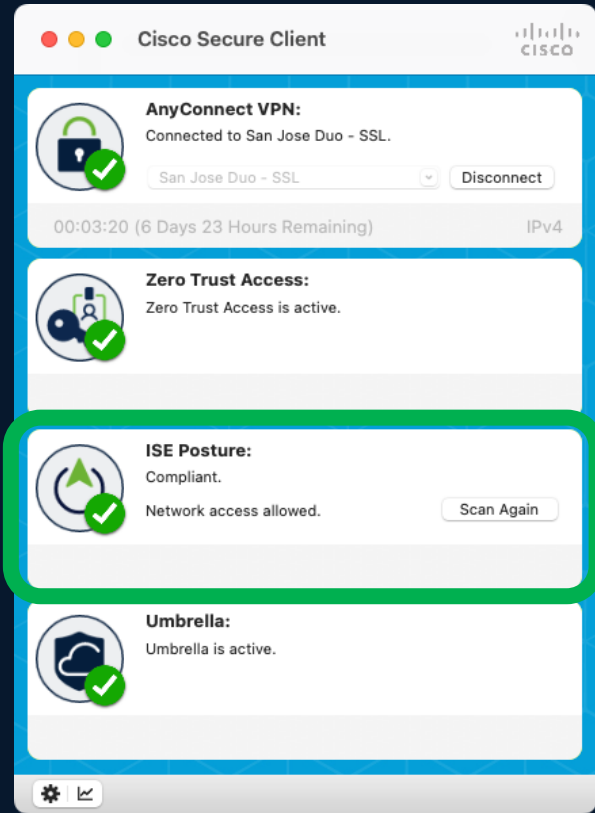
36 Enabled policies with no matched endpoints
⚠

Policies will be processed sequentially based on the rank you set here [?](#)

<input type="checkbox"/>	Rank	Name	Status	Type	MFC: Endpoint type	MFC: Manufacturer	MFC: Model	MFC: OS	Endpoints	<input type="button" value="⚙"/>
<input type="checkbox"/>	1	Name	✔	Custom	—	—	—	Linux	120 matched	...
<input type="checkbox"/>	2	Name	✔	Direct mapping	⌘ Value from JAMF: Endpoint type	⌘ Value from JAMF: Manufacture	⌘ Value from JAMF: Model	⌘ Value from JAMF: OS	180 matched	...
<input type="checkbox"/>	3	Name	⊘	Custom	dhcpDeviceType	App manufacturer	—	—	589 matched	...
<input type="checkbox"/>	4	Name	✔	Custom	Printer	intune manufacture OS	Lexmark-Printer E260dn	iOS	287 matched	...
<input type="checkbox"/>	5	Name	✔	AI	—	—	—	Linux	749 matched	...
<input type="checkbox"/>	6	Name	⊘	Direct mapping	⌘ Value from JAMF: Endpoint type	⌘ Value from JAMF: Manufacture	⌘ Value from JAMF: Model	⌘ Value from JAMF: OS	358 matched	...
<input type="checkbox"/>	7	Name	⊘	Custom	dhcpDeviceType	App manufacturer	—	—	976 matched	...
<input type="checkbox"/>	8	Name	✔	Custom	Printer	intune manufacture OS	Lexmark-Printer E260dn	iOS	267 matched	...
<input type="checkbox"/>	9	Name	✔	Custom	—	—	—	iOS	156 matched	...
<input type="checkbox"/>	10	Name	⊘	Direct mapping	⌘ Value from JAMF: Endpoint type	⌘ Value from JAMF: Manufacture	⌘ Value from JAMF: Model	Linux	987 matched	...
<input type="checkbox"/>	11	Name	⊘	Custom	dhcpDeviceType	App manufacturer	—	—	968 matched	...
<input type="checkbox"/>	12	Name	✔	AI	Printer	intune manufacture OS	Lexmark-Printer E260dn	—	275 matched	...
<input type="checkbox"/>	13	Name	✔	Direct mapping	—	—	—	iOS	10 matched	...

# Posturing for Compliance

# ISE Posture with Cisco Secure Client Checks



System Checks

Software/ Application Checks

Custom Scripts and external Conditions

Script Remediation

Windows updates Patch Management

Remediation/ Reassessment

Hardware Inventory
USB Checks
File Checks
Registry Checks
Service Checks
Disk Encryption
Application Checks
Application Inventory
Anti-Malware Checks
Firewall Installation Checks
Custom scripts
External Conditions (AD, Location)
Compound condition support

Script Remediation
Patch Management – MS SCCM
Windows Update
WSUS remediation (legacy)
Application, Antimalware, File, Firewall, USB Block, Link
Passive Reassessment

## Remediations



# Agentless Posture

Status	Rule Name	Conditions	Profiles	Security Groups
Unknown		AND Network_Access_Authentication_Passed Compliance_Unknown_Devices	Agentless_Posture	Network_Serv...
Compliant		AND Network_Access_Authentication_Passed Compliant_Devices	PermitAccess	Employees

Authorization Profile

\* Name: Agentless\_Posture

Description: [ ]

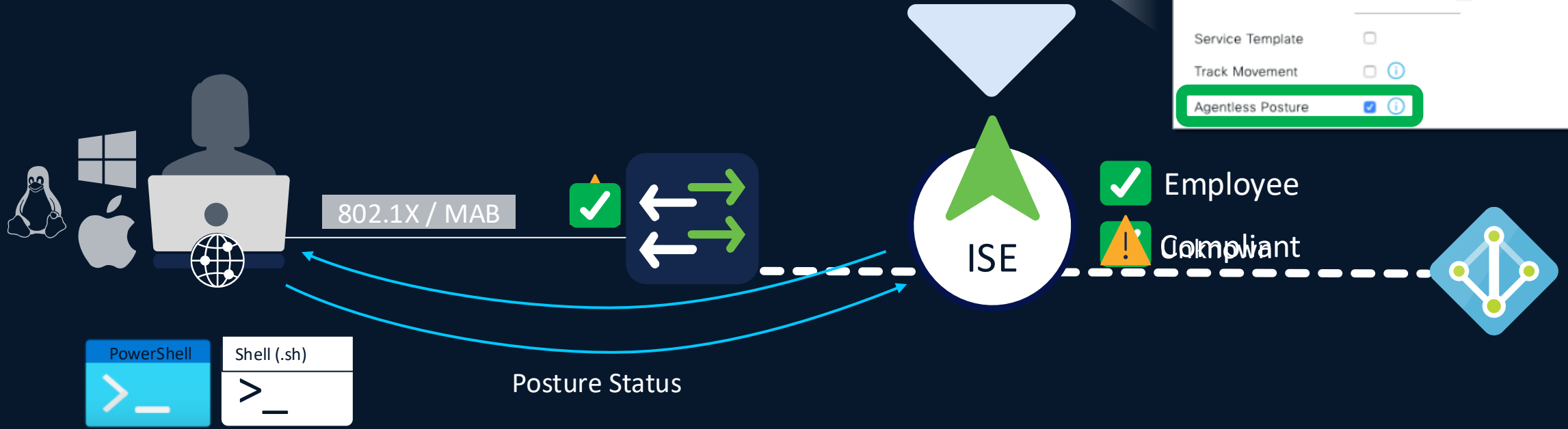
\* Access Type: ACCESS\_ACCEPT

Network Device Profile: Cisco

Service Template: [ ]

