CISCO Engage | Tech Day

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

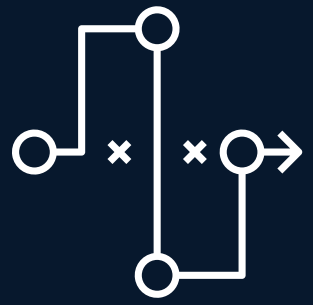
A little about me

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

cisco

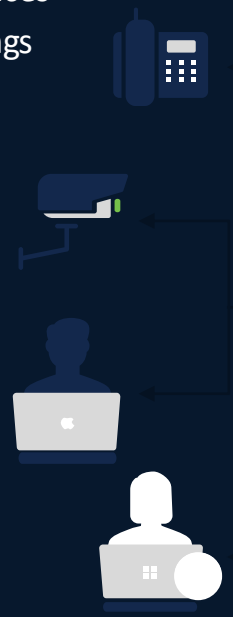
Network Access Control

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

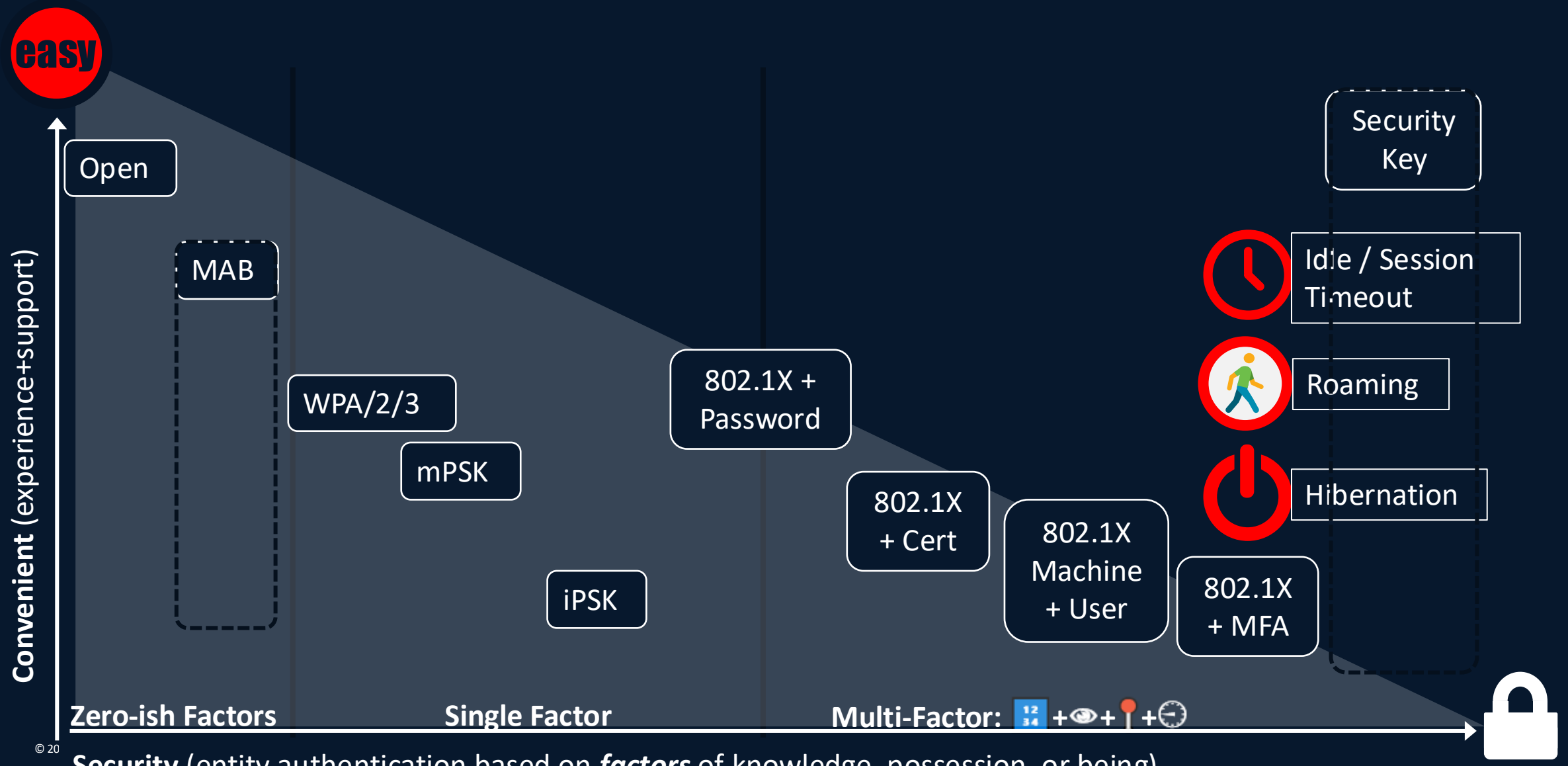
- Entra, AD
- LDAP, ODBC
- MDM
- SAML/MFA

Security Services

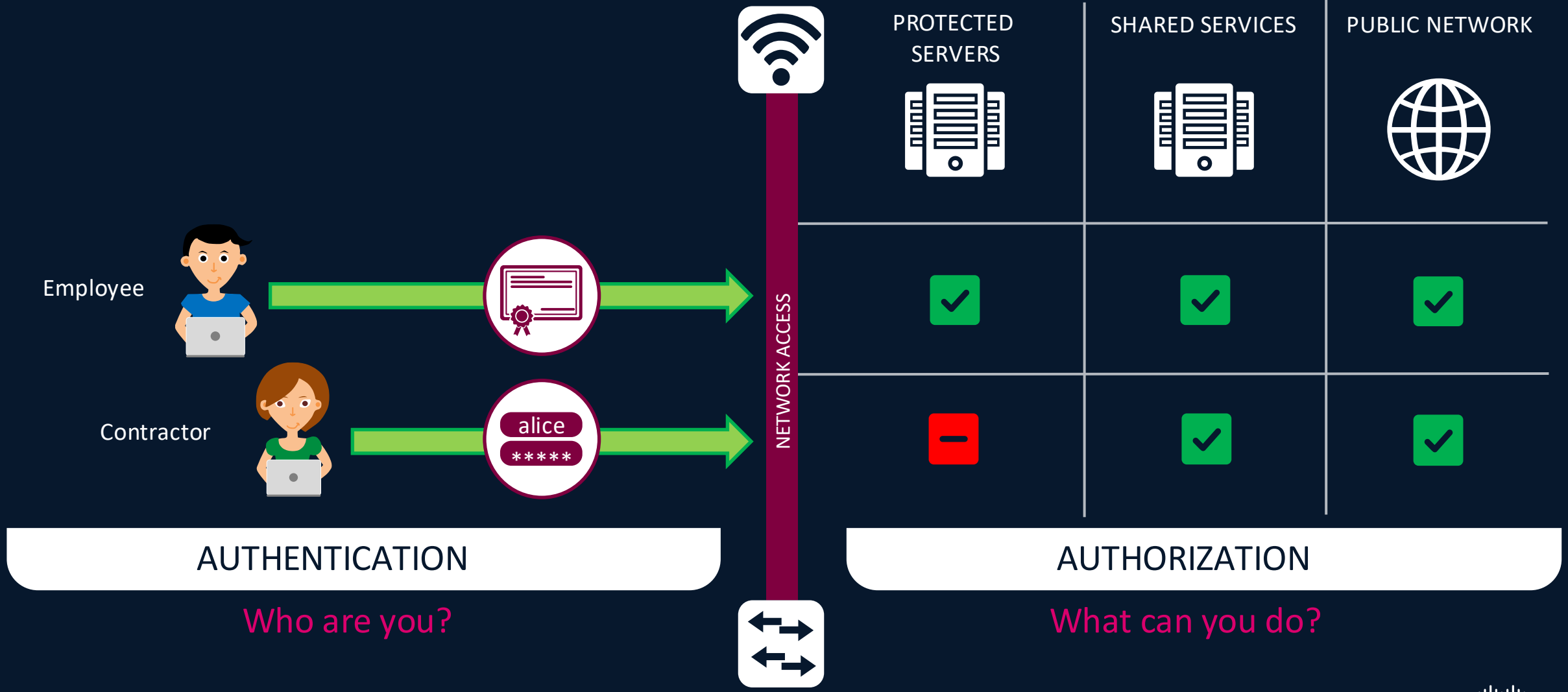
- Cloud Analytics
- Secure Firewall
- Partners

Visibility → Segmentation → Containment

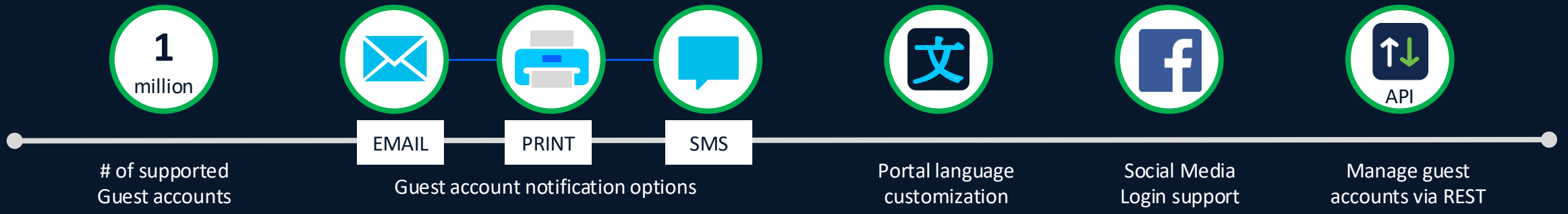
Network Access Authentication is a Spectrum



Authentication and Authorization



Guest Solution Overview

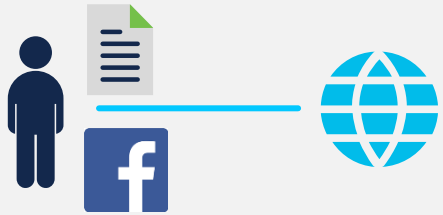


The 3 types of guest access

Hotspot

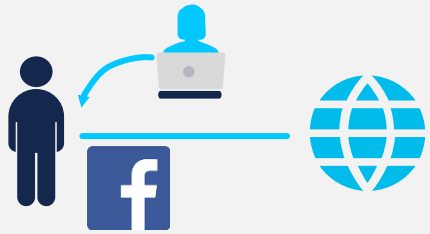
Immediate, un-credentialed Internet access

