

# End-to-End Micro-Segmentation & Agent Security Part 1:

## Zero Trust in the Campus



Chase Abrams

Jacob Schneider

October 15, 2025

# Cisco Segmentation Specialists – US Commercial

Helping customers simplify and scale segmentation across identity, network, and workload.



Chase Abrams –  
Principal Advisor, Segmentation



Jacob Schnieder–  
Segmentation Solutions Architect

- 11 years @ Cisco, 19 years in Enterprise Security & Networking Sales
- Deep experience across US Commercial, Global Enterprise, & Service Provider
- Specializes in Zero Trust, Segmentation, and Unified Security Architecture
- Background in Security & DC solutions
- Based in Boulder, CO

- 22+ years of experience designing & deploying Cisco Security & Networking solutions
- 12 years @ Cisco
- Cisco Live Distinguished Speaker & recognized CCIE (#24940)
- Deep Background in Service Provider & Security architectures
- Based in Miami, FL

# Cisco Live 2025 *Pre-Event Customer Survey*

## Top Business Priorities

1. Improving Cybersecurity
2. Automation
3. Cost Reduction & Efficiency
4. Customer Experience
5. Digital Transformation

## Cisco Value Proposition Familiarity

**81%**

are somewhat-not at all familiar with Cisco's strategy around **AI-ready data centers**.

**68%**

are somewhat-not at all familiar with Cisco's strategy around **future-proofed workplaces**.

**60%**

are somewhat-not at all familiar with Cisco's strategy around **digital resilience**.

## IT Strategy & Roadmap Focus Areas

Security

Automation

AI

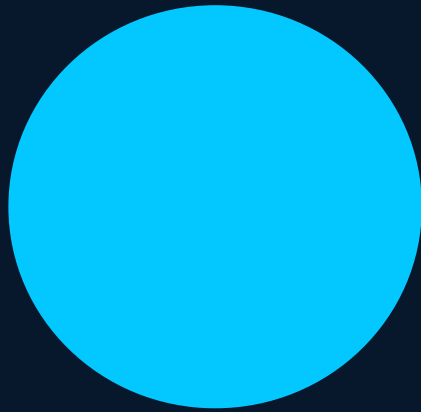
Wireless & Mobility

Campus Networking Infrastructure

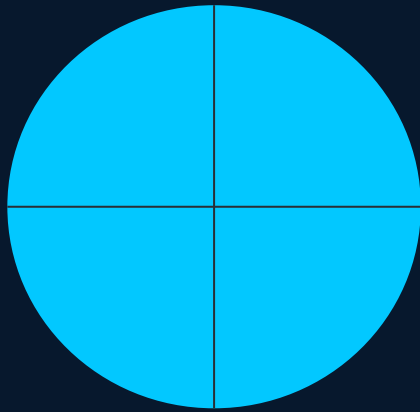
Data Center Infrastructure

# What is Segmentation?

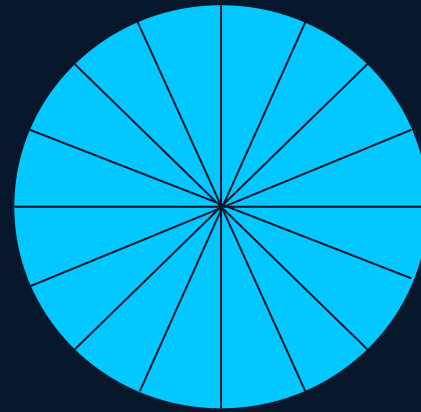
*“ Segmentation is the practice of dividing a larger system into smaller, isolated parts to improve control, security, and performance.”* – CIRCUIT (a.k.a BridgeIT).



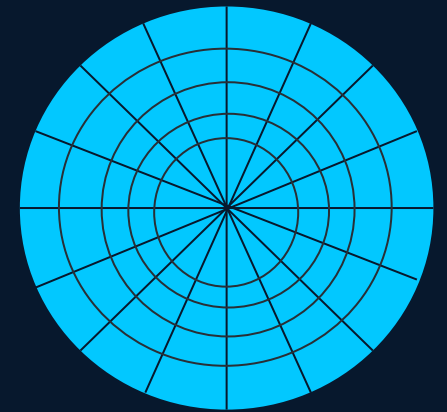
No Segmentation



Macro Segmentation

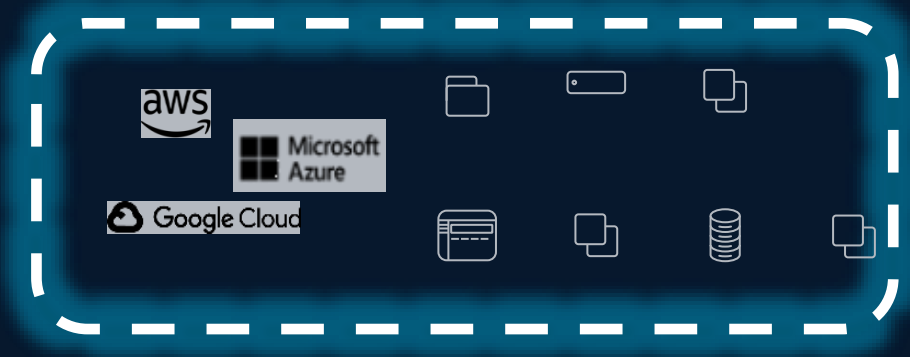
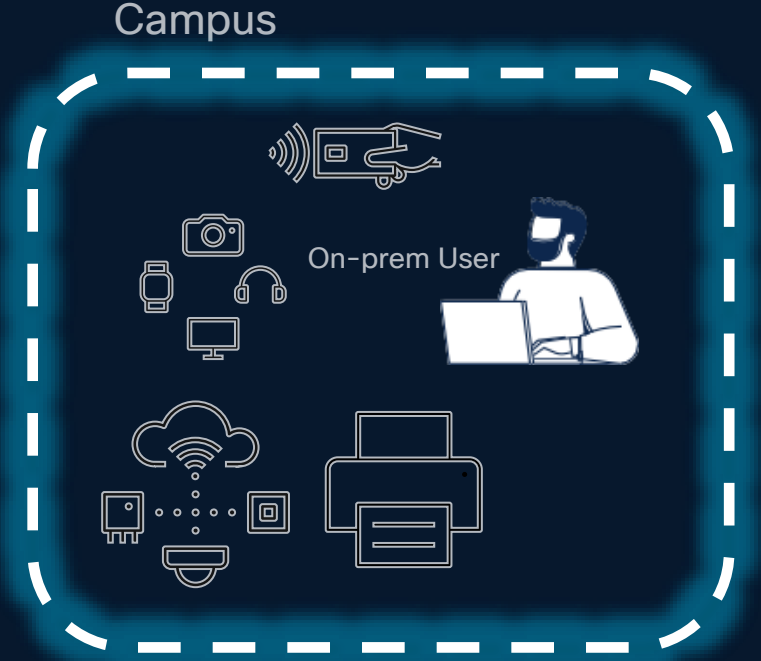


Micro Segmentation

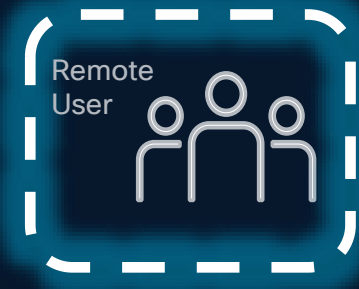
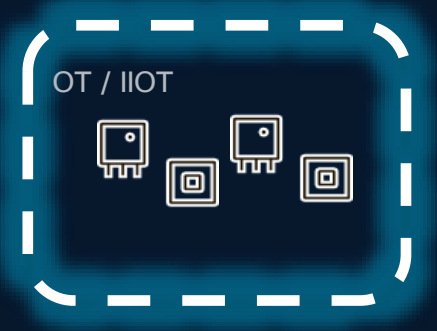
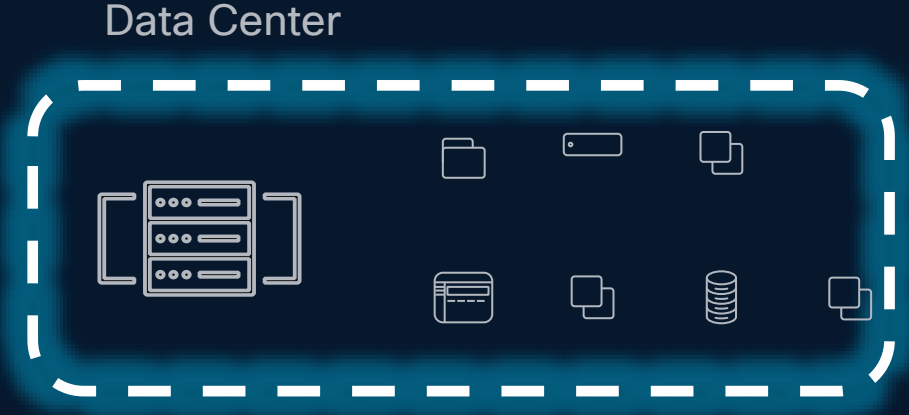


Nano Segmentation??