Track Movement: [ ]

Agentless Posture [ ]



# Posture Deployment Options

- ✔ Supported
- ! Limitations
- ✗ Not Supported

Capability	Cisco Secure Client			AC Stealth		Temporal		Agentless	
	Windows	Apple	Linux	Windows	Apple	Windows	Apple	Windows	Apple
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	✔	✗	✗	✔	✗	✔	✗	✔	✗
WSUS remediation (legacy)	✔	N/A	N/A	✔	N/A	✗	✗	✗	✗
Remediation	Auto, Manual	Partial	Partial	Part Auto	Partial	Text	Text	✗	✗
Reassessment	✔	✔	✔	✔	✔	✗	✗	✗	✗

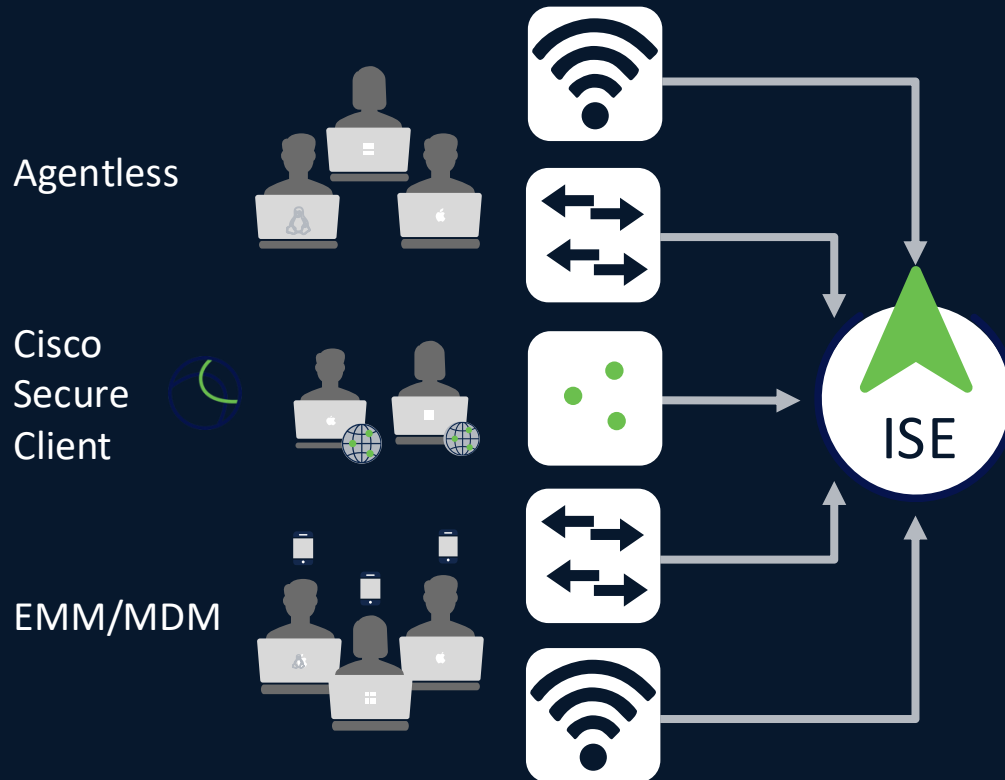
Visibility (Less Effort)

Experience (Less Time)

Security (More Protection)

# Posture & Compliance

 [cisco.com/go/csta](https://cisco.com/go/csta)



## Authorization Policy

IF JailBroken is No  
AND PinLock is Yes  
THEN Compliant

AbsoluteSoftware

SOPHOS

GLOBO

IBM Security

Microsoft

SOTI

tangoe

Meraki

XenMobile

jamf

SAP

MobileIron

Symantec

airwatch  
by vmware

## MDM Attributes

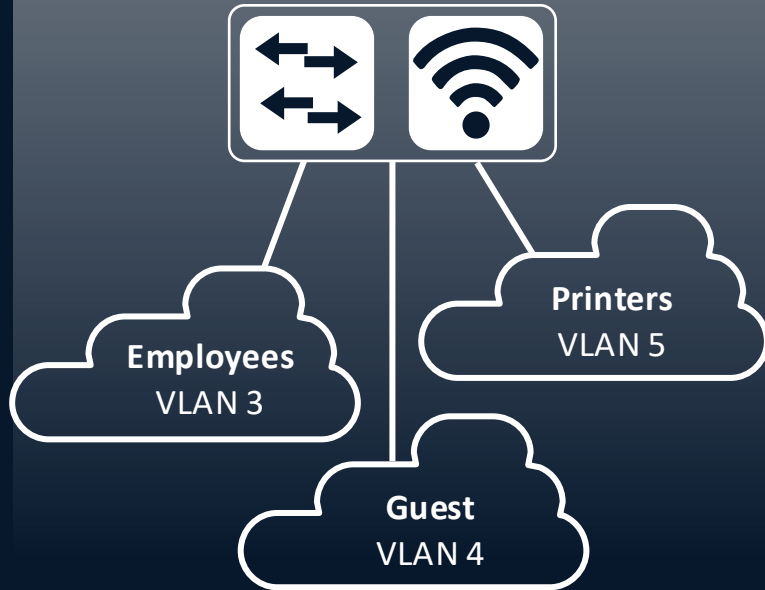
- ActivityType
- AdminAction
- AdminActionUUID
- AnyConnectVersion
- DaysSinceLastCheckin
- DetailedInfo
- DeviceID
- DeviceName
- DeviceType
- DiskEncryption
- EndPointMatchedProfile
- FailureReason
- IdentityGroup
- IMEI
- IpAddress
- JailBroken
- LastCheckinTimeStamp
- MacAddress
- Manufacturer
-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

Segmentation

# ISE Segmentation Options

## VLANs

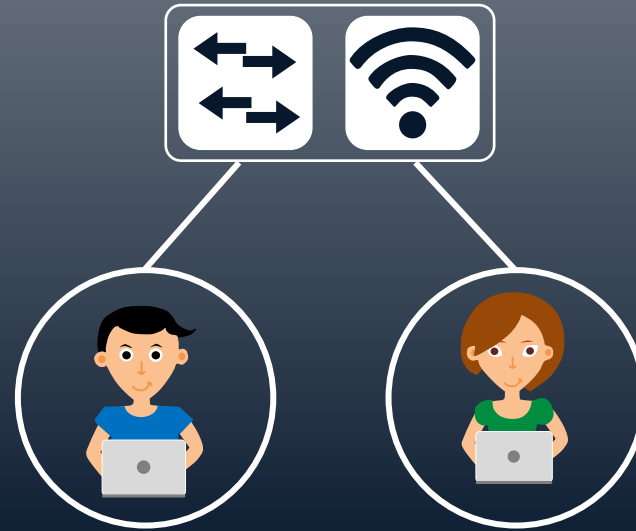
Dynamic VLAN Assignments



Per port / Per Domain / Per MAC

## ACLs: DL, Named, DNS

Downloadable ACL (Wired) or  
Named ACL (Wired + Wireless)