Self Registered



Self-registration by guests, Sponsors may approve access

Sponsored Guest Access



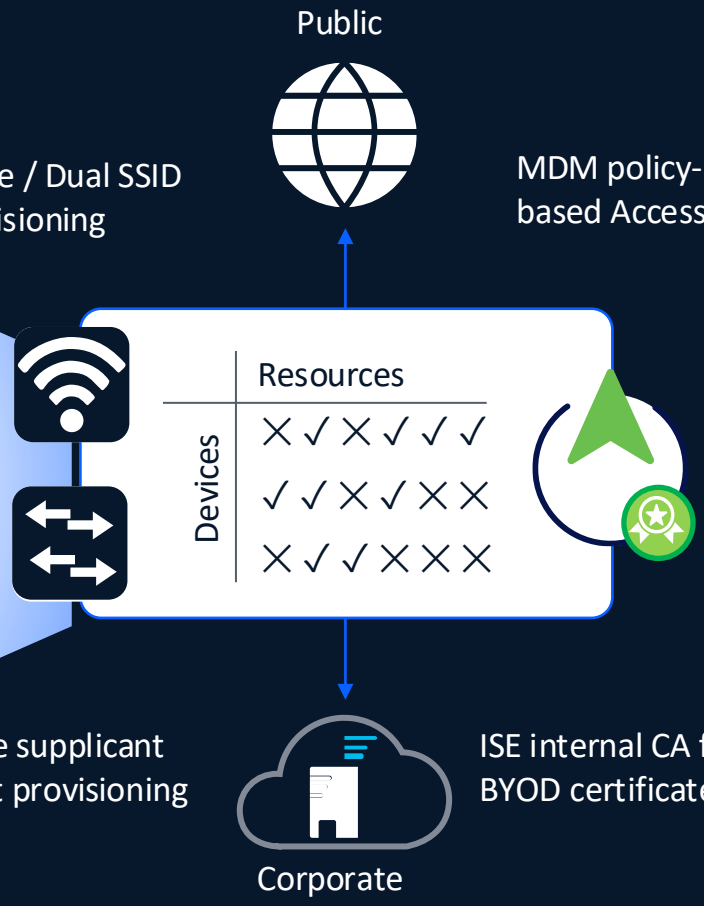
Authorized sponsors create account and share credentials

ISE BYOD / EMM / MDM Solutions

EMM: Enterprise Mobility Management | MDM: Mobile Device Management

Device Support

- iDevice
- Android
- macOS
- Windows
- ChromeOS



- 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

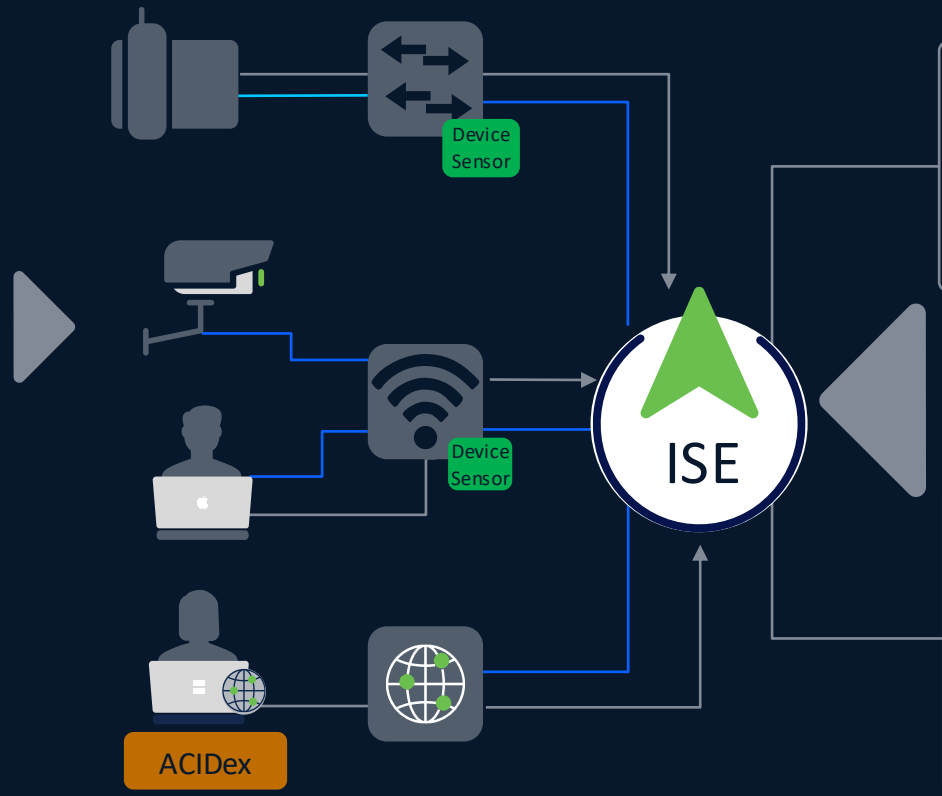
cisco.com/go/csta

Profiling Endpoints

Endpoint Profiling

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

Endpoints send interesting data, that reveal their device type



ISE Data Collection Methods for Device Profiling

Primary Collection Methods: DHCP | DNS | HTTP | RADIUS | NMAP | SNMP | AD | Netflow

Device Sensor: CDP| LLDP | DHCP | HTTP | H323 | SIP | MDNS

Cisco Secure Client (formerly AnyConnect): ACIDex

Feed Service (Online/Offline)

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

Turing Attributes into Profiles, Profiles into Protection

Attribute Sources

1. **Probes:** DHCP | DNS | HTTP | RADIUS | NMAP | SNMP (incl. to endpoint) | AD
2. **Device Sensor:** CDP| LLDP | DHCP | HTTP | H323 | SIP | MDNS
3. **Device management:** MDM, Cisco Secure Client
4. **Endpoint Custom Attributes:** Admin created