# Segmentation Domains



Cloud / SaaS





Security is a patchwork



# Segmentation is a solution, but it is complex.

Cisco is dedicated to solving customers' needs



People, process and technology



Scale, speed and granularity



Customers need flexibility and choice to address unique scenarios

### Why it matters to our customers

- App modernization and multicloud adoption
- Ransomware threat – contain lateral movement
- Meet compliance requirement
- Automation at scale
- Visibility



# Cisco intent-based access in the Campus

Cisco's campus intent-based access that lets you:

**See**  
Users, endpoints and applications



**Secure**  
By controlling network access and segmentation

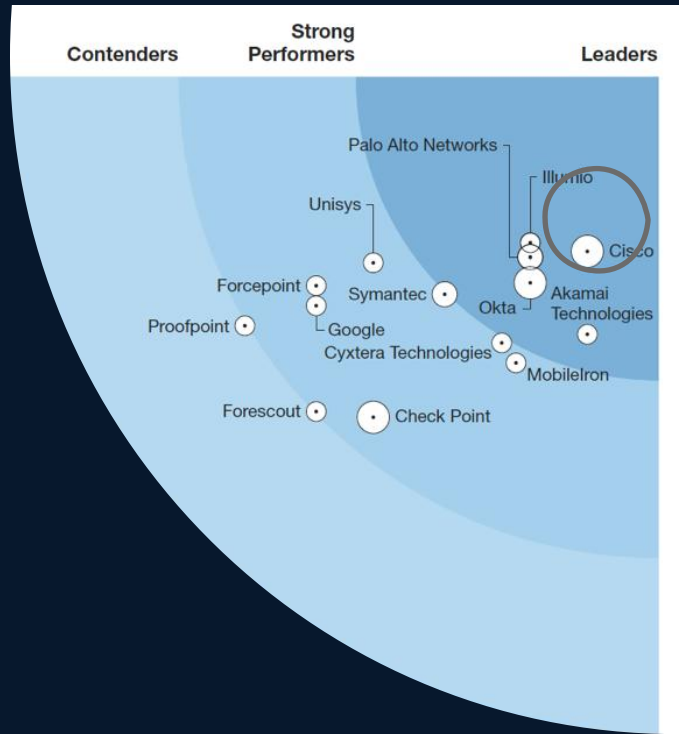


**Share**  
Context with partners for enhanced operations



# ISE is the access control and policy enforcement market leader

#1 in Forrester Wave ZT ranking



ISE Market Maturity

10+ yrs  
of market leadership

75,000+  
Deployments

4.8%  
Market Share  
-Gartner

ISE as a Control Point

Secure Networking  
ISE is the enabler of Segmentation for Catalyst and Meraki

Zero Trust  
ISE is a critical control point.

ISE is the Bridge  
ISE sits between Networking and Security

# Why Customers Buy ISE



## Device Administration

**TACACS+** Allows for secure, identity-based access to the network devices

<https://cs.co/ise-tacacs>



## Secure Access

Secure wired, wireless, or VPN access using industry standard protocols **RADIUS** and **802.1X**

<https://cs.co/ise-wired>



## Guest Access

Choose from Hotspot, Self-Registered Guest, and Sponsored Guest access options

<https://cs.co/ise-guest>



## Asset Visibility

Use the probes in ISE and Cisco devices to classify endpoints and authorize them

<https://cs.co/ise-profiling>



## Compliance & Posture

Use **agentless posture**, **Cisco Secure Client**, **MDM**, or **EMM** to check endpoints' posture

<https://cs.co/ise-posture>



## Context Exchange

Integrate applications and vendors with ISE for endpoint identity, context, and automated Enforcement

<https://cs.co/ise-pxgrid>



## Segmentation

**Group-based Policy** with Security Group Tags (SGT) and Security Group ACLs (SGACL) instead of VLAN/ACLs

<https://cs.co/segmentation-resources>



## Cisco Catalyst Center

ISE integrates with **Catalyst Center** to automate the network fabric and policies using SDA

<https://cs.co/ise-ccc>



## EMM/MDM

Endpoint Management is required for provisioning endpoints with certificates and controls for secure network access

<https://cs.co/ise-mdm>



## Threat Containment

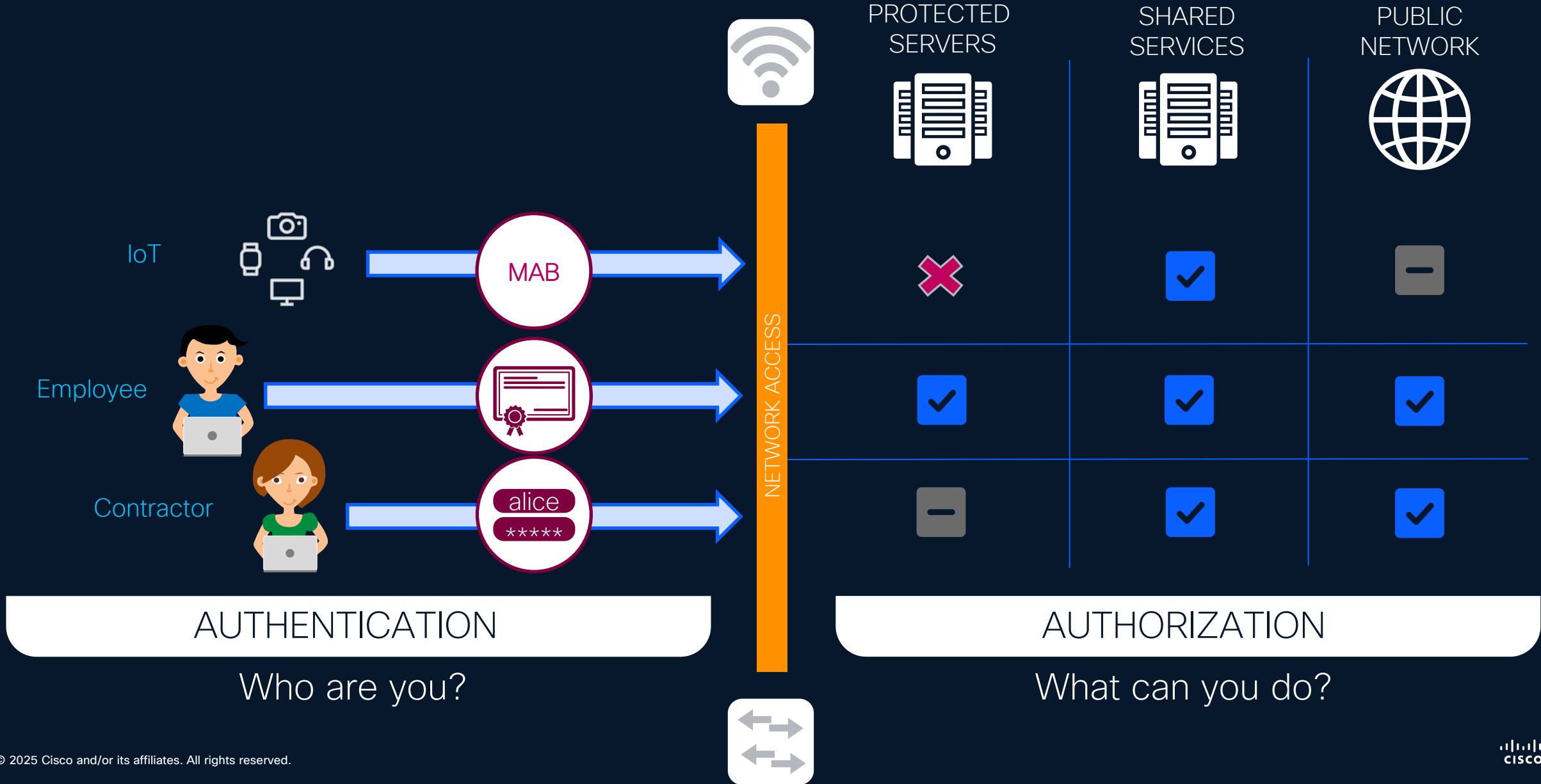
Use Threat Analysis tools to grade an endpoint's threat score and automatically quarantine it if