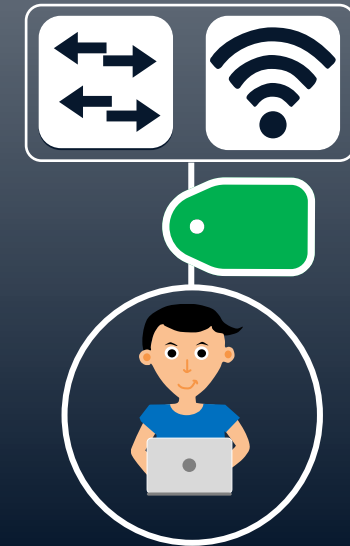


**Employee**  
`permit ip any any`

**Contractor**  
`deny ip host <critical>`  
`permit ip any any`

## Security Group Tags

Cisco Group-Based Policy



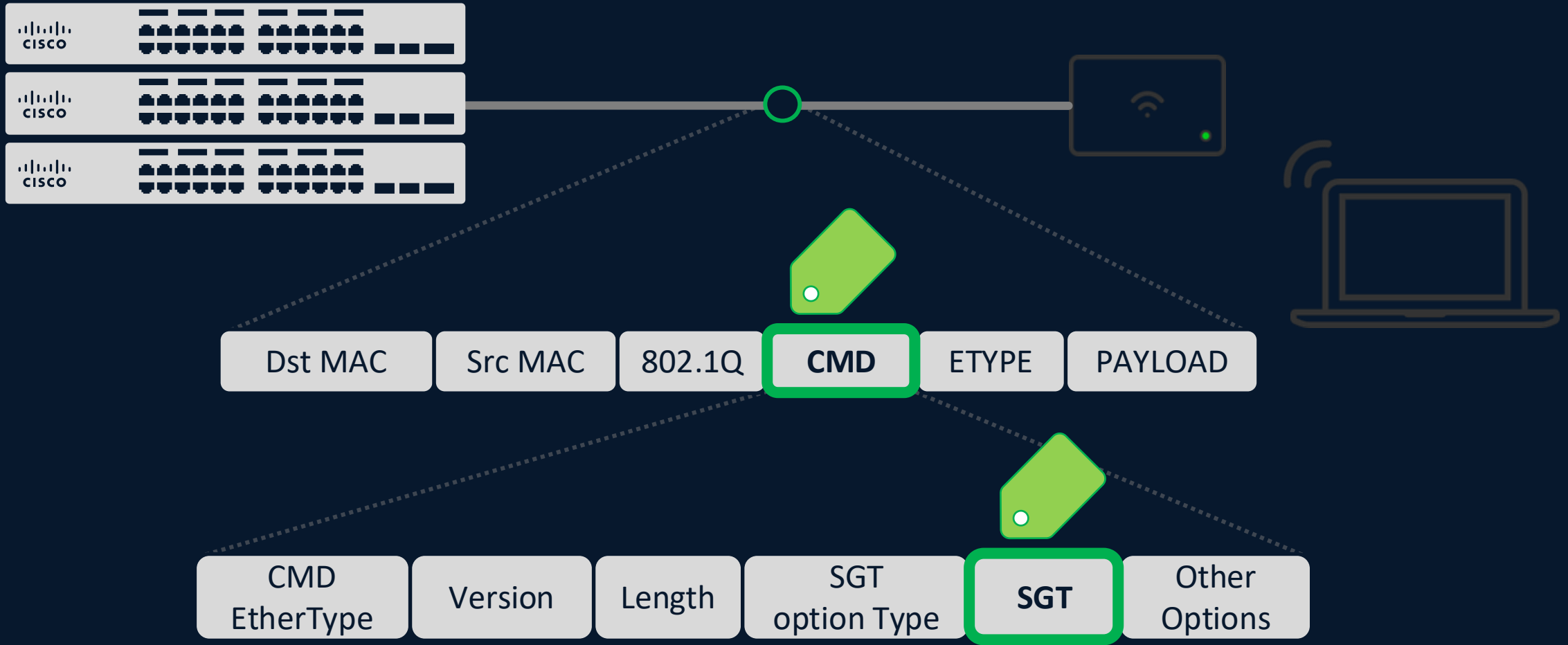
16-bit SGT assignment and SGT  
based Access Control