Profile Generation

Cisco-provided

AI-proposed

Admin-created

Integrations

MFC Profiles

Mfg

Model

OS Version

Endpoint Type

Profile Tag

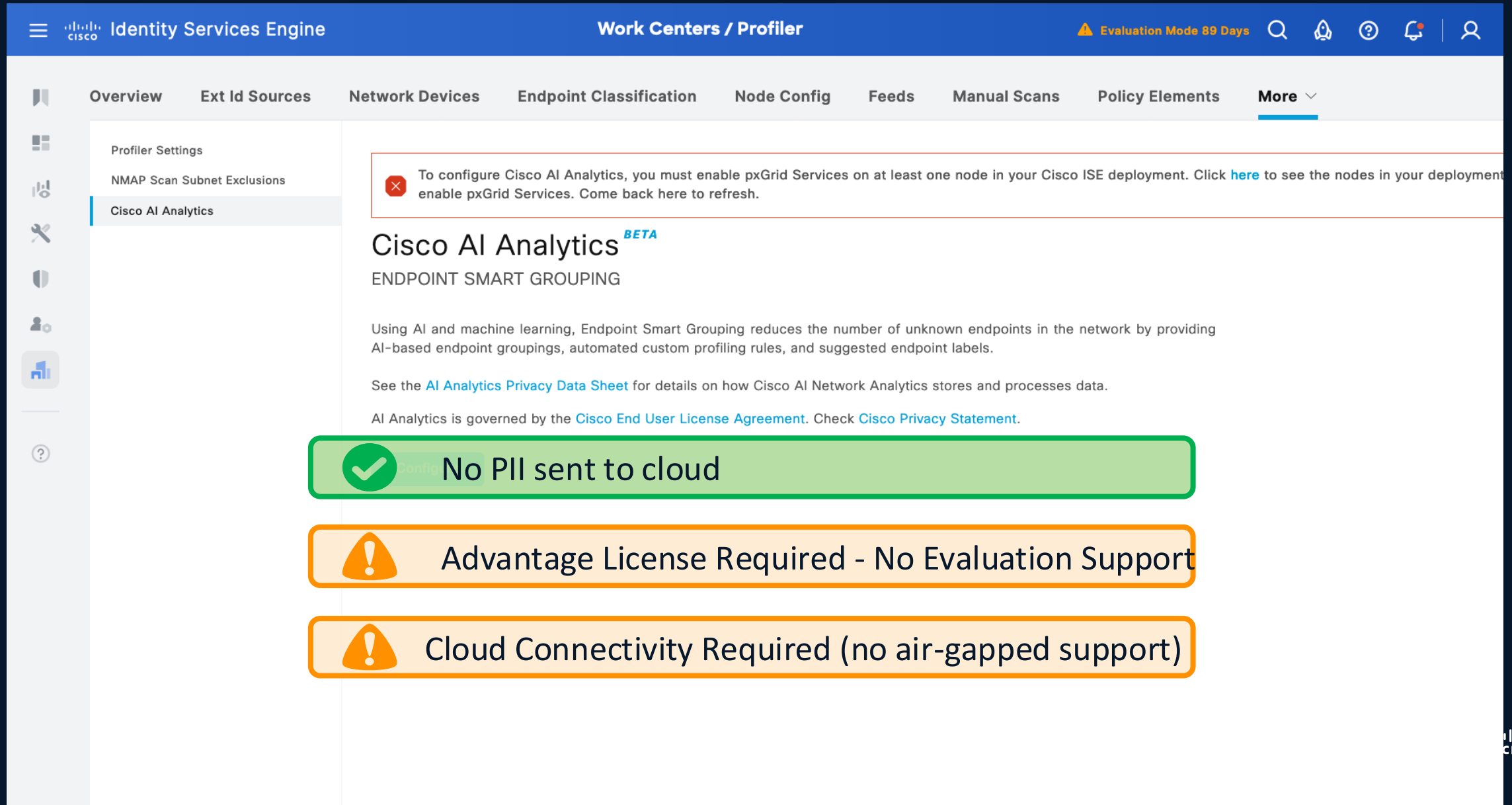
Certainty Factor Profiles

Authorization

Segmentation

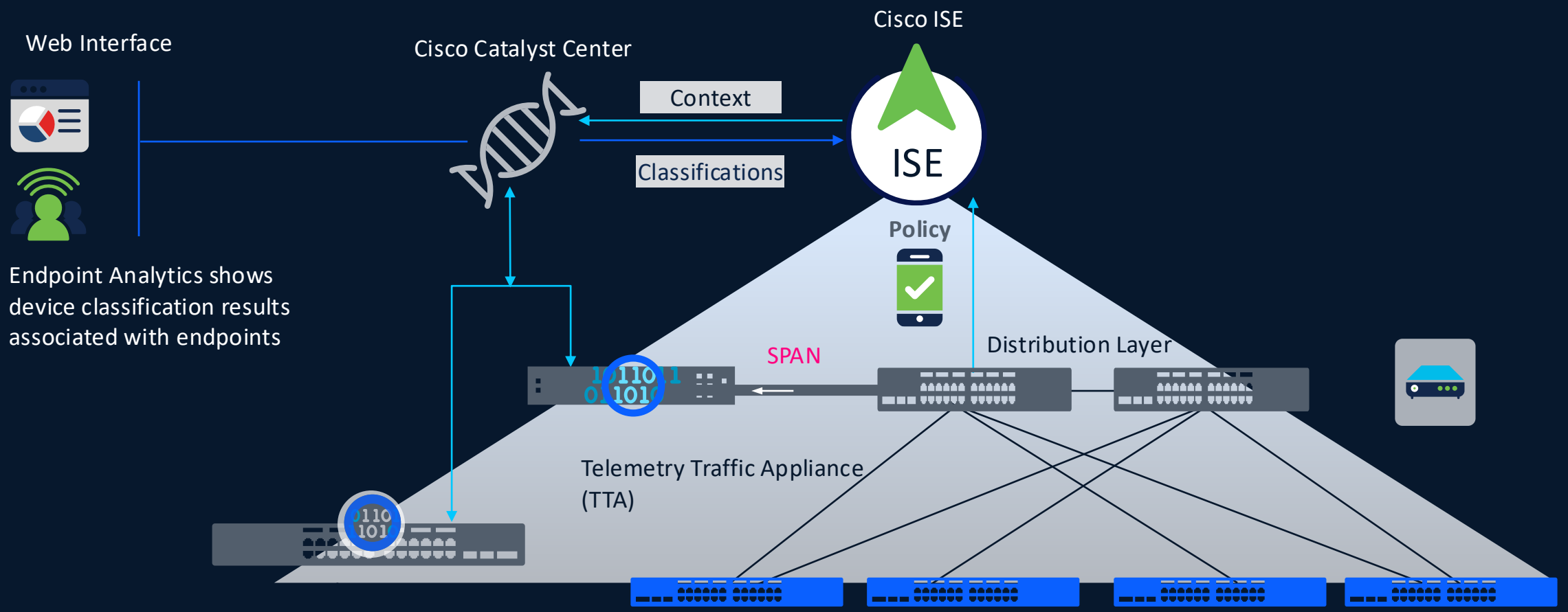
cisco

Cisco AI Analytics

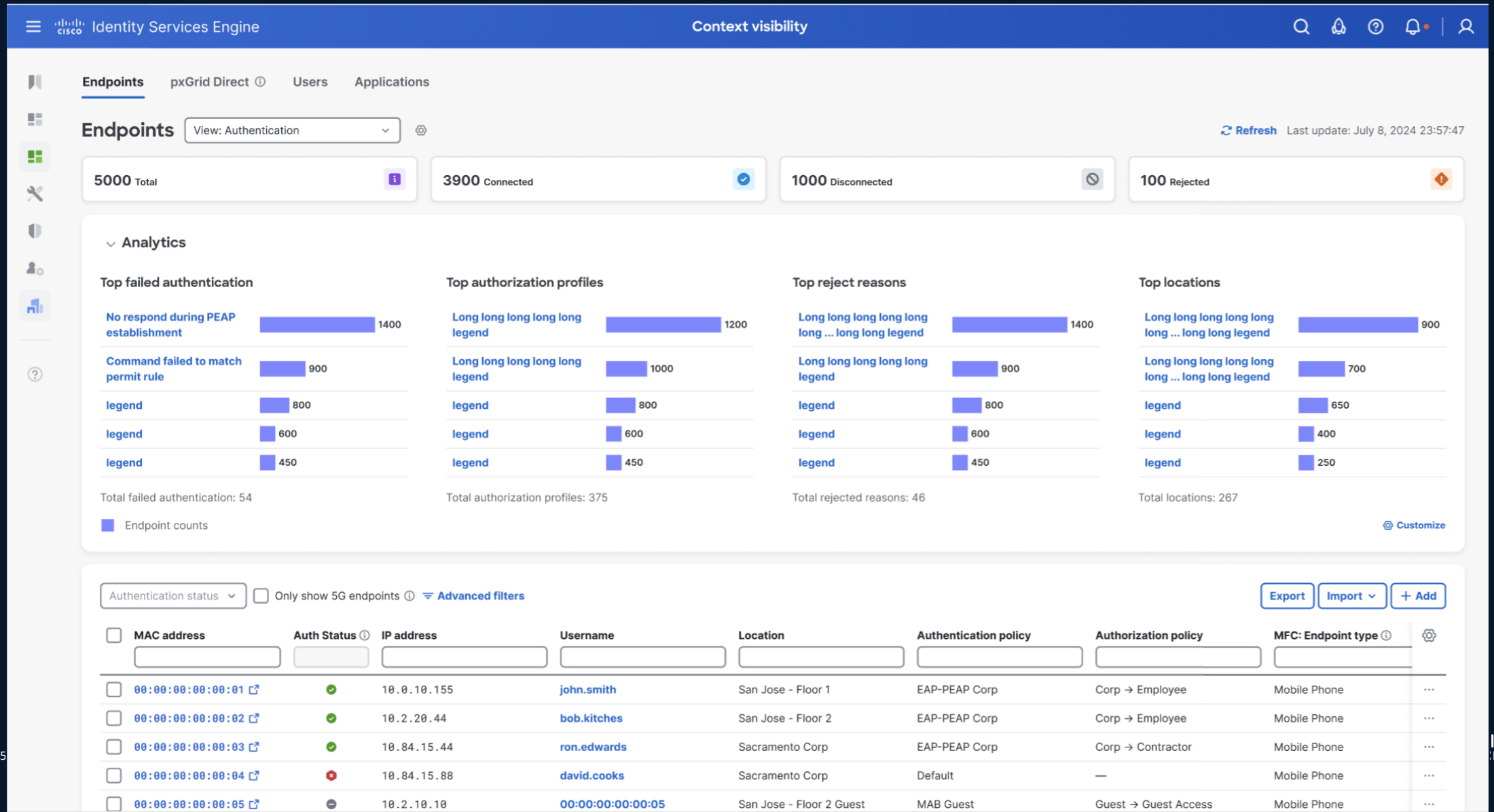


AI Endpoint Analytics on ISE

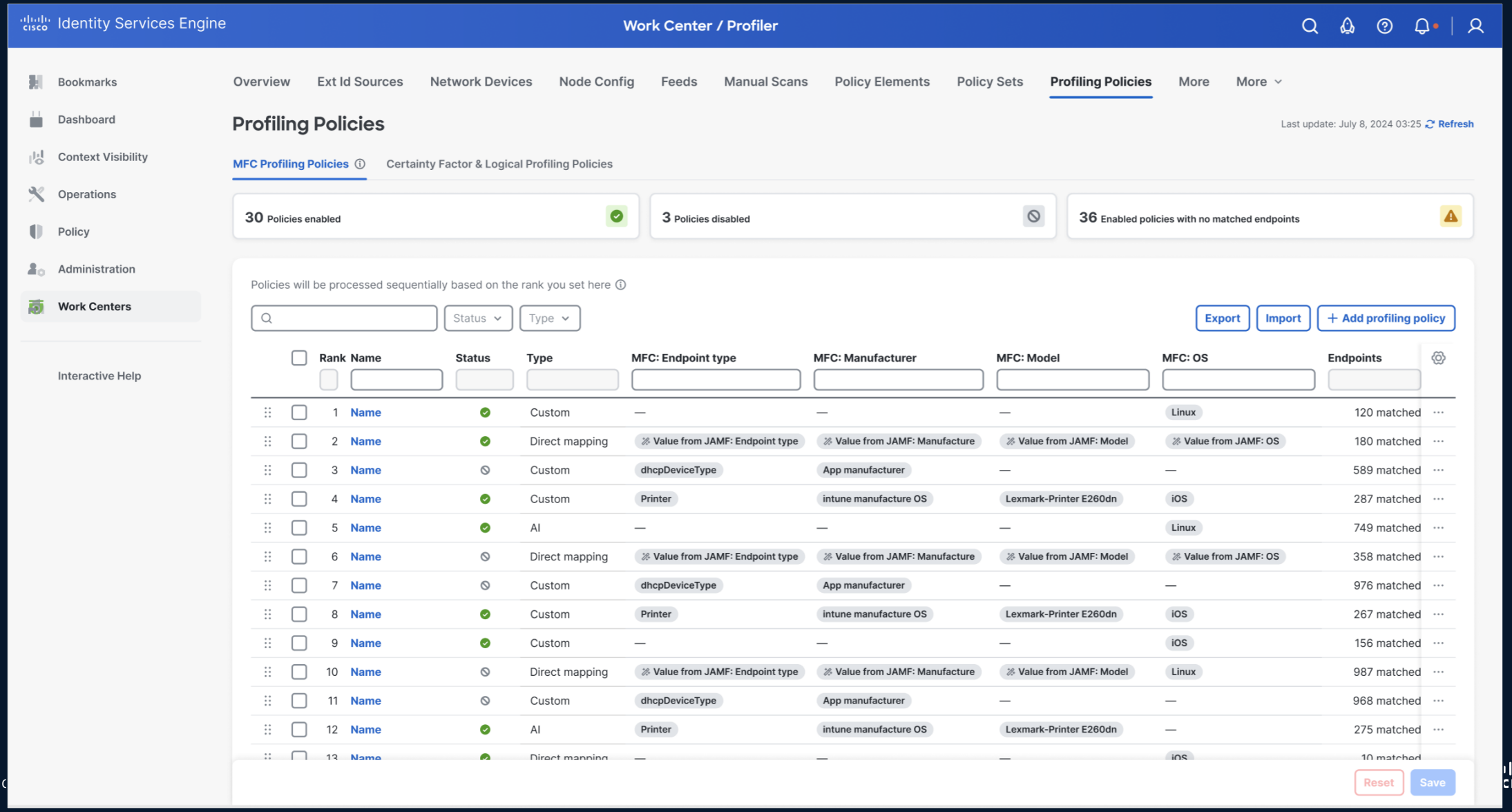
Cisco AI Analytics



New Context Visibility UI

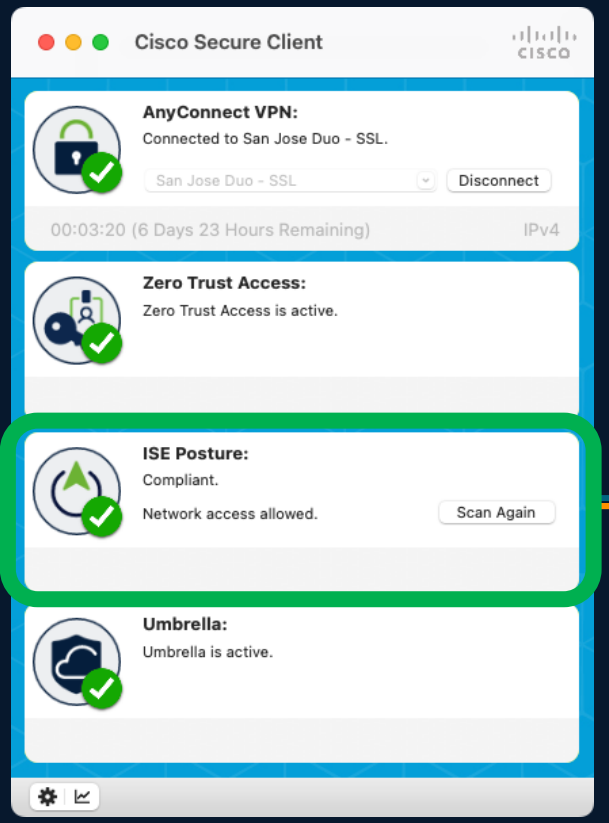


Improved Profiling Policy Management



Posturing for Compliance

ISE Posture with Cisco Secure Client



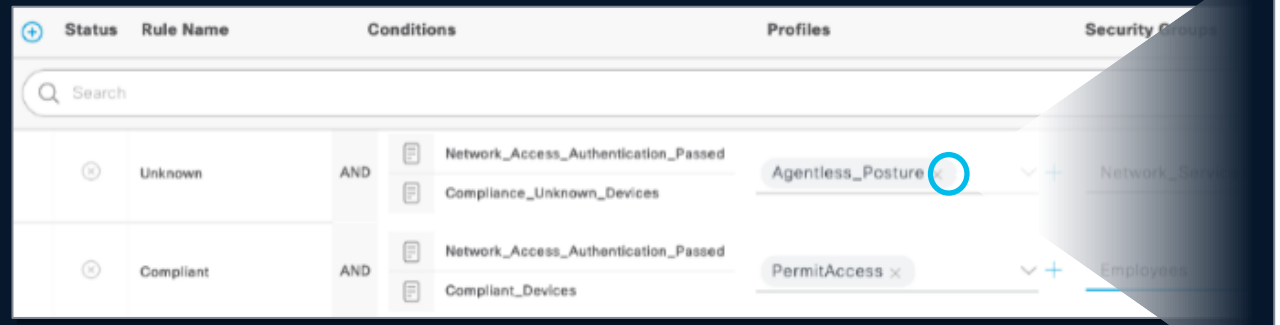
Checks

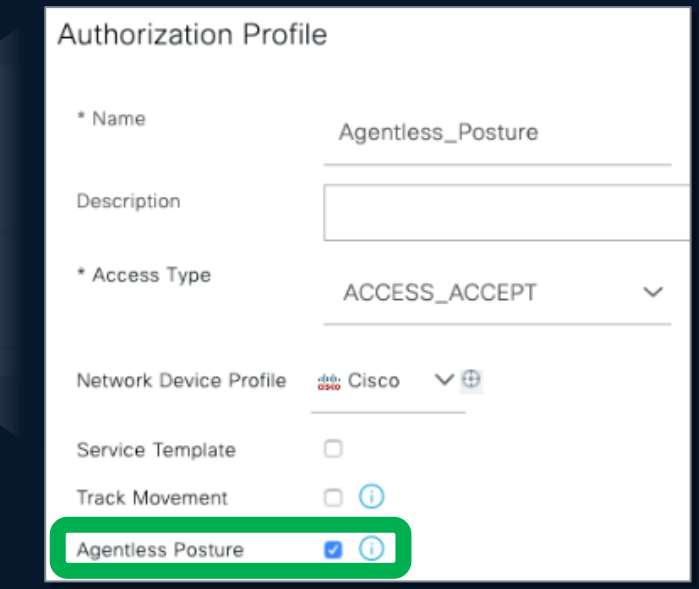
- **System Checks**
  - Hardware Inventory
  - USB Checks
  - File Checks
  - Registry Checks
  - Service Checks
  - Disk Encryption
- **Software/ Application Checks**
  - Application Checks
  - Application Inventory
  - Anti-Malware Checks
  - Firewall Installation Checks
- **Custom Scripts and external Conditions**
  - Custom scripts
  - External Conditions (AD, Location)
  - Compound condition support

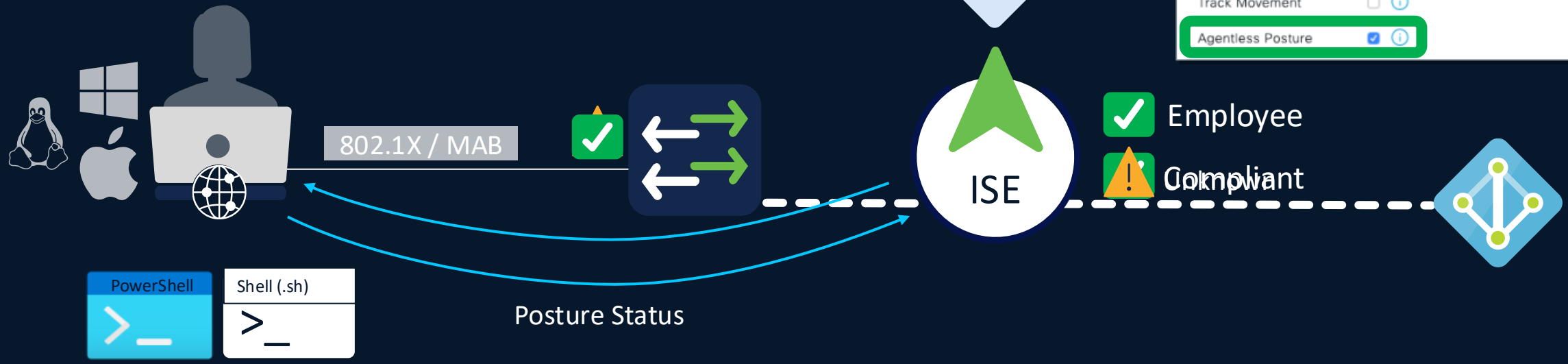
Remediations

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