<https://cs.co/ise-tnac>



# Campus Segmentation

# Authentication and Authorization

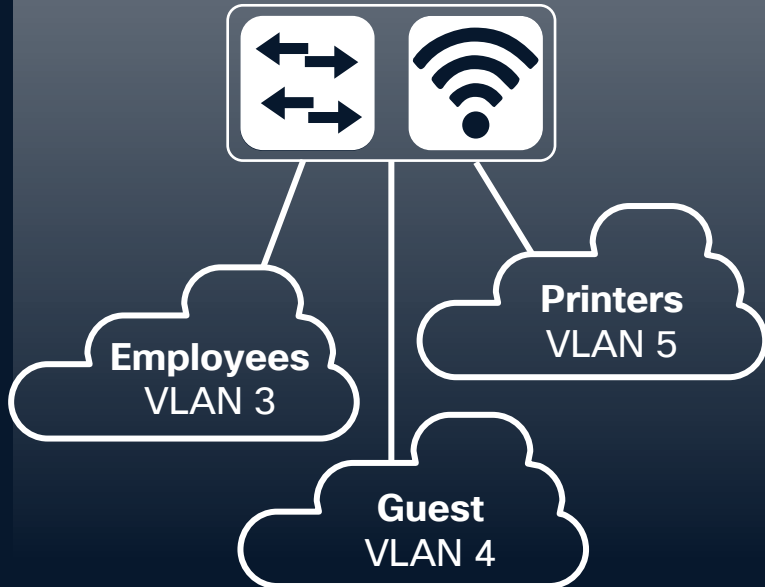


# ISE Segmentation Options

Beyond RADIUS Access-Accept / Access-Reject

## VLANs

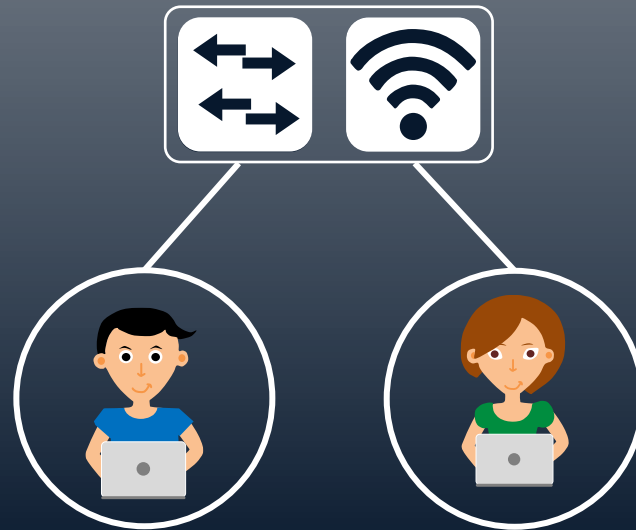
Dynamic VLAN Assignments



Per port / Per Domain / Per MAC

## ACLs: DL, Named, DNS

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



**Employee**

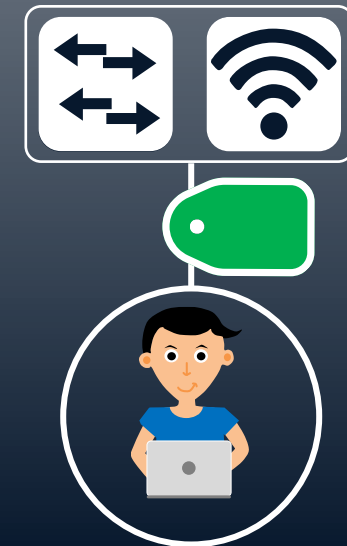
```
permit ip any any
```

**Contractor**

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

## Security Group Tags

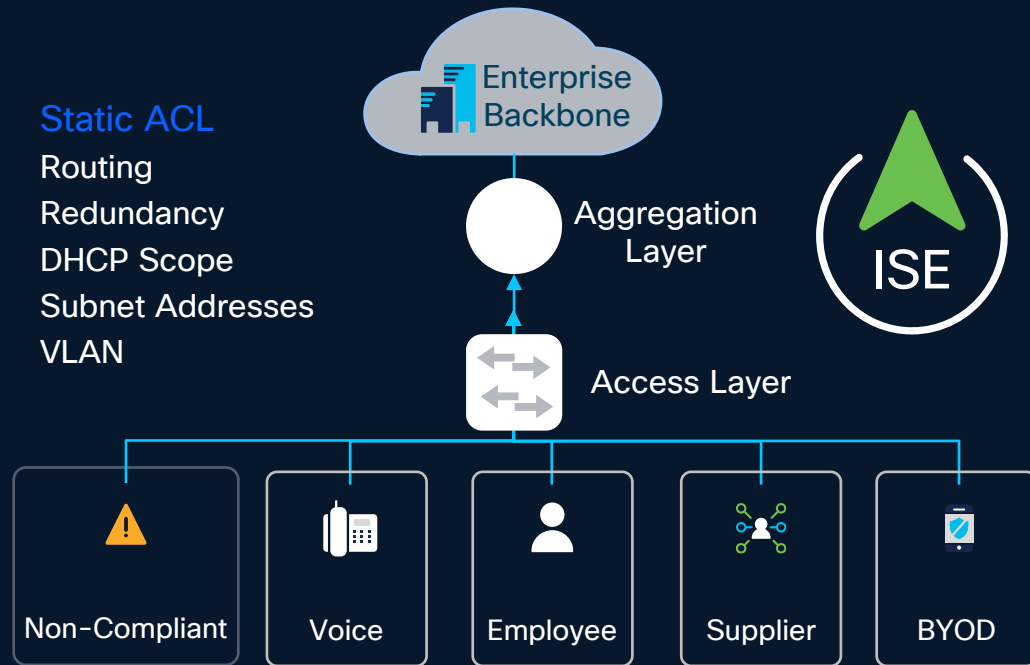
Cisco Group-Based Policy



16-bit SGT assignment and  
SGT based Access Control

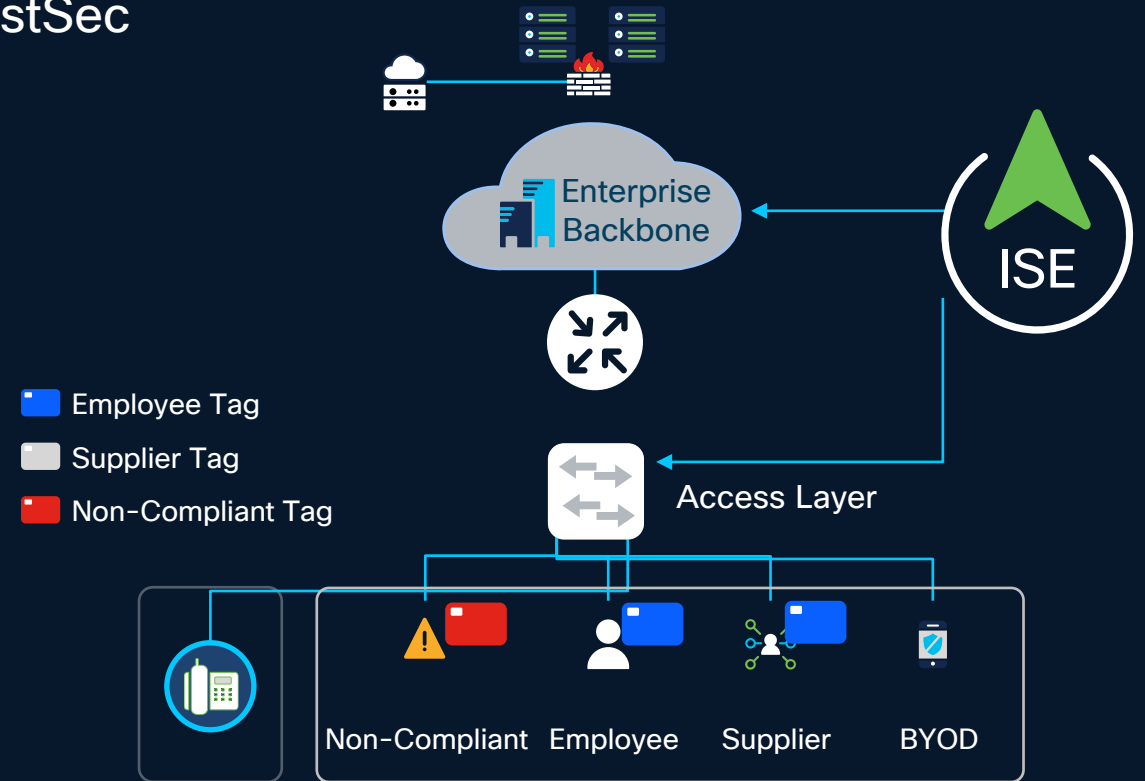
# Group Based Policy Simplifies Segmentation

## Traditional Segmentation



Security Policy based on Topology  
High cost and complex maintenance

## TrustSec



Use existing topology and automate  
security policy to reduce OpEx

# 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 with TrustSec

Identity Services Engine Work Centers / TrustSec Evaluation Mode 86 Days

Overview Components **TrustSec Policy** Policy Sets SXP Integrations Troubleshoot Reports Settings

## Egress Policies (144) Matrix · Production

Only show this dropdown and the 'Matrices List' tab when multi-matrix is enabled in settings.

+ Create Policy Monitor All Enabled Deploy Verify Deploy Reset All Policies Import Export

As of Today @ 2:45p (PST) View: Default View Default Policy: Permit

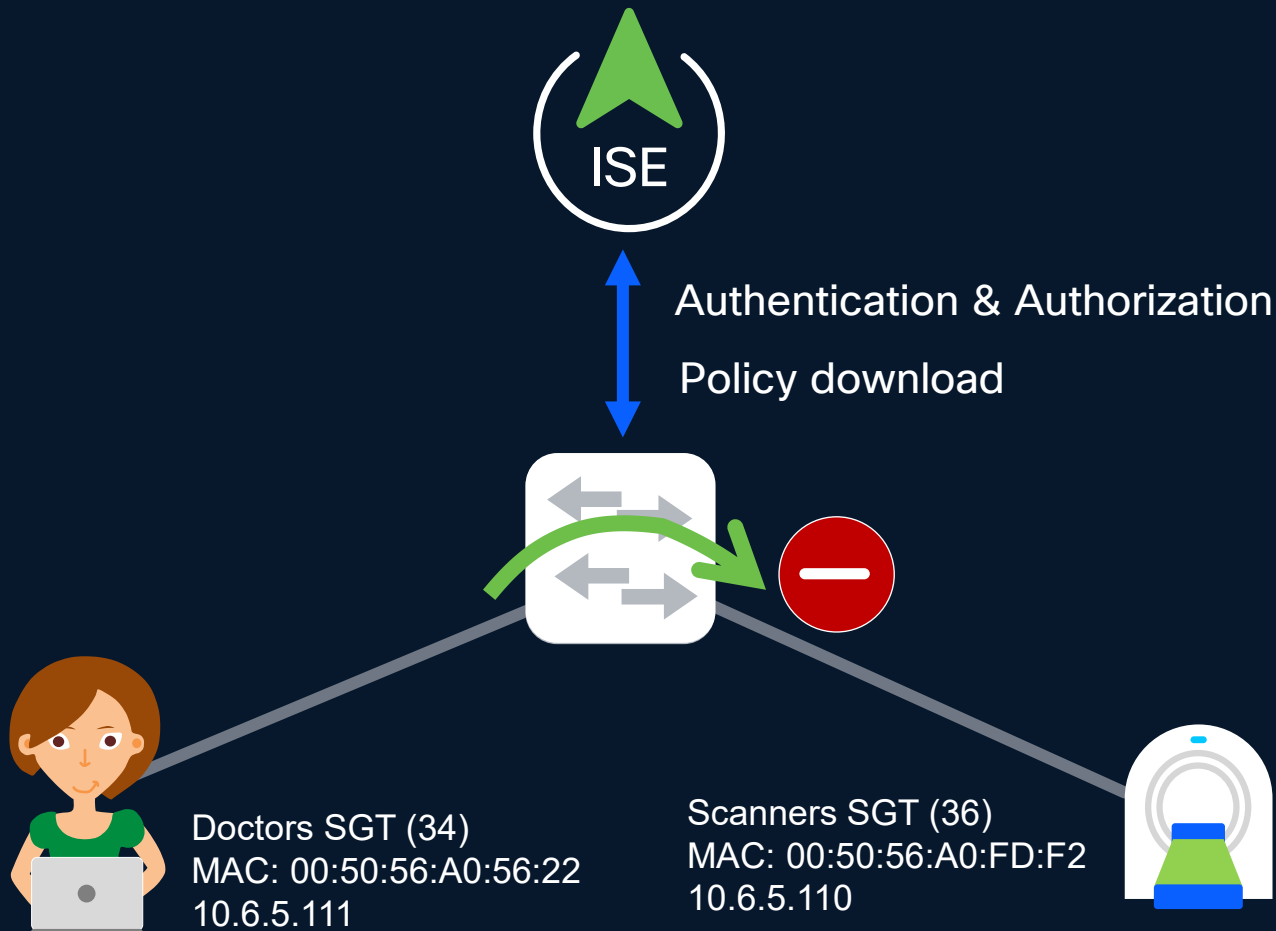
Source	1/0001	2/0002	3/0003	4/0004	5/0005	6/0006	7/0007	8/0008	9/0009	10/000A	11/000B	12/000C	13/000D	14/000E	15/000F	16/000G	17/000H	18/000I	19/0013	20/0014	21/0015	22/0016	23/0017	24/0018
SGTabc_abcdef... 1/0001	✓	✓	👁	👁	✖	✓	✖	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
SGTabc_abcdef... 2/0002	✓	👁	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
SGTabc_abcdef... 3/0003	✓	✓	✖	✖	✖	✓	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖
SGTabc_abcdef... 4/0004	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
SGTabc_abcdef... 5/0005	✓	✖	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
SGTabc_abcdef... 6/0006	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
SGTabc_abcdef... 7/0007	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
SGTabc_abcdef... 8/0008	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
SGTabc_abcdef... 9/0009	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
SGTabc_abcdef... 10/000A	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
SGTabc_abcdef... 11/000B	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
SGTabc_abcdef... 12/000C	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
SGTabc_abcdef... 13/000D	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
SGTabc_abcdef... 14/000E	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
SGTabc_abcdef... 15/000F	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
SGTabc_abcdef... 16/000G	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
SGTabc_abcdef... 17/000H	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
SGTabc_abcdef... 18/000I	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
SGTabc_abcdef... 19/0013	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
SGTabc_abcdef... 20/0014	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
SGTabc_abcdef... 21/0015	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
SGTabc_abcdef... 22/0016	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
SGTabc_abcdef... 23/0017	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
SGTabc_abcdef... 24/0018	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