# Can You See the Business Intent Here?

```
access-list 102 permit tcp 131.249.33.123 0.0.0.127 lt 4765 71.219.207.89 0.255.255.255 eq 606
access-list 102 deny tcp 112.174.162.193 0.255.255.255 gt 368 4.151.192.136 0.0.0.255 gt 4005
access-list 102 permit ip 189.71.213.162 0.0.0.127 gt 2282 74.67.181.47 0.0.0.127 eq 199
access-list 102 deny udp 130.237.66.56 255.255.255.255 lt 3943 141.68.48.108 0.0.0.255 gt 3782
access-list 102 deny ip 193.250.210.122 0.0.1.255 lt 2297 130.113.139.130 0.255.255.255 gt 526
access-list 102 permit ip 178.97.113.59 255.255.255.255 gt 178 111.184.163.103 255.255.255.255 gt 959
access-list 102 deny ip 164.149.136.73 0.0.0.127 gt 1624 163.41.181.145 0.0.0.255 eq 810
access-list 102 permit icmp 207.221.157.104 0.0.0.255 eq 1979 99.78.135.112 0.255.255.255 gt 3231
access-list 102 permit tcp 100.126.4.49 0.255.255.255 lt 1449 28.237.88.171 0.0.0.127 lt 3679
access-list 102 deny icmp 157.219.157.249 255.255.255.255 gt 1354 60.126.167.112 0.0.31.255 gt 1025
access-list 102 deny icmp 76.176.66.41 0.255.255.255 lt 278 169.48.105.37 0.0.1.255 gt 968
access-list 102 permit ip 8.88.141.113 0.0.0.127 lt 2437 105.145.196.67 0.0.1.255 lt 4167
access-list 102 permit udp 60.242.95.62 0.0.31.255 eq 3181 33.191.71.166 255.255.255.255 lt 2422
access-list 102 permit icmp 186.246.40.245 0.255.255.255 eq 3508 191.139.67.54 0.0.1.255 eq 1479
access-list 102 permit ip 209.111.254.187 0.0.1.255 gt 4640 93.99.173.34 255.255.255.255 gt 28
access-list 102 permit ip 184.232.88.41 0.0.31.255 lt 2247 186.33.104.31 255.255.255.255 lt 4481
access-list 102 deny ip 106.79.247.50 0.0.31.255 gt 1441 96.62.207.209 0.0.0.255 gt 631
access-list 102 permit ip 39.136.60.170 0.0.1.255 eq 4647 96.129.185.116 255.255.255.255 lt 3663
access-list 102 permit tcp 30.175.189.93 0.0.31.255 gt 228 48.33.30.91 0.0.0.255 gt 1388
access-list 102 permit ip 167.100.52.185 0.0.1.255 lt 4379 254.202.200.26 255.255.255.255 gt 4652
access-list 102 permit udp 172.16.184.148 0.255.255.255 gt 4163 124.38.159.247 0.0.0.127 lt 3851
access-list 102 deny icmp 206.107.73.252 0.255.255.255 lt 2465 171.213.183.230 0.0.31.255 gt 1392
access-list 102 permit ip 96.174.38.79 0.255.255.255 eq 1917 1.156.181.180 0.0.31.255 eq 1861
access-list 102 deny icmp 236.123.67.53 0.0.31.255 gt 1181 31.115.75.19 0.0.1.255 gt 2794
access-list 102 deny udp 14.45.208.20 0.0.0.255 lt 419 161.24.159.166 0.0.0.255 lt 2748
access-list 102 permit udp 252.40.175.155 0.0.31.255 lt 4548 87.112.10.20 0.0.1.255 gt 356
access-list 102 deny tcp 124.102.192.59 0.0.0.255 eq 2169 153.233.253.100 0.255.255.255 gt 327
access-list 102 permit icmp 68.14.62.179 255.255.255.255 lt 2985 235.228.242.243 255.255.255.255 lt 2286
access-list 102 deny tcp 91.198.213.34 0.0.0.255 eq 1274 206.136.32.135 0.255.255.255 eq 4191
access-list 102 deny udp 76.150.135.234 255.255.255.255 lt 3573 15.233.106.211 255.255.255.255 eq 3721
access-list 102 permit tcp 126.97.113.32 0.0.1.255 eq 4644 2.216.105.40 0.0.31.255 eq 3716
access-list 102 permit icmp 147.31.93.130 0.0.0.255 gt 968 154.44.194.206 255.255.255.255 eq 4533
access-list 102 deny tcp 154.57.128.91 0.0.0.255 lt 1290 106.233.205.111 0.0.31.255 gt 539
access-list 102 deny ip 9.148.176.48 0.0.1.255 eq 1310 64.61.88.73 0.0.1.255 lt 4570
```



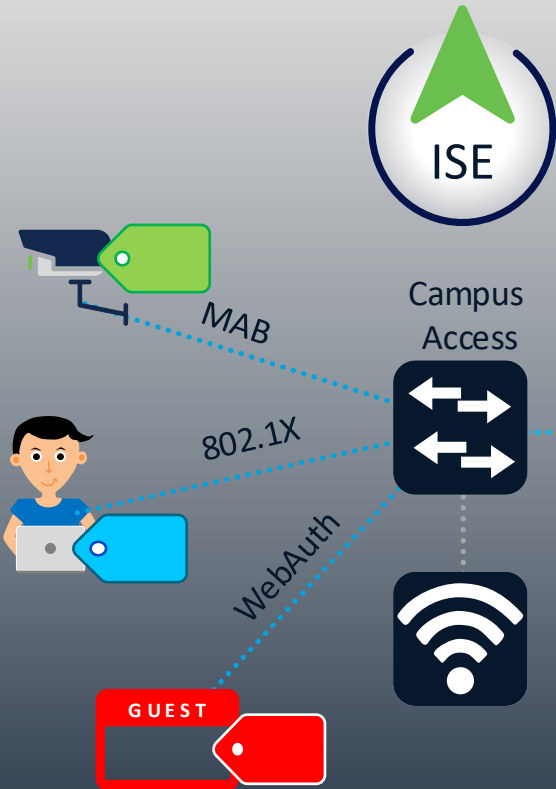
# Security Group Tags (SGTs)