Agentless Posture







Posture Deployment Options

✅ Supported
❗ Limitations
❌ Not Supported

Capability	Cisco Secure Client			AC 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	✅	❌	❌	✅	❌	✅	❌	✅	❌
WSUS remediation (legacy)	✅	N/A	N/A	✅	N/A	❌	❌	❌	❌
Remediation	Auto, Manual	Partial	Partial	Part Auto	Partial	Text	Text	❌	❌
Reassessment	✅	✅	✅	✅	✅	❌	❌	❌	❌

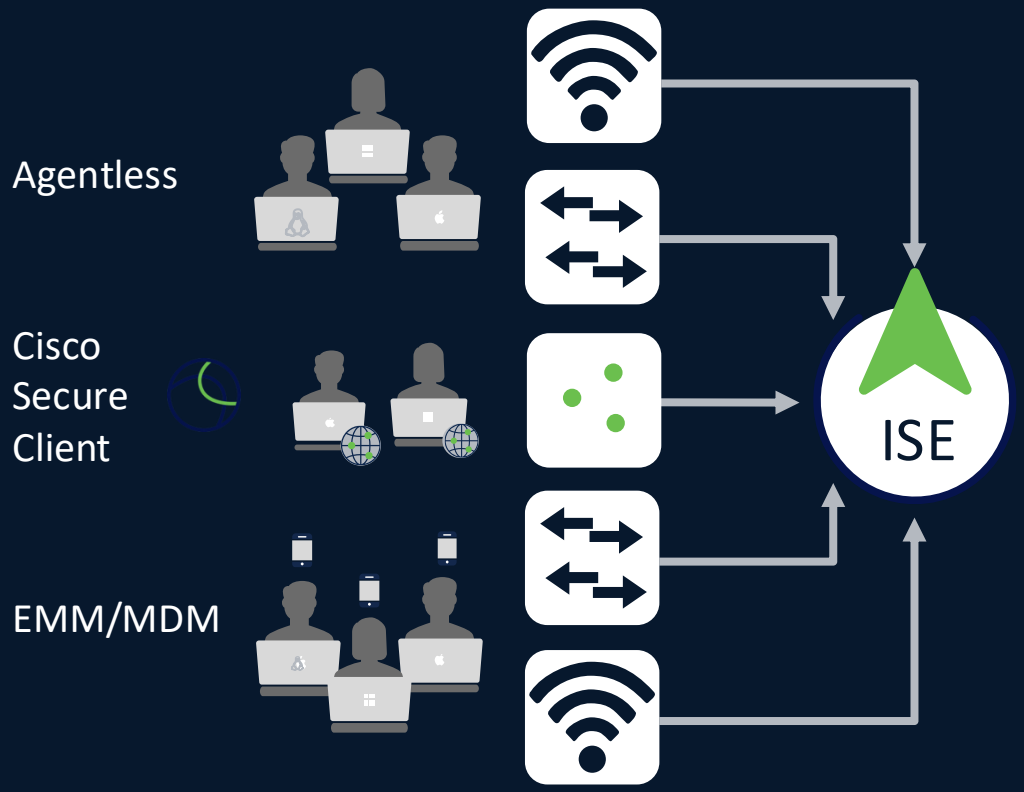
Visibility (Less Effort)

Experience (Less Time)

Security (More Protection)

Posture & Compliance

cisco.com/go/csta



Authorization Policy

IF JailBroken is No
AND PinLock is Yes
THEN Compliant

- Absolute Software
- SOPHOS
- GLOBO
- IBM Security
- Microsoft
- SOTI
- tangoe
- cisco Meraki
- Citrix XenMobile
- jamf
- SAP
- MobileIron
- Symantec
- airwatch by vmware

MDM Attributes

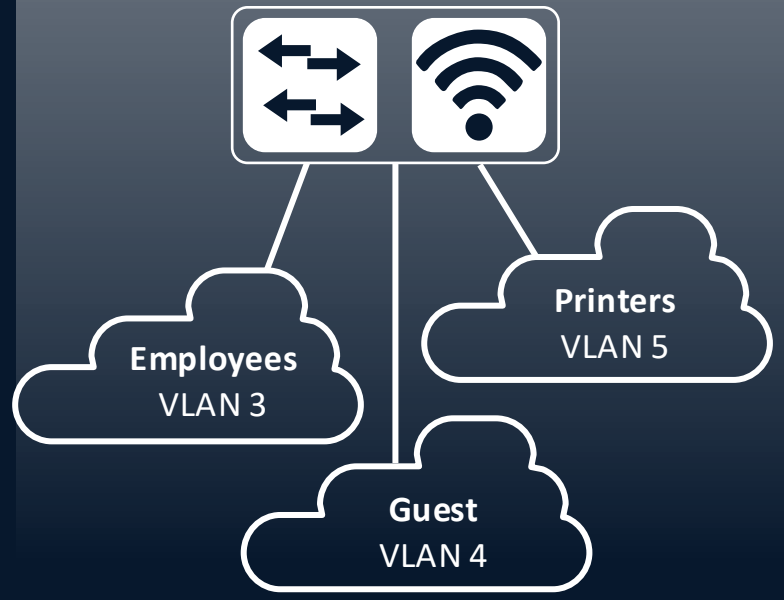
ActivityType
AdminAction
AdminActionUUID
AnyConnectVersion
DaysSinceLastCheckin
DetailedInfo
DeviceID
DeviceName
DeviceType
DiskEncryption
EndPointMatchedProfile
FailureReason
IdentityGroup
IMEI
IpAddress
JailBroken
LastCheckInTimeStamp
MacAddress
Manufacturer
MDMCompliantStatus
MDMFailureReason
MDMServerName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