deny icmp  
deny tcp dst eq 22  
deny udp dst eq 53  
deny udp dst eq 67  
deny udp dst eq 68  
deny udp dst eq 69  
deny tcp dst eq 135  
deny tcp dst eq 137  
deny tcp dst eq 138  
deny tcp dst eq 139  
deny tcp dst eq 445  
deny tcp dst eq 689  
deny udp dst eq 1025  
deny udp dst eq 1026  
deny tcp dst eq 3389  
permit ip

© 2025 Cisco and/or its affiliates. All rights reserved.

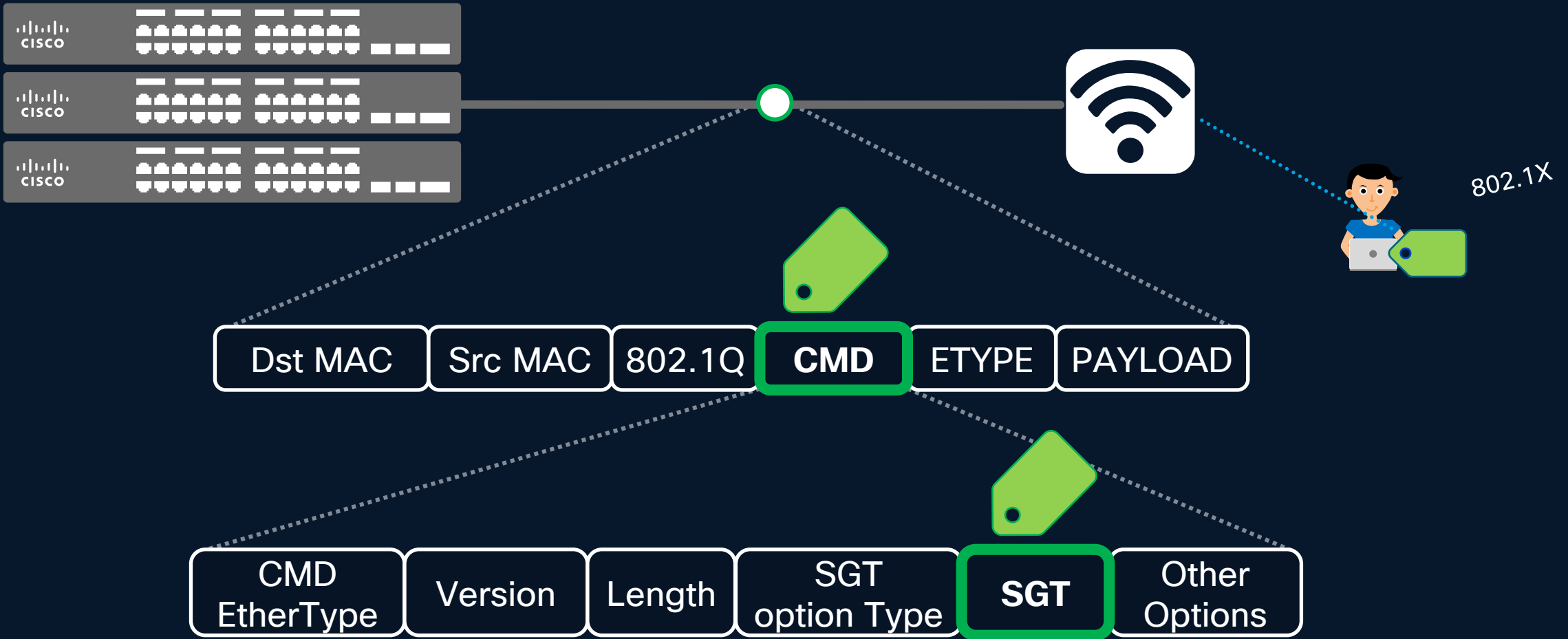
# Classification, SGT Lookup and Enforcement

- Classification: Dynamic/ISE
- Src SGT found, Dst SGT found
- Enforcement: At Egress



		Destination	
Egress Policy		Doctors	Scanners
Source	Doctors	Permit All	Deny All
	Guests	Deny All	Deny All
	Scanners	Deny All	Permit All

# TrustSec Security Group Tags (SGTs)



# TrustSec Security Group Tags (SGTs)

Classification

Propagation

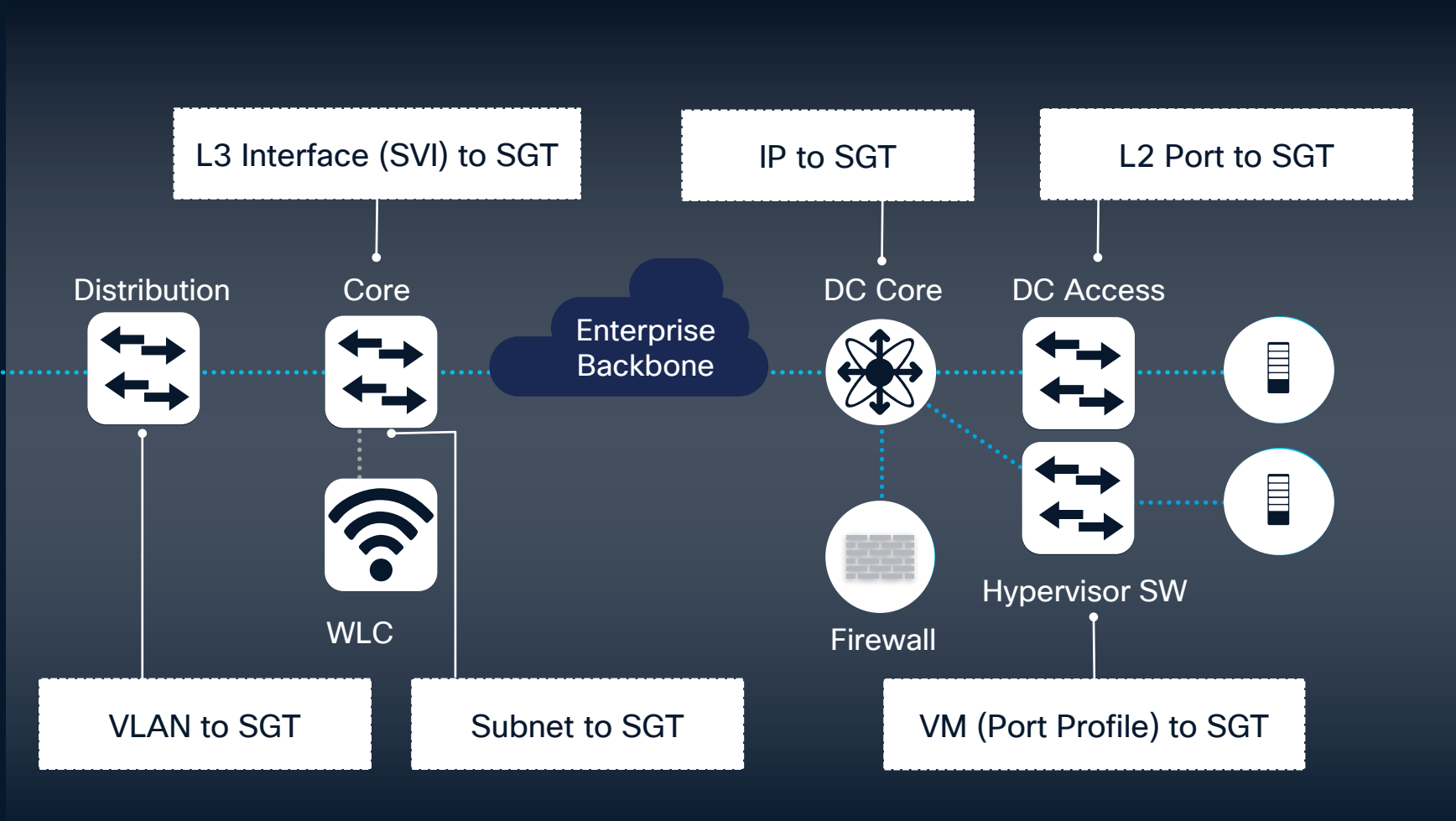
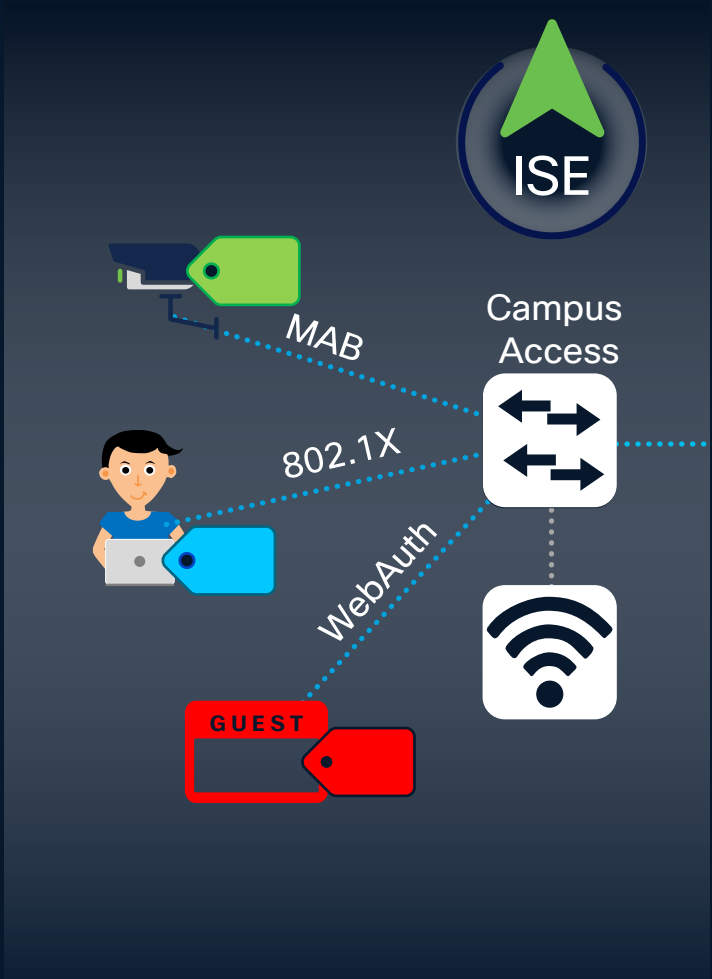
Enforcement