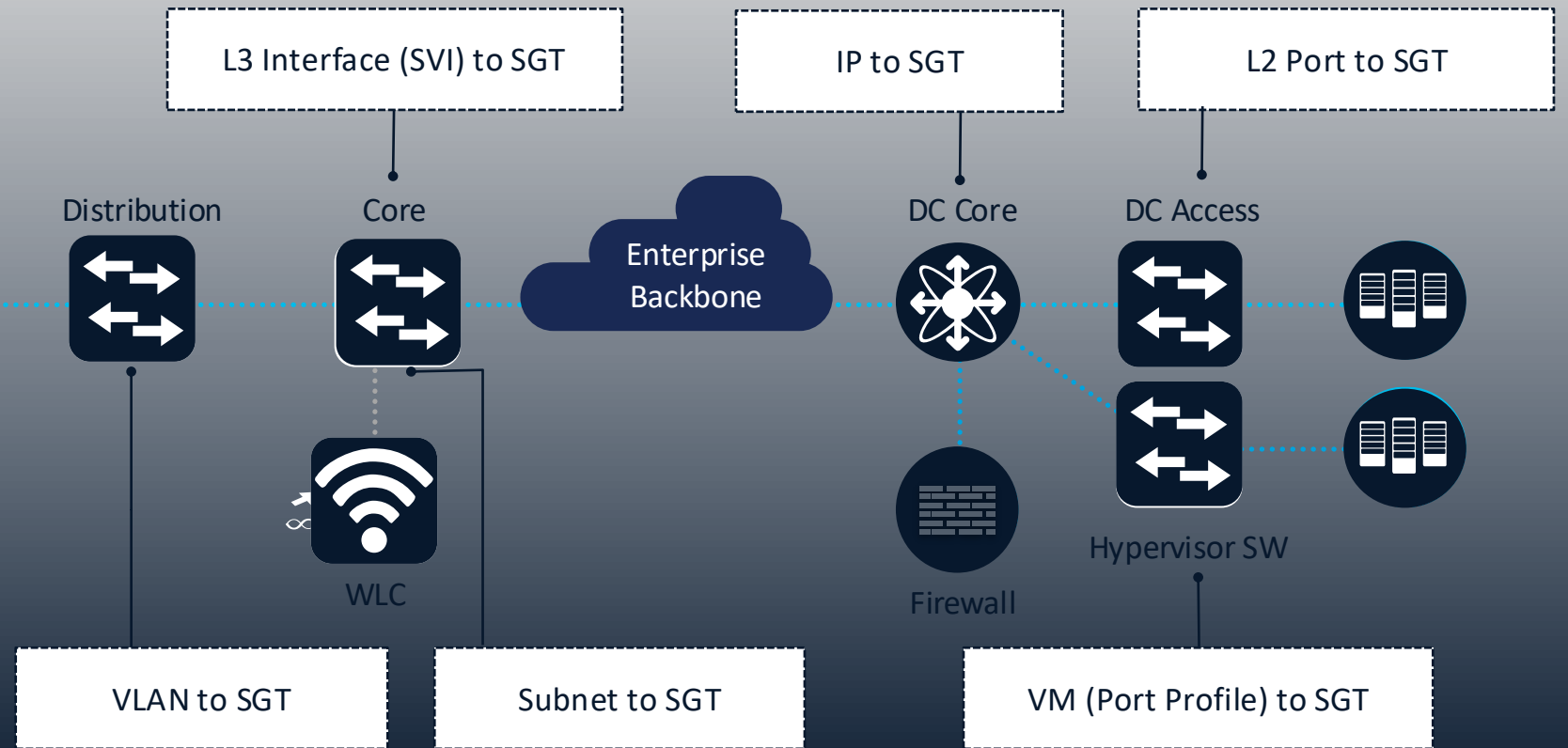
# Classification Mechanisms



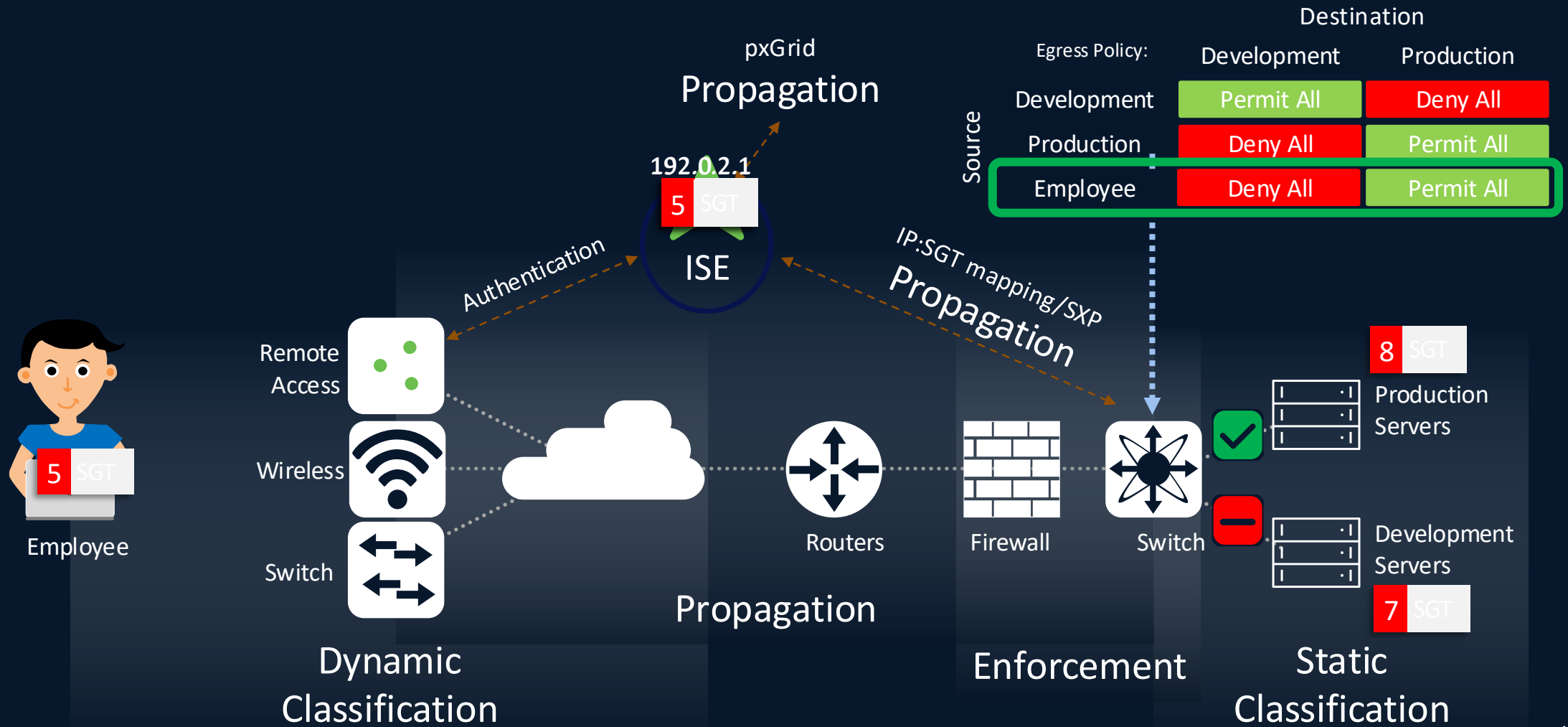
## Dynamic Classification



## Static Classification



# Cisco SGT Propagation & Enforcement



# Integrations to Automate Policy

# Platform Exchange Grid (pxGrid)

- Open and scalable Security Product Integration Framework (SPIF) that allows for bi-directional any-to-any partner platform integration
- Introduced in ISE 1.3
- Integrations with 100+ Cisco and non-Cisco products
- Reduces silos by integrating your security architecture together to share context, respond to threats, and ingest information
- Tons of guides on integrations at [cs.co/ise-guides](https://cs.co/ise-guides)
  - But also check out [developer.cisco.com/site/pxgrid](https://developer.cisco.com/site/pxgrid)

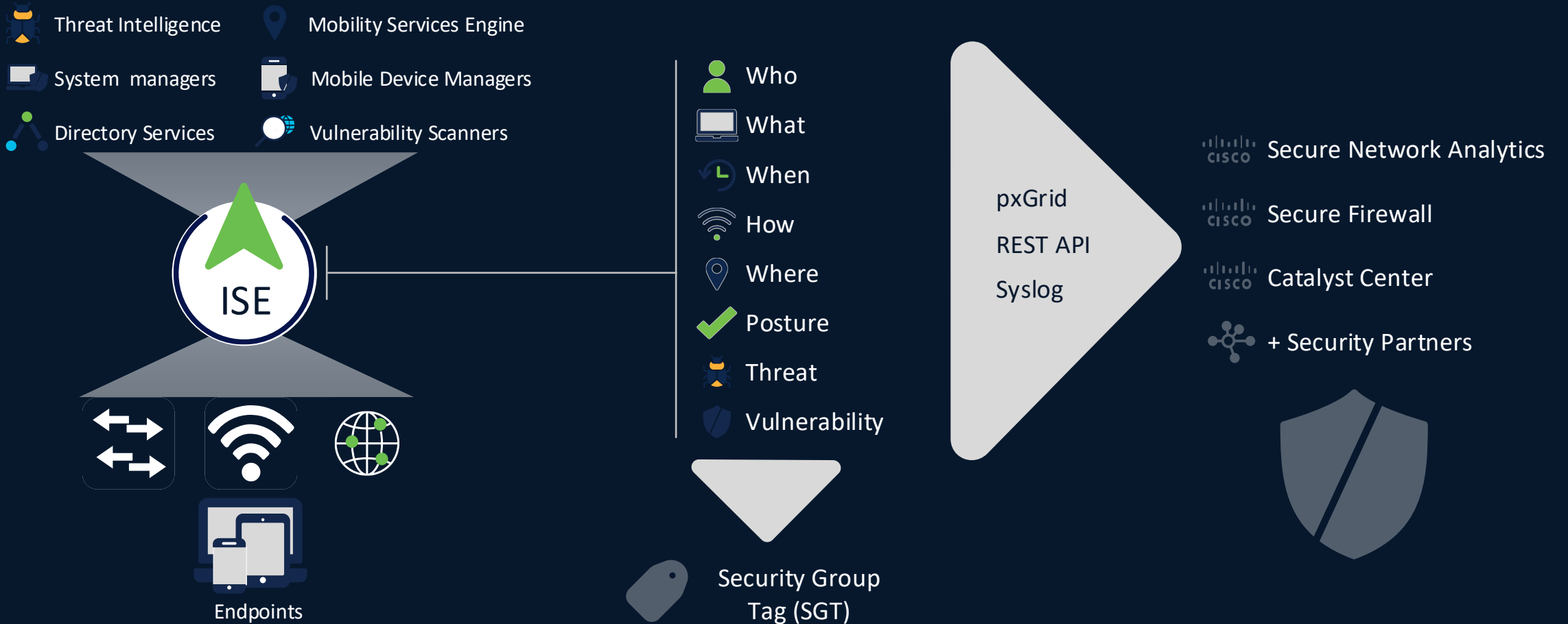
# Context Build, Summarize, Exchange with pxGrid