Segmentation

ISE Segmentation Options

VLANs

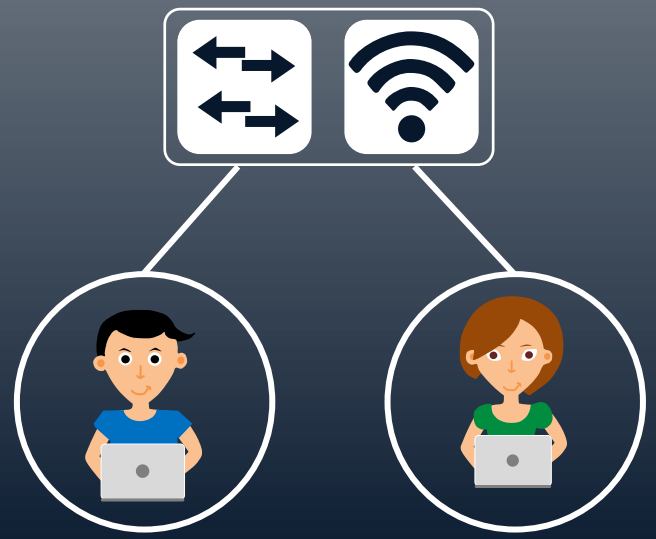
Dynamic VLAN Assignments



Per port / Per Domain / Per MAC

ACLs: DL, Named, DNS

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

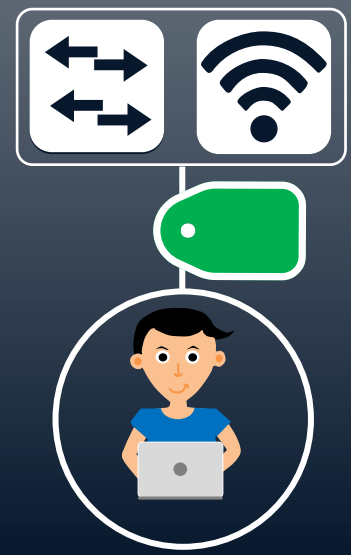


Employee
`permit ip any any`

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

Security Group Tags

Cisco Group-Based Policy

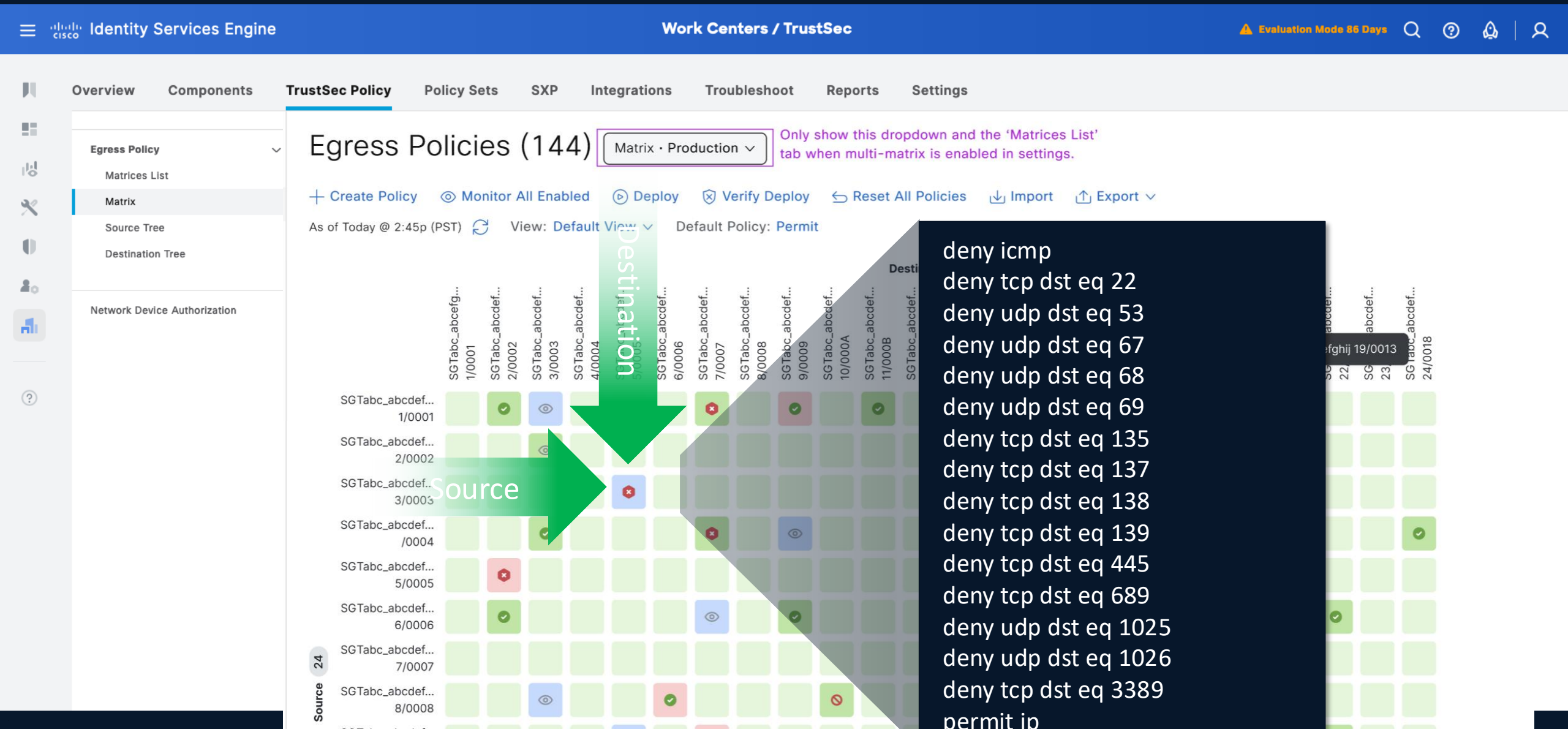


16-bit SGT assignment and SGT based Access Control

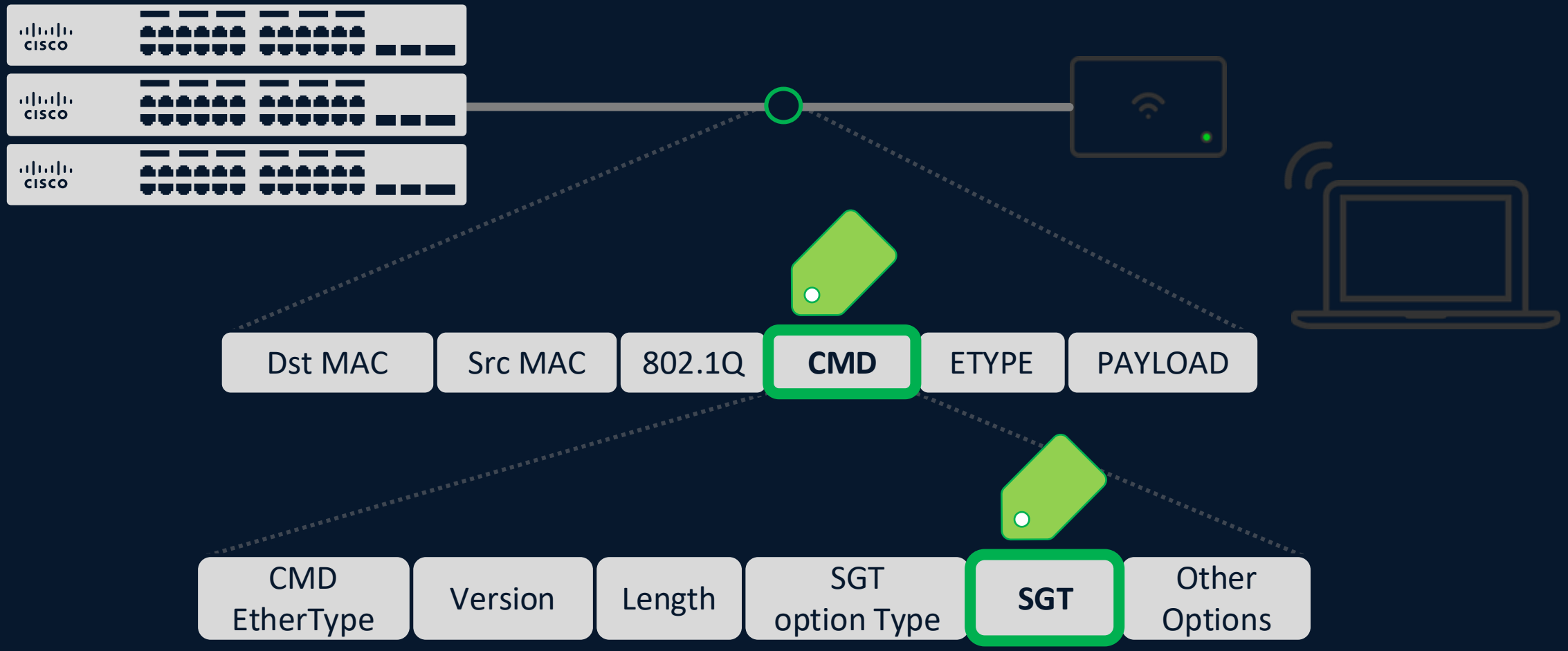
Can You See the Business Intent Here?

```
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
```

Business Intent is Clear



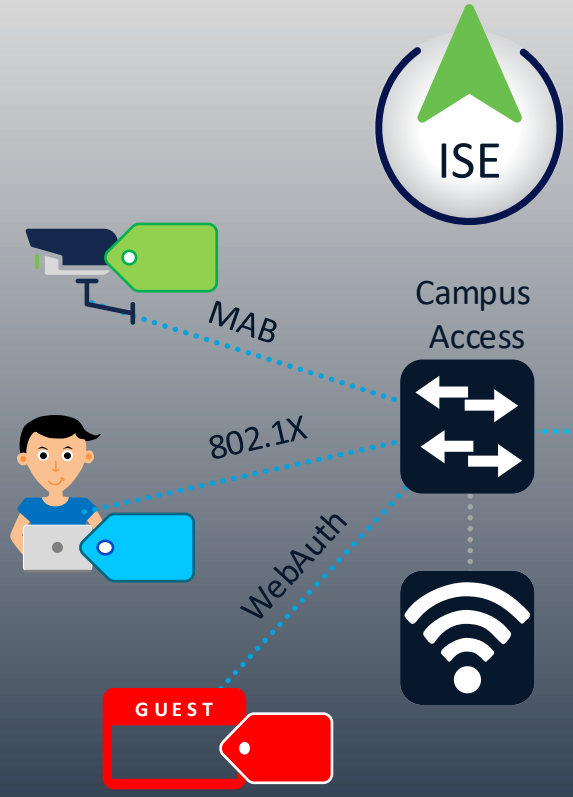
Security Group Tags (SGTs)