# Classification Mechanisms

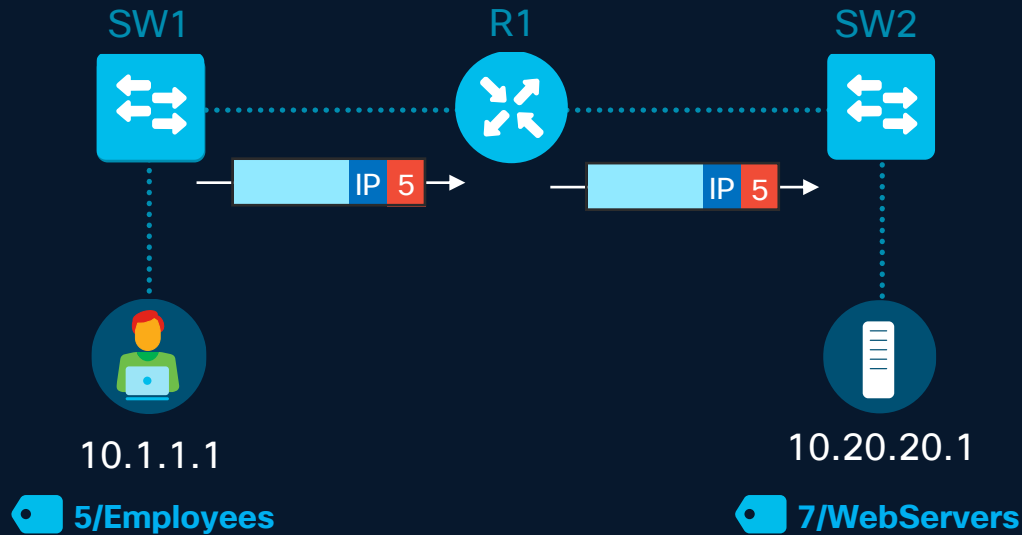
## Dynamic Classification

## Static Classification



# TrustSec Propagation

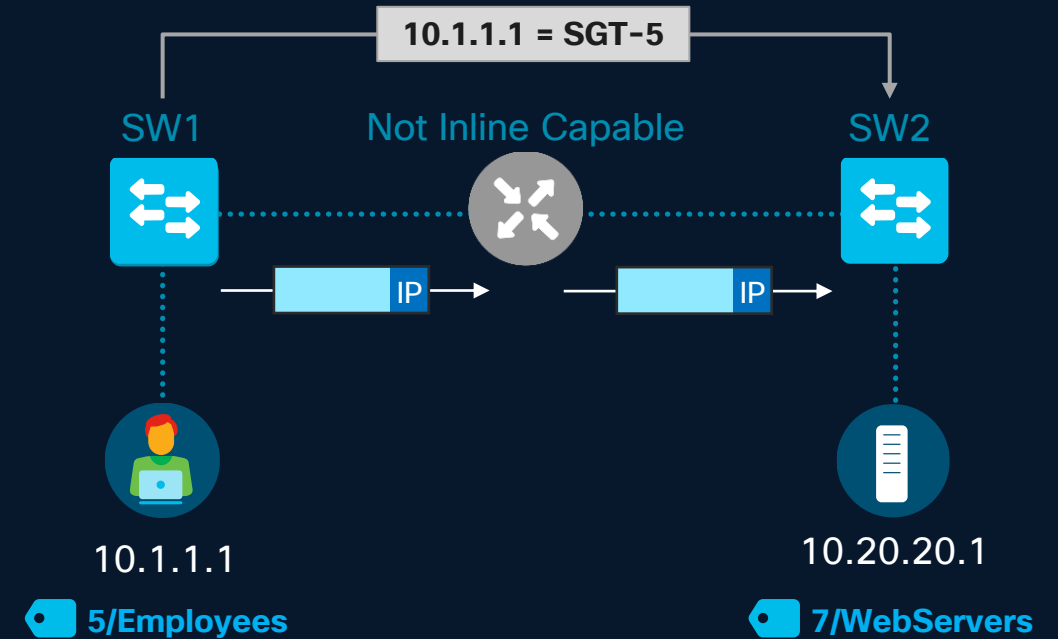
## DATA PLANE PROPAGATION (INLINE TAGGING)



SGT carried inline in the data traffic. Methods include, SGT over:

- Ethernet
- MACSec
- LISP/VxLAN
- IPSec
- DMVPN
- GETVPN

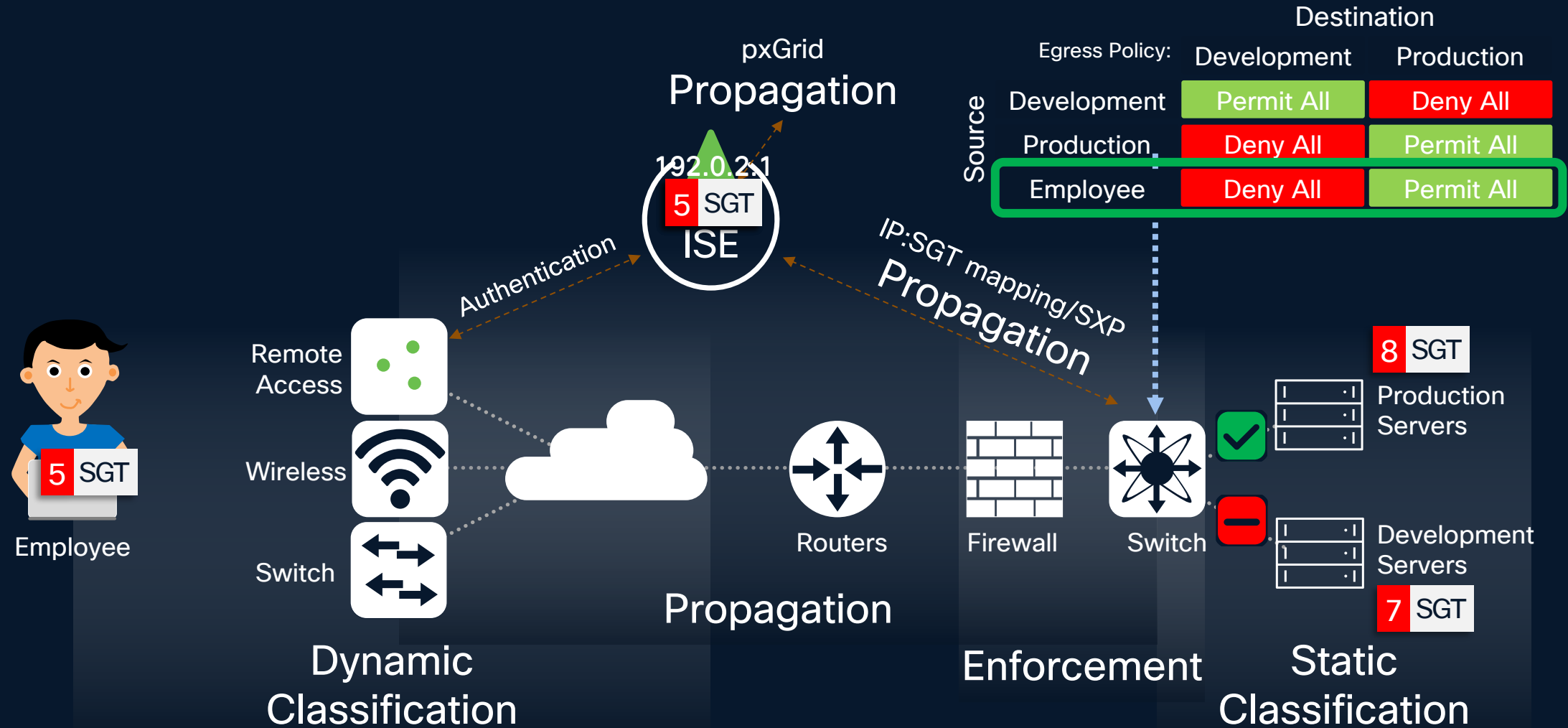
## CONTROL PLANE PROPAGATION (SXP)