## Visibility and Access Control

ISE builds context and applies access control restrictions to users and devices

## Context Reuse

by eco-system partners for analysis & control



# On-Prem pxGrid Integration

1. Both ISE and the pxGrid Client need to have an identity (pxGrid) certificate issued from a Root CA the other trusts.  
Note: Certificate EKU must have Client and Server Authentication



2. The pxGrid client is configured with the IP addresses of ISE's pxGrid nodes

3. The pxGrid initiates the connection to ISE and authenticates itself with its identity (pxGrid) certificate



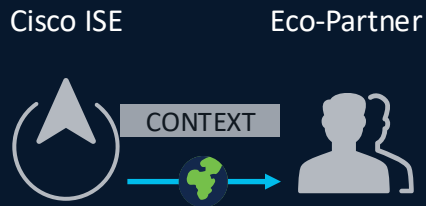
4. ISE will authenticate itself back to the client with its own pxGrid certificate

5. ISE should now list the pxGrid client in the pxGrid dashboard and share session context with the client by default. In the pxGrid dashboard, this client can also be assigned additional permissions by being added pxGrid groups such as ANC

Note: Password-based pxGrid authentication is available but rarely used

# Context Sharing with pxGrid

## Context to Partner



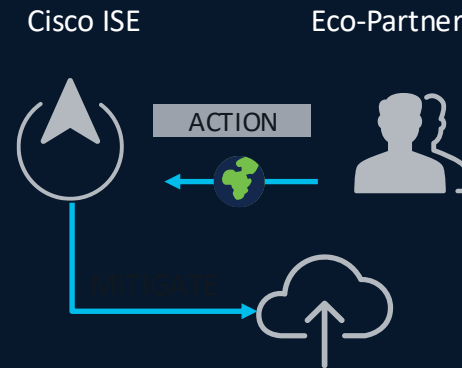
ISE makes Customer IT Platforms User/Identity, Device and Network Aware

## Enrich ISE Context



Enrich ISE context. Make ISE a better Policy Enforcement Platform

## Threat Mitigation



Enforce dynamic policies into the network based on Partner's request

## Context Brokerage



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

# pxGrid/ANC Policies in ISE

The screenshot displays the Cisco Identity Services Engine (ISE) dashboard. The top navigation bar includes the Cisco logo, "Identity Services Engine", and "Dashboard". The main content area is divided into several sections:

- Summary:** A row of six cards showing metrics: Total Endpoints (0), Active Endpoints (0), Rejected Endpoints (0), Anomalous Behavior (0), Authenticated Guests (0), and BYOD Endpoints (0). Each card has a refresh icon and a help icon.
- Authentication Table:** A table with columns: Identity Store, Identity Group, Network Device, Failure Reason. It displays "No data available." with a large grey circle.
- Network Devices Table:** A table with columns: Device Name, Type, Location. It displays "No data available." with a large grey circle.
- Endpoints Table:** A table with columns: Profile, Logical Profile. It displays "No data available." with a large grey circle.
- BYOD Endpoints Table:** A table with columns: Type, Profile. It displays "No data available." with a large grey circle.
- Alarms Table:** A table with columns: Severity, Name, Occu..., Last Occurred. It shows a dropdown menu for "Name".
- System Summary:** A summary card showing "1 node(s)" and "ISE". It includes filters for "All" and "24HR".

# Other pxGrid Use-Case Examples

- Secure Firewall
  - Share IP-to-Username binding, SGT, and profile information with Secure Firepower
  - Create ACPs in Firepower based on profile, identity/AD Group, and SGT
  - Quarantine endpoints from ISE based on detections from Secure Firewall
- Secure Network Analytics (SNA)
  - Shares IP-to-Username binding, SGT, and profile information with SNA
  - Create network-based detection policies in SNA that will quarantine or change access endpoint access level through ISE
- And much more...