Classification Mechanisms

Classification — Propagation — Enforcement

Dynamic Classification



Static Classification

L3 Interface (SVI) to SGT

IP to SGT

L2 Port to SGT

Distribution

Core

Enterprise Backbone

DC Core

DC Access

WLC

Firewall

Hypervisor SW

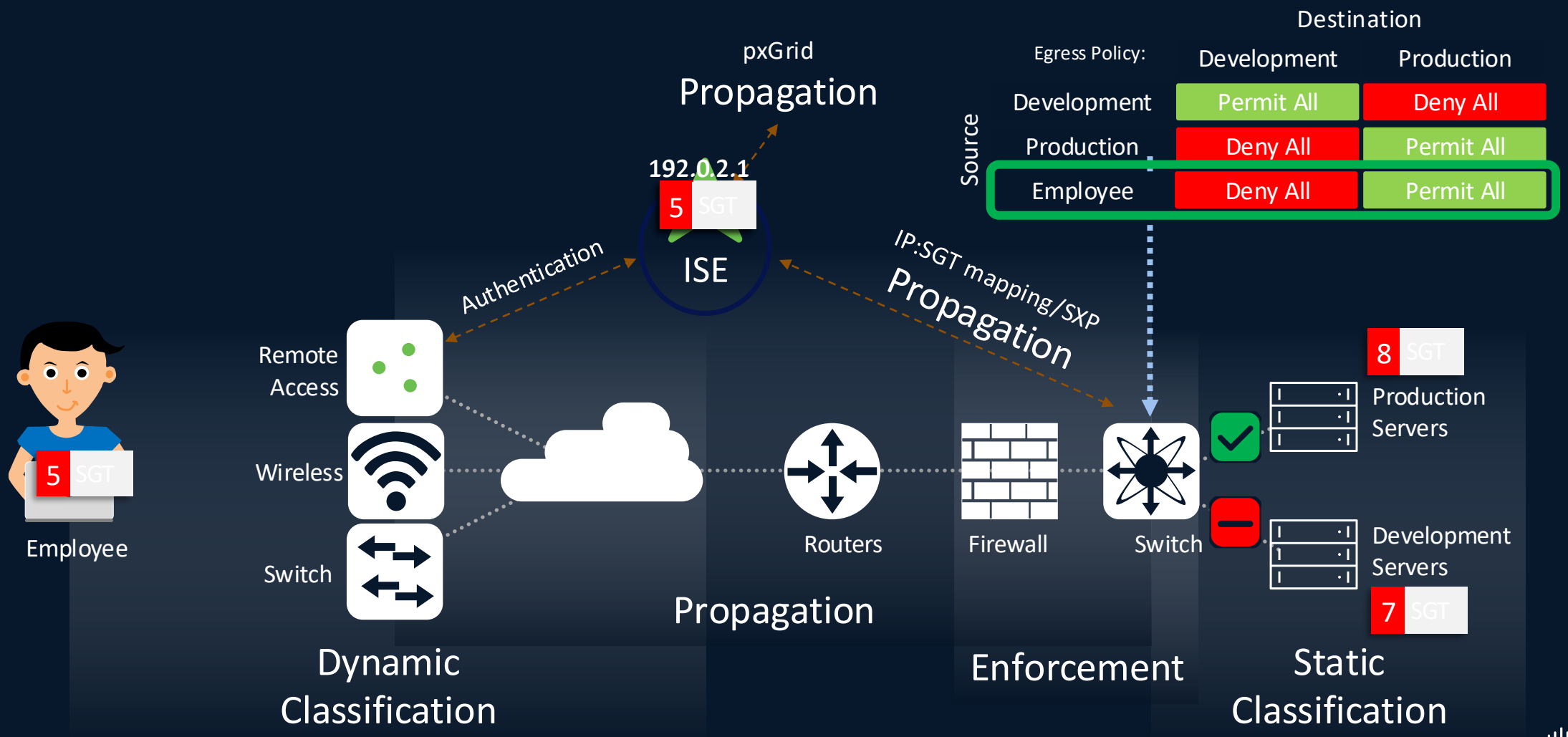
VLAN to SGT

Subnet to SGT

VM (Port Profile) to SGT

cisco

Cisco SGT Propagation & Enforcement



Integrations to Automate Policy

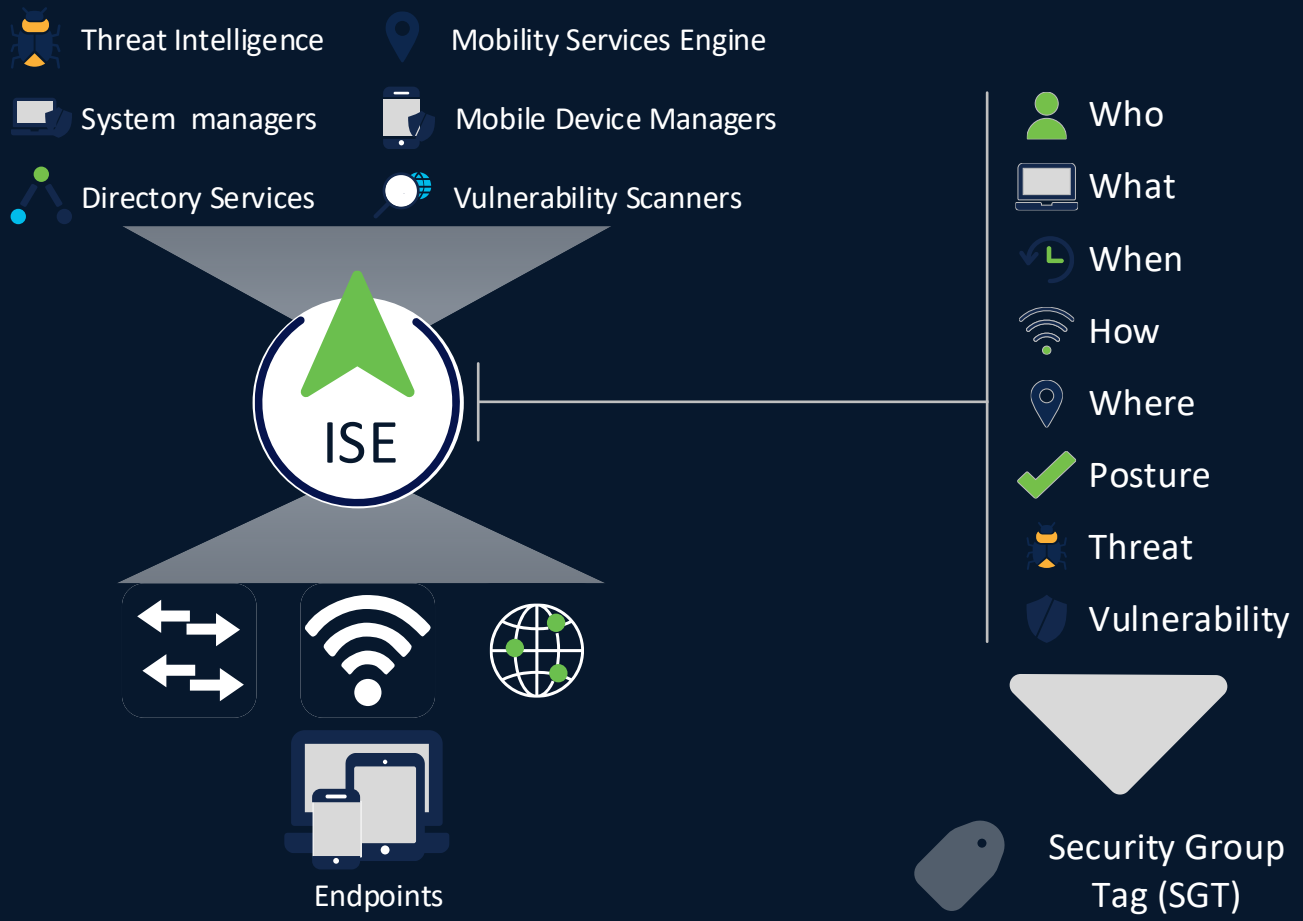
Platform Exchange Grid (pxGrid)

- Open and scalable Security Product Integration Framework (SPIF) that allows for bi-directional any-to-any partner platgorm 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
  - But also check out developer.cisco.com/site/pxgrid

Context Build, Summarize, Exchange with pxGrid

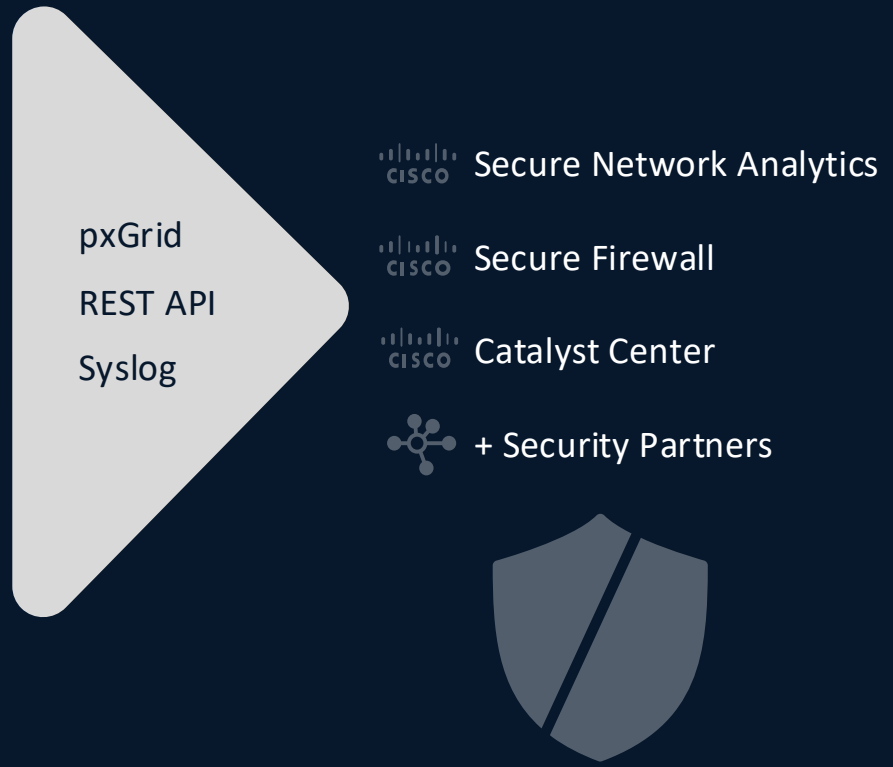
Visibility and Access Control

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 it's identity (pxGrid) certificate