IP-to-SGT data shared over control protocol. No SGT in the data plane. Methods include, IP-to-SGT exchange over:

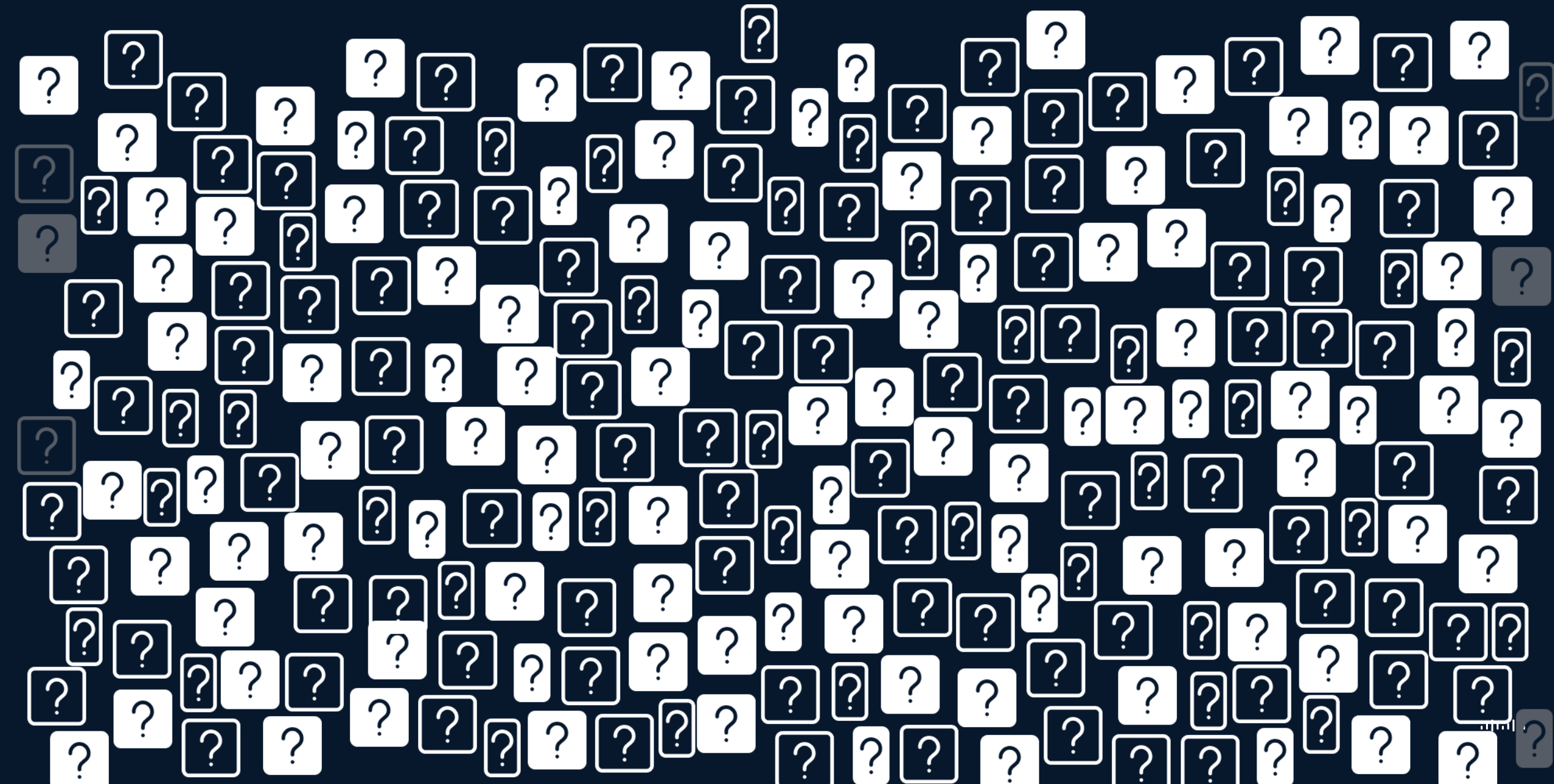
- SXP
- pxGrid

# Cisco SGT Propagation & Enforcement



# Dynamic Classification

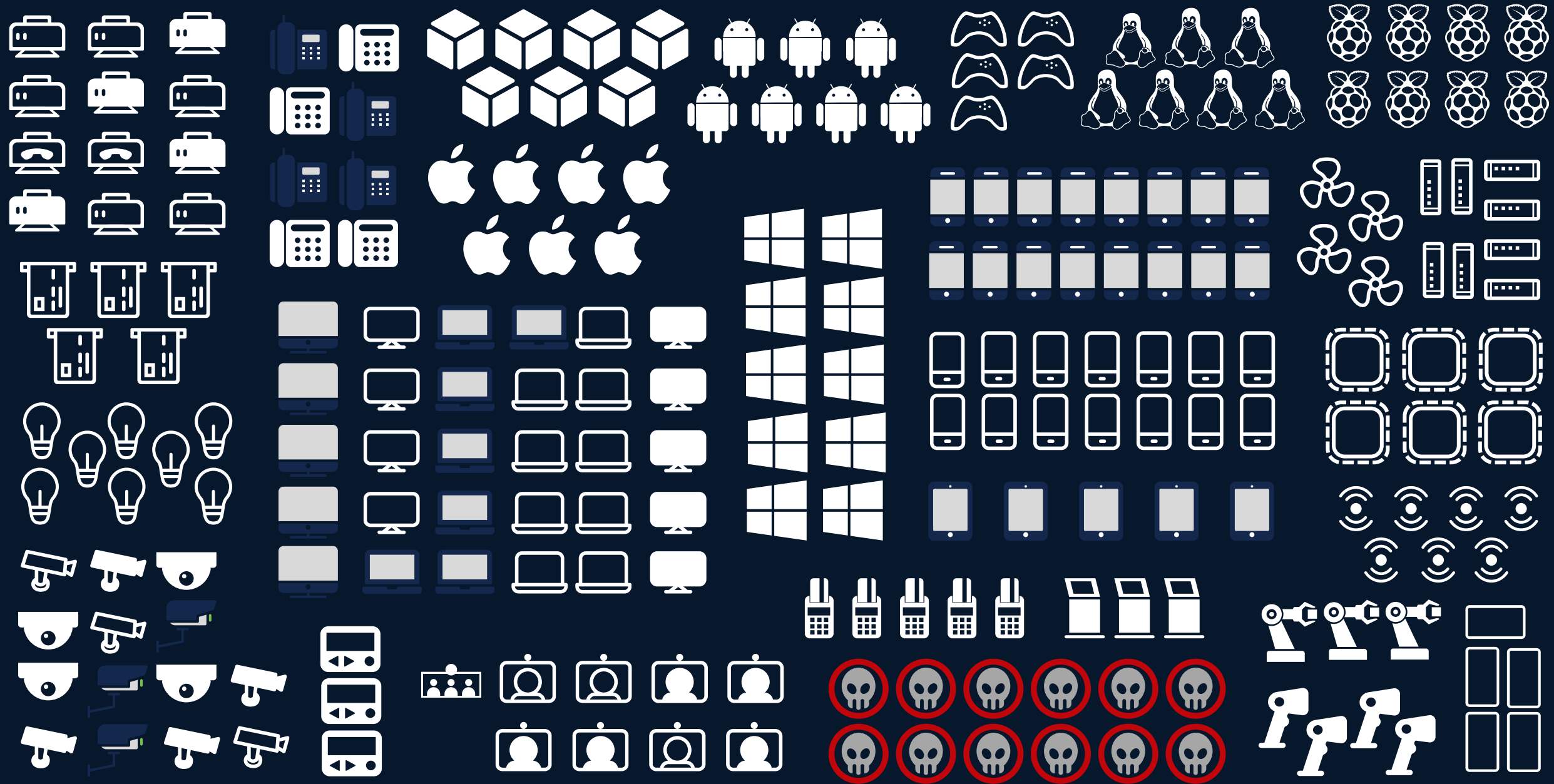
# The Challenge: Unknowns ...