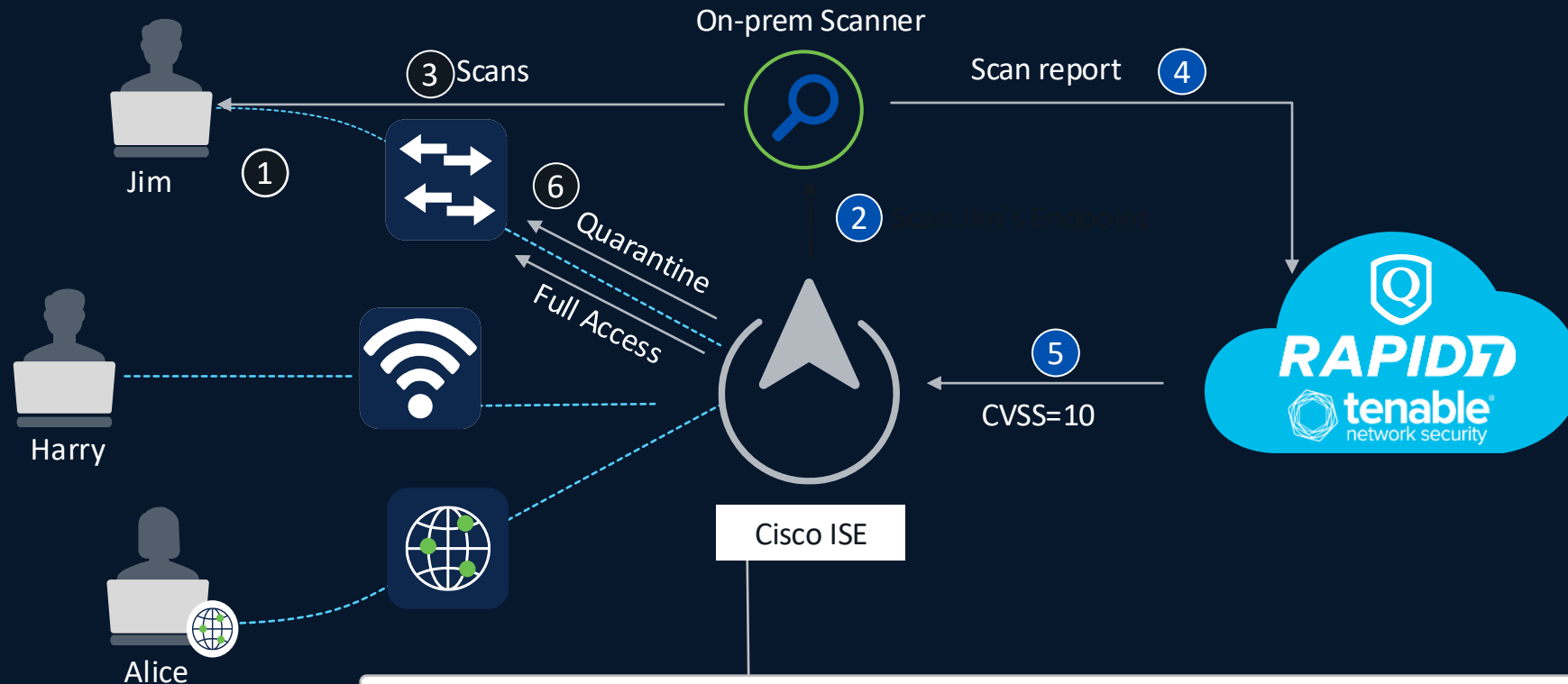
# pxGrid Integration Tips

- Start with integrating to share context out:
  - Gives information to a pxGrid subscriber such as username-to-IP binding, profile, SGT, etc
- (Optional) Migrated data in for richer profiling:
  - Custom third party attributes don't build the profiles themselves
  - Will still need to build profiles
  - Leverage AI Analytics to help
- Rapid Threat Containment:
  - Automates the change of access based on a trigger from a pxGrid subscriber
  - Start with the “low hanging fruit” – Don't need to quarantine everything

# Threat-Centric NAC (TC-NAC)

- Integrates with third-party vulnerability scanners such as Qualys, Rapid7, and Tenable
  - Trigger an endpoint scan
  - Ingest vulnerability information into ISE
- Integrates with Cisco Secure Endpoint and Cognitive Threat Analytics
  - Ingests threat information about an endpoint
- Contextual information stored under endpoint attributes as well as Context Visibility dashboards to see overview of the data

# Vulnerability Assessment with Threat-Centric NAC



## Authorization Policy

If **CVSS is Greater than 5** = true, then **Quarantine**

CVSS: Common Vulnerability Scoring System

# MDM Integrations

- Integrates with many third-party MDM vendors
- Onboard endpoints to MDM through ISE
- Control and visibility into non-corporate and mobile devices
- MDM posture checks in ISE authorization rules

Name	Internal Name	Description
DaysSinceLastCheckin	days_since_lastc...	Number of days since last checkin
DeviceCompliantStatus	compliant_status	Compliant Status of device on MDM
DeviceRegisterStatus	register_status	Status of device registration on MDM
DiskEncryptionStatus	disk_encryption_on	Device disk encryption on MDM
IMEI	imei	IMEI
JailBrokenStatus	jail_broken	Is device jail broken
Manufacturer	manufacturer	Manufacturer name
MDMFailureReason	mdm_failure_reas...	Reason for MDM Server connection failure
MDMServerName	mdmServerName	MDM server name
MDMServerReachable	MDMserverReach...	MDM server reachability
MEID	meid	MEID
Model	model	Device model
OsVersion	os_version	Device Operating System
PhoneNumber	phone_number	Phone number
PinLockStatus	pin_lock_on	Device Pin lock status
SerialNumber	serial_number	Device serial number
ServerType	server_type	Type of device management server
UDID	udid	UDID
UserNotified	user_notified	Has the user been notified

# MDM Integration Example

The screenshot displays the Cisco Identity Services Engine (ISE) Dashboard. The top navigation bar includes the Cisco logo, the text "Identity Services Engine", and the word "Dashboard". On the right side of the navigation bar are icons for search, notifications, help, and user profile.

Below the navigation bar is a secondary menu with tabs for "Summary", "Endpoints", "Guests", "Vulnerability", and "Threat". The "Summary" tab is currently selected. To the right of these tabs is a "Manage" dropdown menu.

The main content area features a row of six summary cards, each with a title and a large blue "0" value:

- Total Endpoints
- Active Endpoints
- Rejected Endpoints
- Anomalous Behavior
- Authenticated Guests
- BYOD Endpoints

Below the summary cards are six data panels, each with a title and a table header:

- AUTHENTICATIONS**: Table with columns "Identity Store", "Identity Group", "Network Device", and "Failure Reason".
- NETWORK DEVICES**: Table with columns "Device Name", "Type", and "Location".
- ENDPOINTS**: Table with columns "Profile" and "Logical Profile".
- BYOD ENDPOINTS**: Table with columns "Type" and "Profile".
- ALARMS**: Table with columns "Severity", "Name", "Occu...", and "Last Occurred".
- SYSTEM SUMMARY**: Shows "1 node(s)" and "ISE".

Each data panel currently displays "No data available." and a large grey circle graphic. The "ALARMS" table has one entry:

Severity	Name	Occu...	Last Occurred
<span style="color: blue;">i</span>	Configuration Chang...	7259	2 mins ago