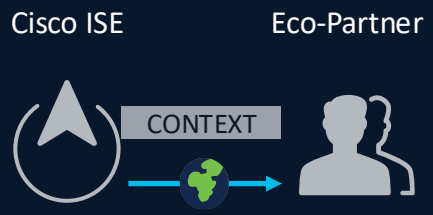
4. ISE will authenticate itself back to the client with its own pxGrid certificate

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

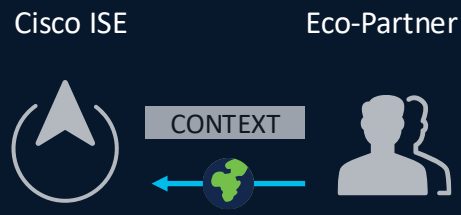
Context Sharing with pxGrid

Context to Partner



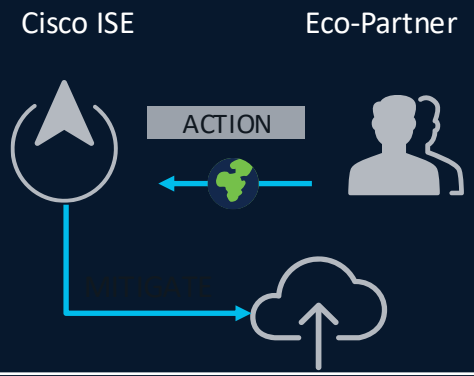
ISE makes Customer IT Platforms User/Identity, Device and Network Aware

Enrich ISE Context



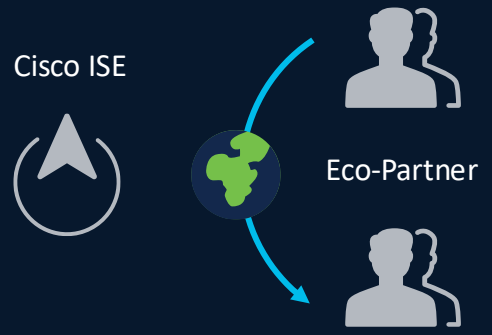
Enrich ISE context. Make ISE a better Policy Enforcement Platform