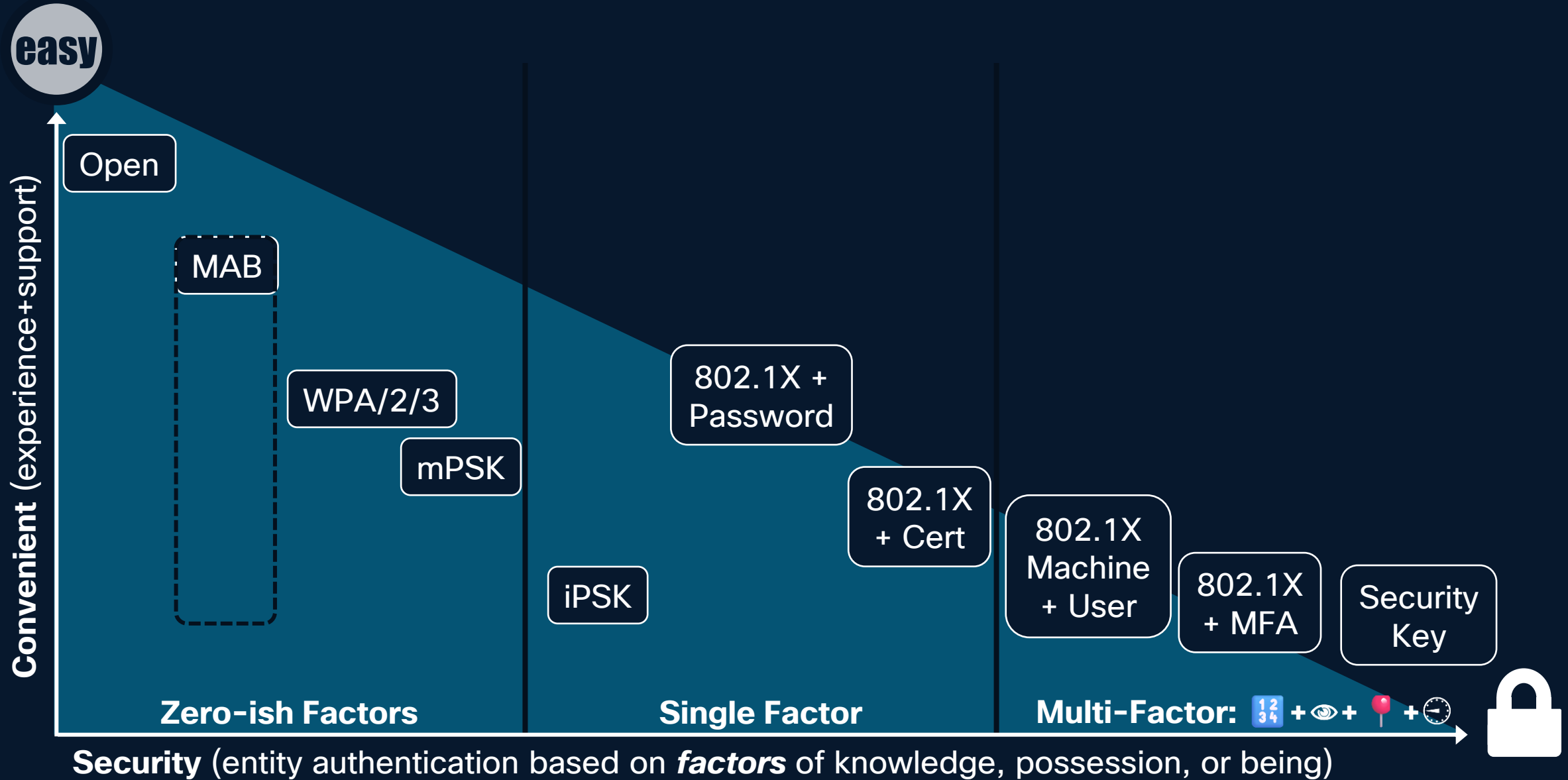
# The Challenge: Unknowns to Known ...



# The Challenge: Unknowns to Known to Classified



# Network Access Authentication is a Spectrum



# RADIUS : 802.1X



RFC2865 : RADIUS

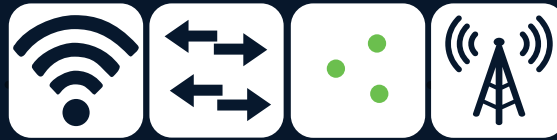
RFC3579 : EAP Support

RFC2866 : Accounting

RFC5176 : CoA Support



802.1X



EAPoL-Start

EAP: Extensible Authentication Protocol



Access-Request

Auth @ UDP:1812



Credentials:  
- Certificate  
- Password  
- Token



VLAN  
ACL  
SGT  
Group Policy  
...



Access-Accept/Reject

10.x.x.x



Accounting Session-Start

Acct @ UDP:1813



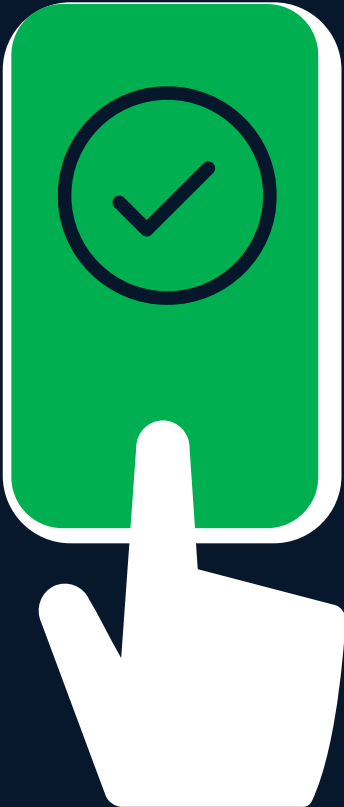
- User Disconnect  
- Session-Timeout  
- RADIUS CoA