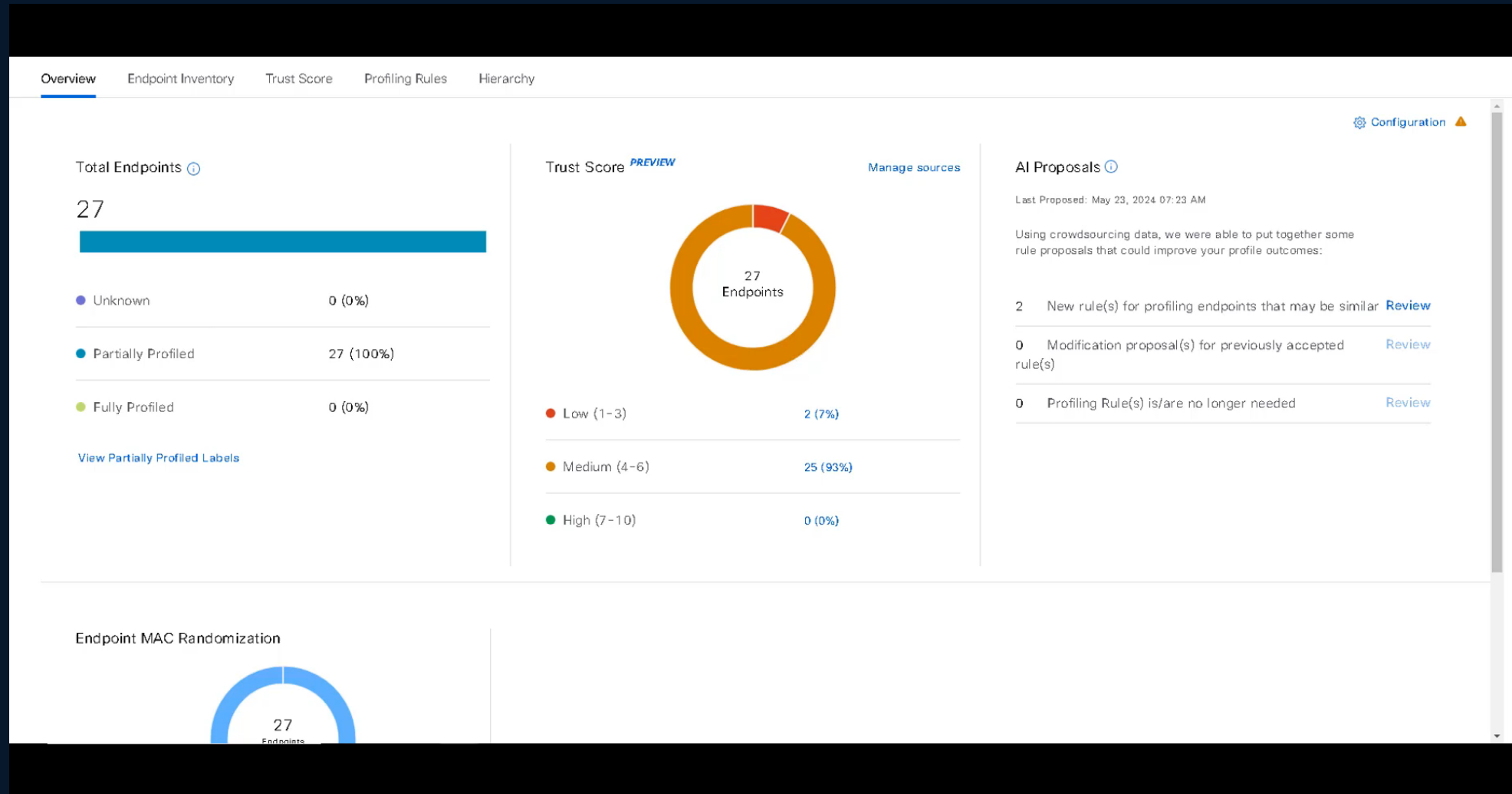
# ISE APIs and Automation



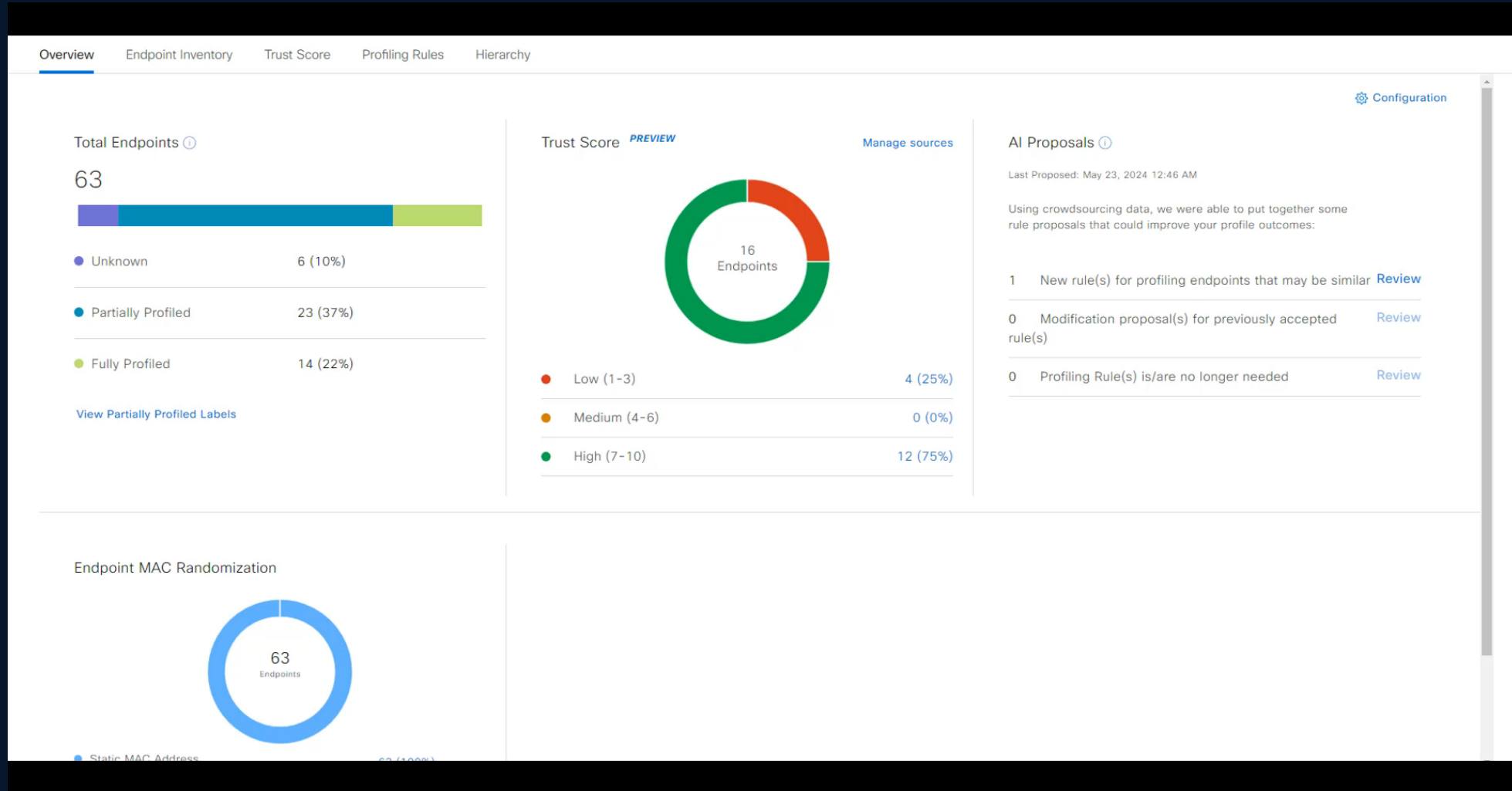
# Integration Example: Catalyst Center and ISE

- Catalyst Center supercharges AI Analytics
  - Granular profile recommendations utilizing telemetry and DPI
- Zero trust: Trust Score
  - Score based on:
    - Change in profile label
    - Traffic pattern anomaly
    - Unauthorized ports and weak credentials
    - and more
  - Quarantine low scoring endpoints via ISE integration
- Configure Trustsec SGACLs and policy utilizing historic traffic patterns

# Catalyst Center Trust Score and Spoofing Detection



# Catalyst Center AI Endpoints Telemetry



# TrustSec Policies with Catalyst Center Integration