Threat Mitigation



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

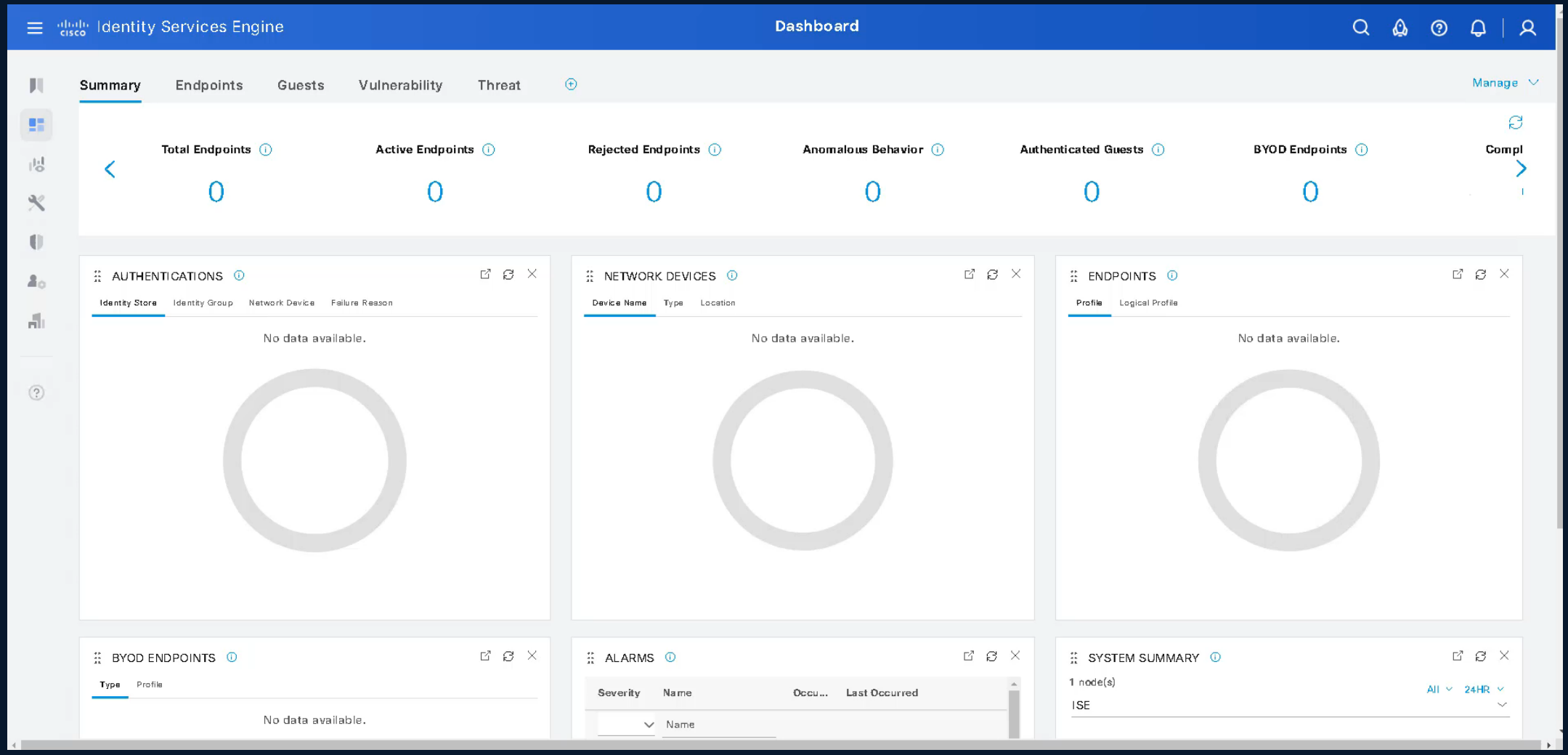
Context Brokerage



ISE 2.2+

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

pxGrid/ANC Policies in ISE



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…

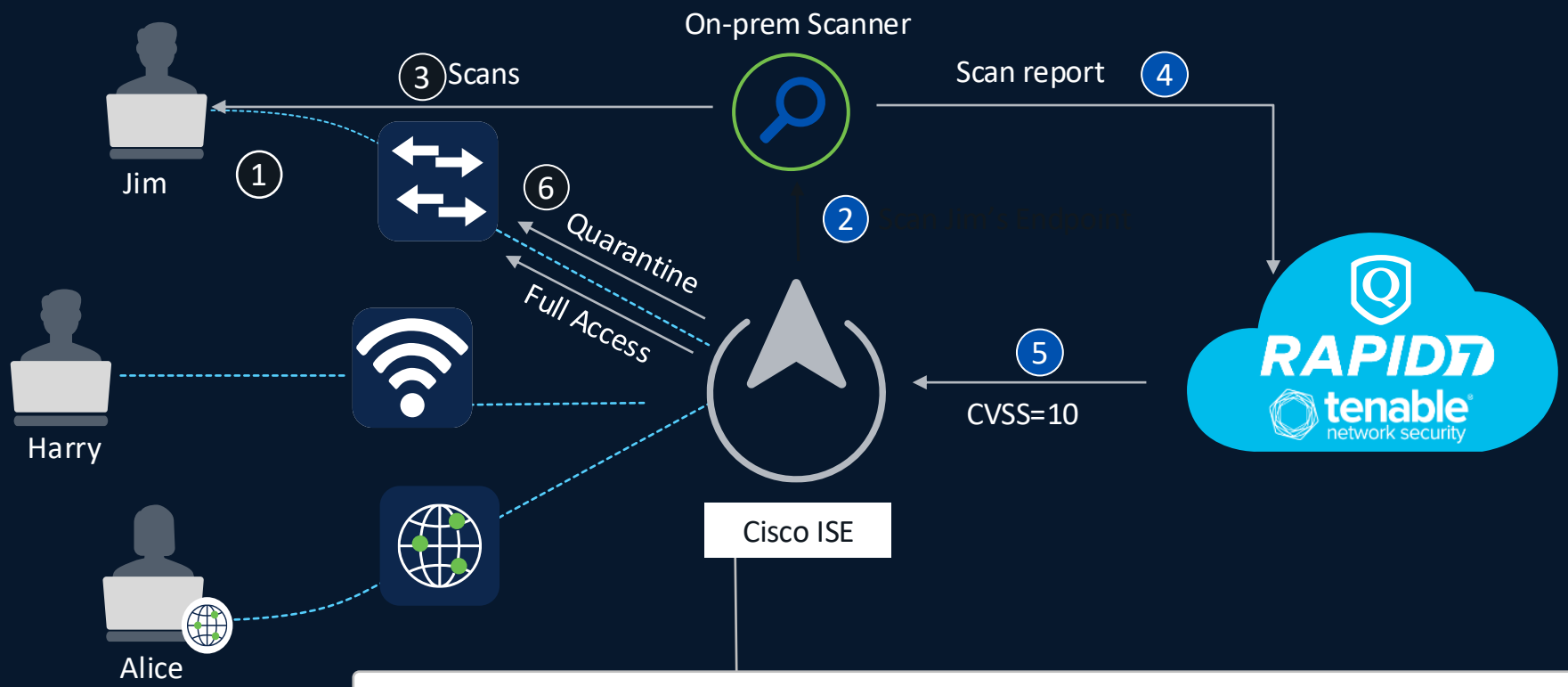
pxGrid Integration Tips

- 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

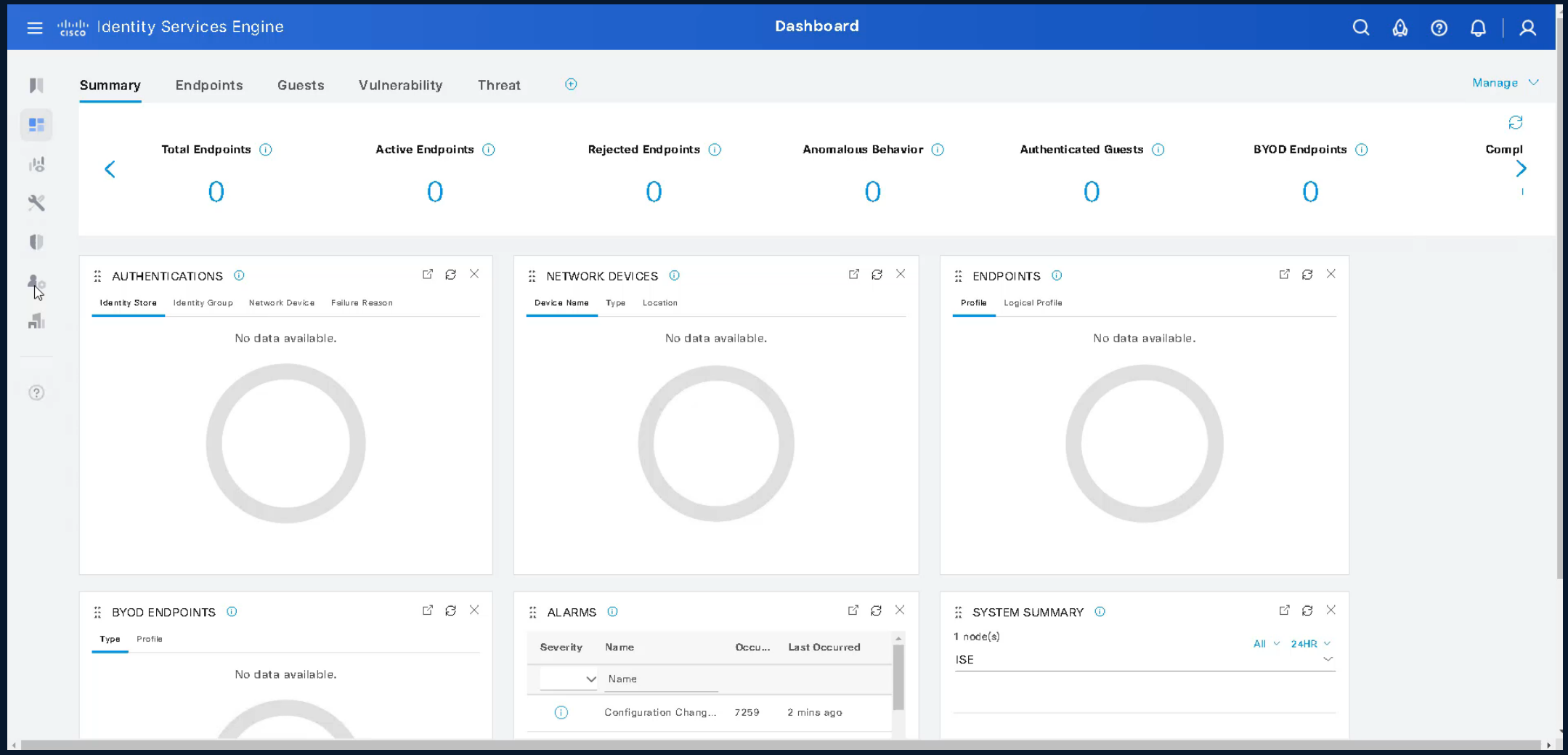
CVSS: Common Vulnerability Scoring System

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

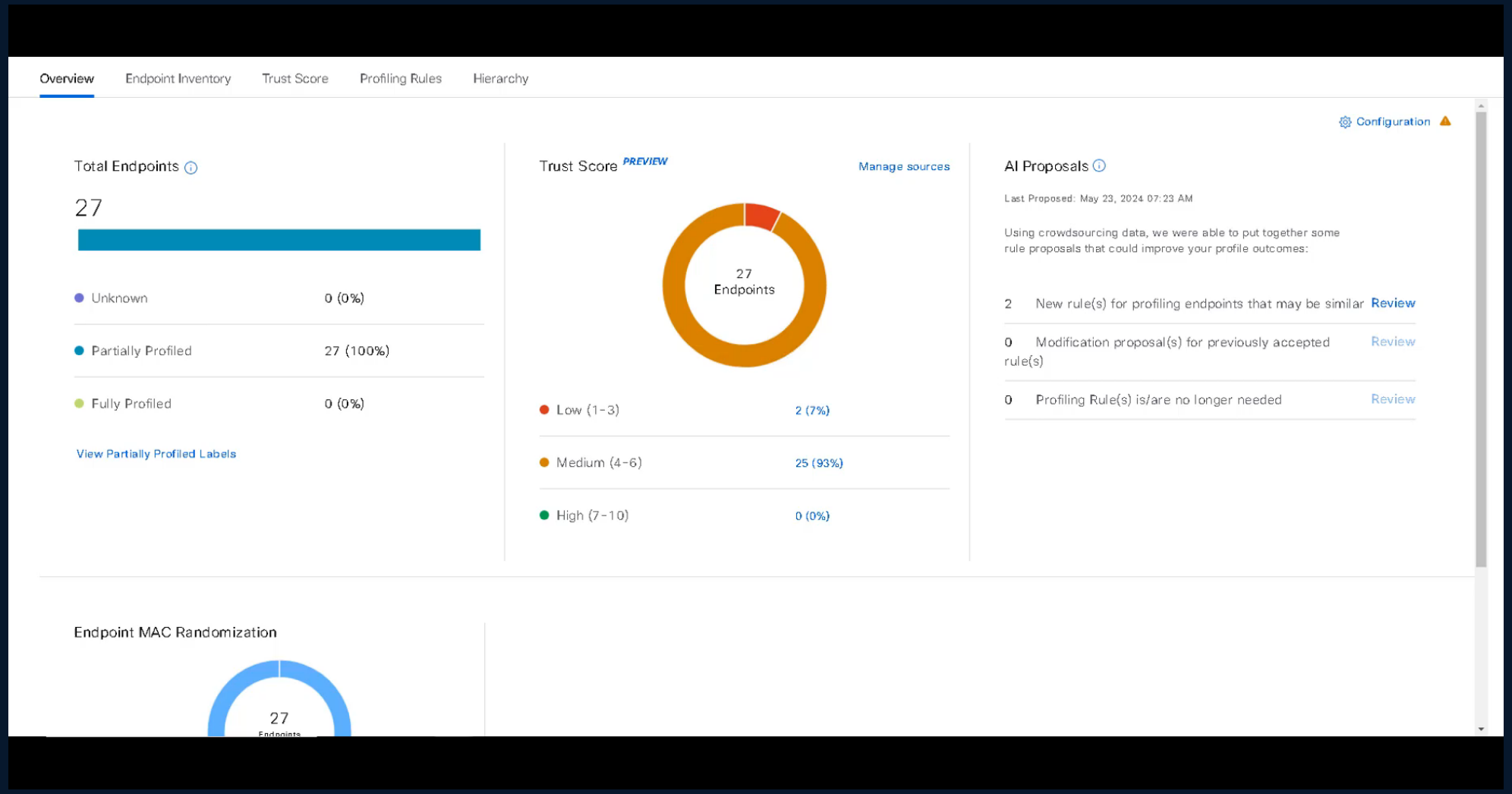


ISE APIs and Automation

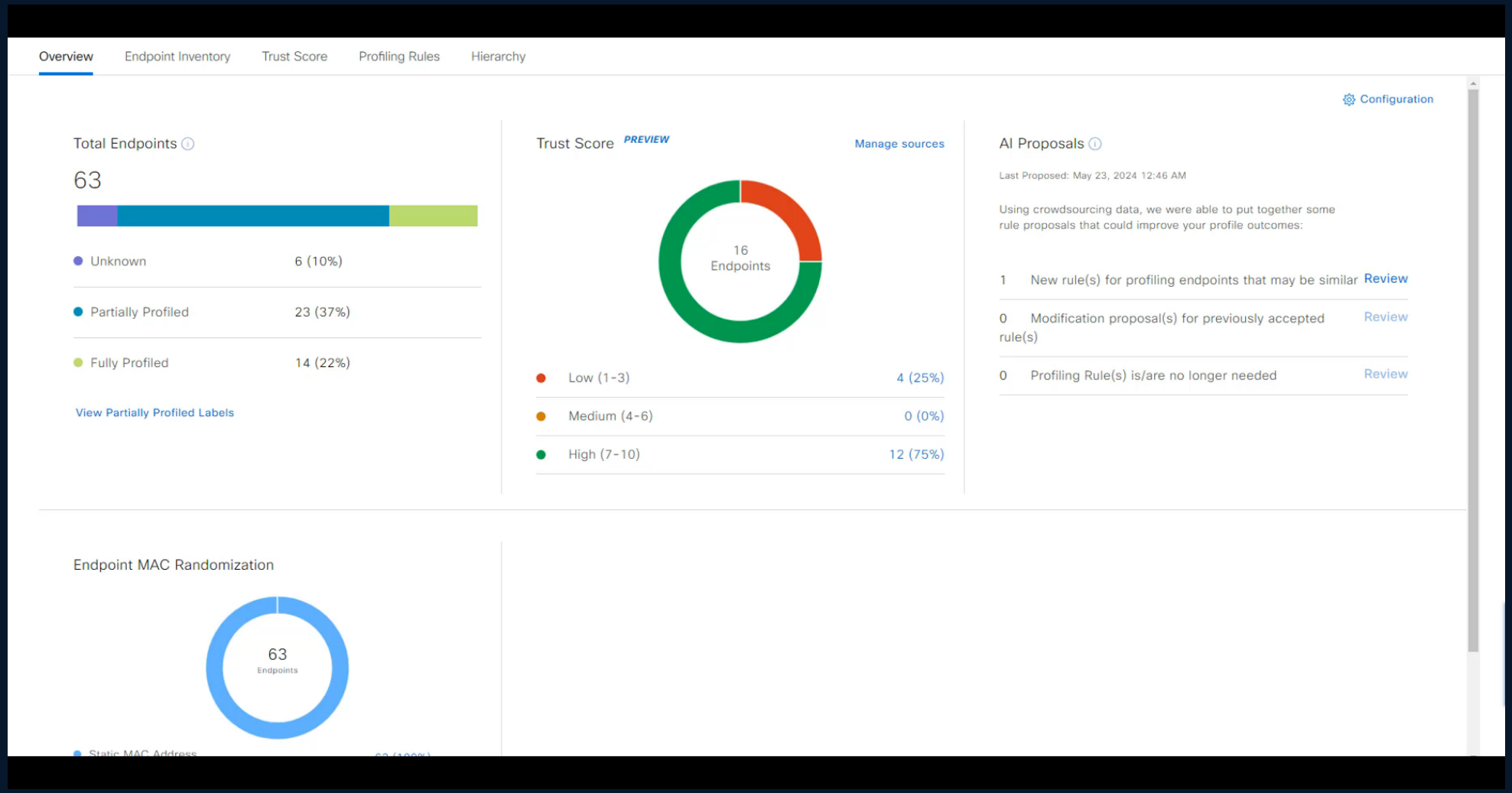
Integration Example: Catalyst Center and ISE

- 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