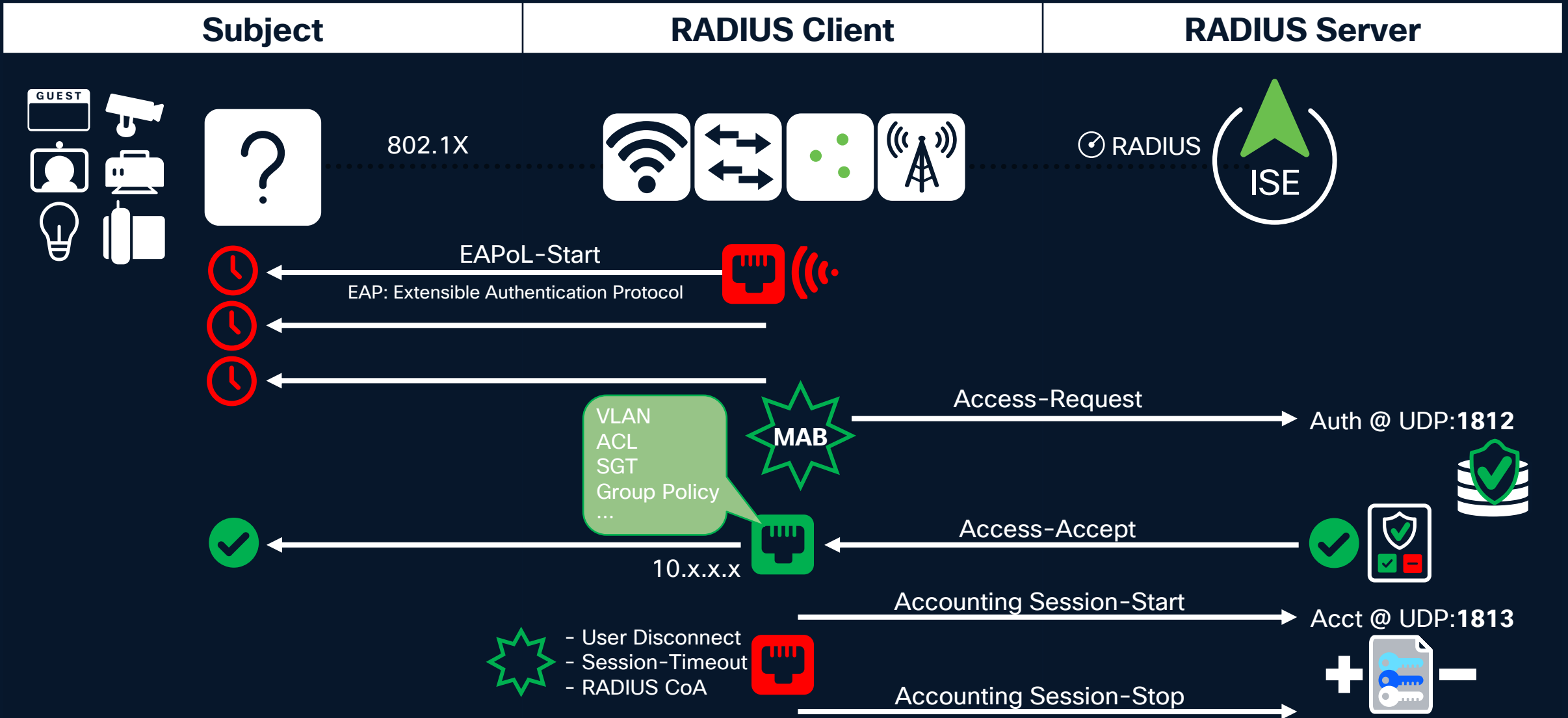
Accounting Session-Stop



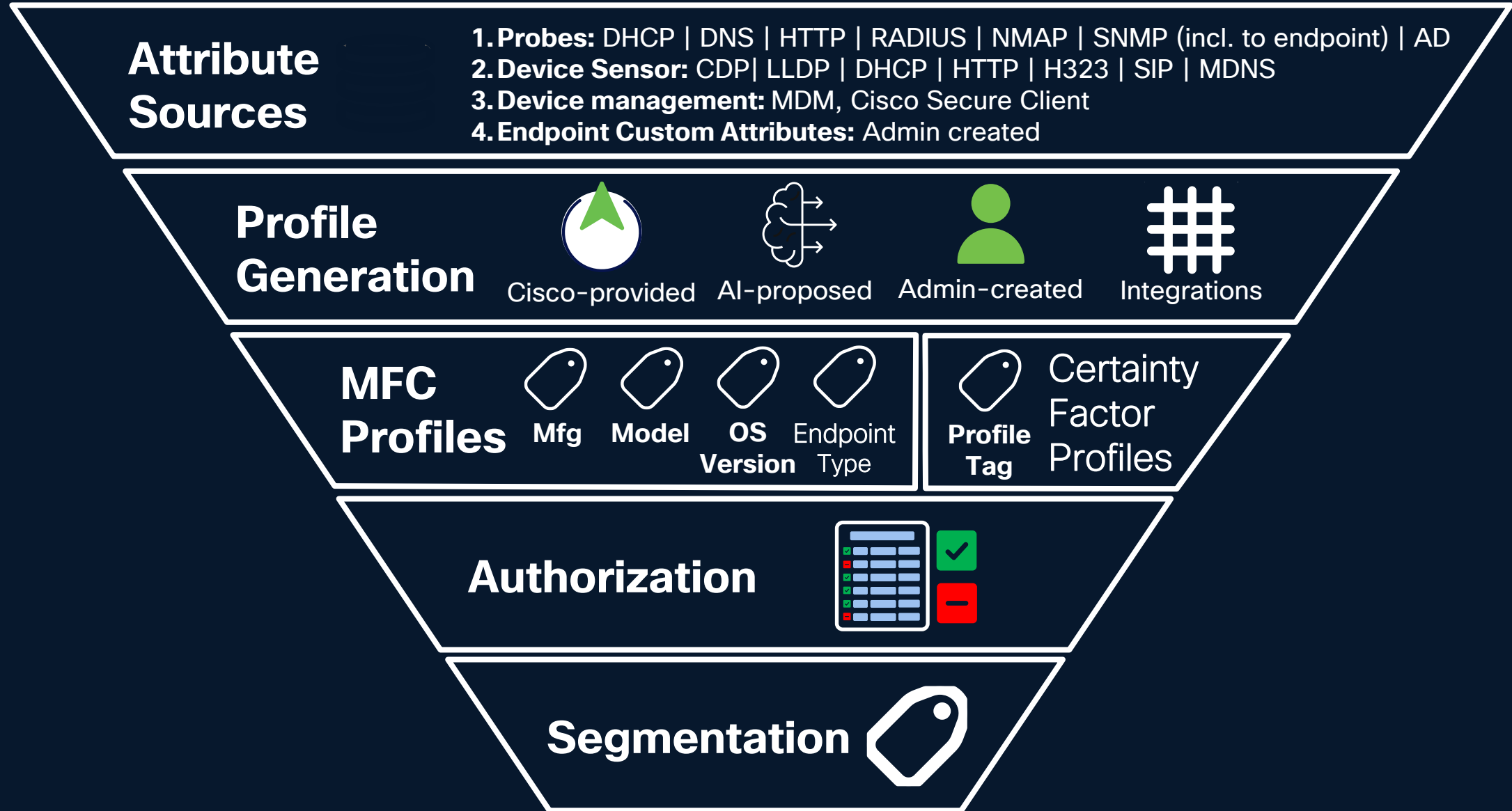
# 801.X Requires a Supplicant - MFA Requires a Finger



# RADIUS : MAC Authentication Bypass (MAB)



# Turning Attributes Into Profiles, Profiles Into Protection



# Multi-Factor Classification on ISE

MFC-Manufacturer: Cisco  
MFC-EndpointType: IP-Phone  
MFC-Model: IP Phone  
MFC-OS: 7980  
IOS



MFC-Manufacturer



Cisco



Apple



Arlo



Lenovo



MFC-EndpointType



IP-  
Phone



Laptop



Camera



Laptop



MFC-Model



IP Phone  
7980



MacBook  
Pro



Pro Wireless  
Cam



Thinkpad 540



MFC-OS



IOS



macOS  
12.0.1

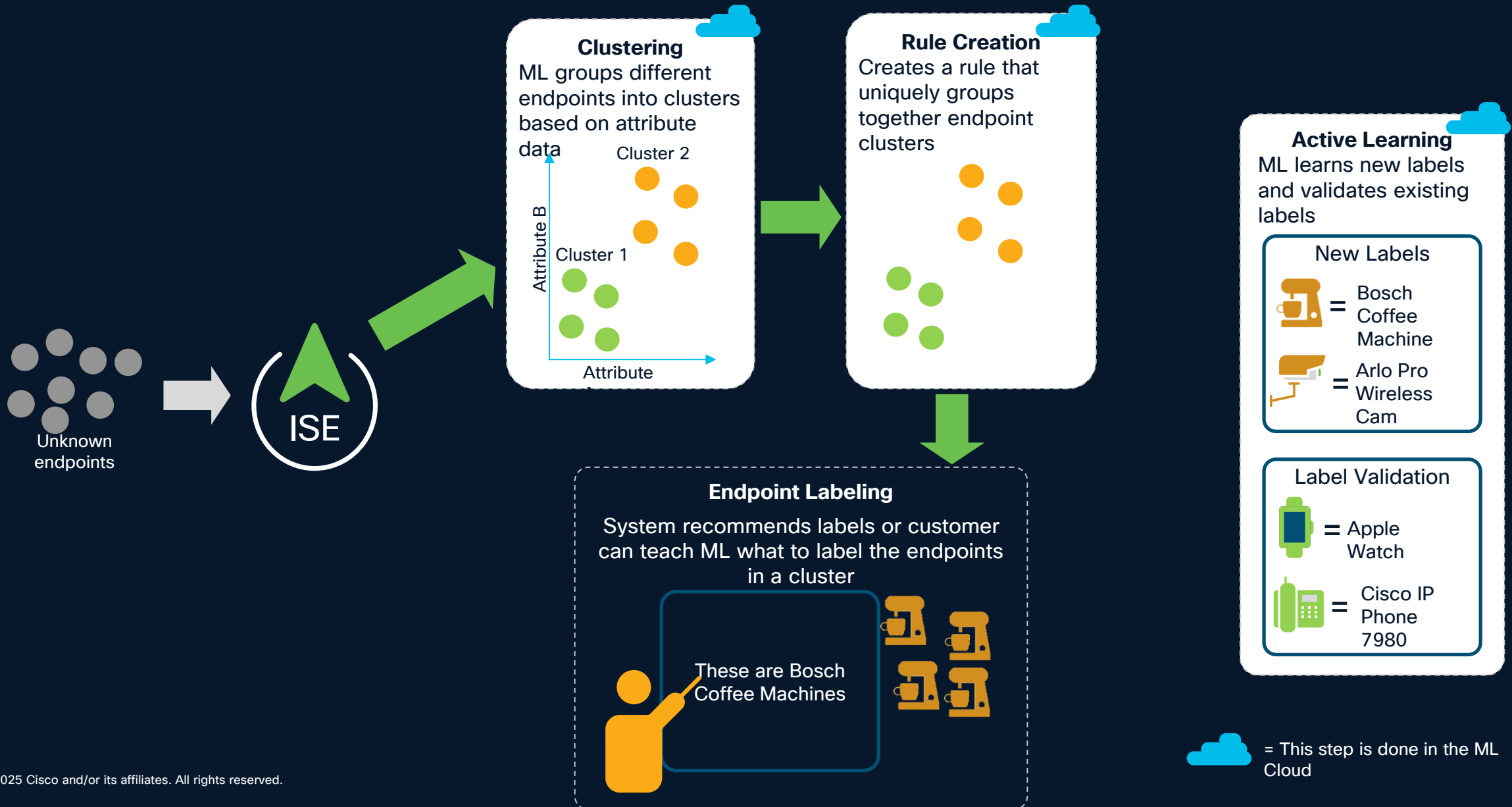


Linux

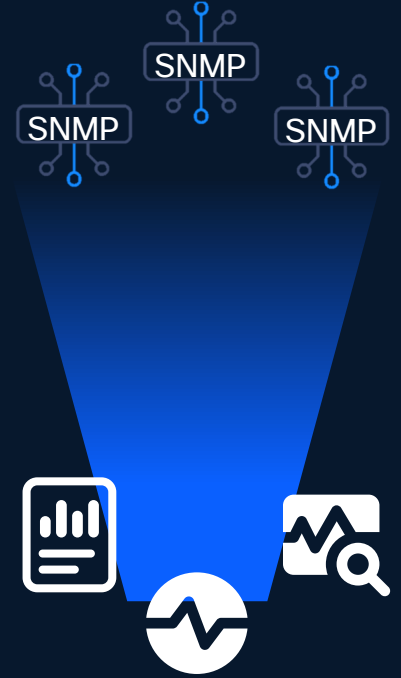
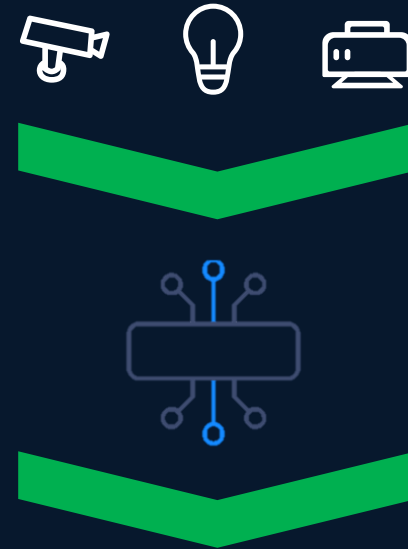
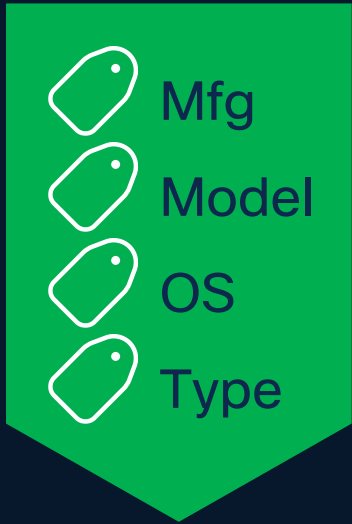


Windows  
Enterprise

# Cisco AI Machine Learning Profiling



# ISE 3.5 Profiler Features



- New Classification Engine and Rules based on MFCs**
- Use Multi-Factor Classification MFCs to Label Endpoints**
- Map Authoritative Source Attributes to MFCs**
- SNMP Endpoint Scanning for Profiling to MFCs**
- SNMP Probe Status Summary of Insights**

# Multi-Factor Classification (MFC) Profiles

ISE 3.5

## Problem

Custom profiling using Certainty factor required creating conditions in a separate flow, returning to profiling, then determining the minimum certainty factor

## Solution

Use “if/and/or” logic with standard operators (contains, equals, etc.) and then manage profiles in a redesigned screen

New profiling experience enables greater flexibility, more dictionaries and attributes, and therefore more granular profiling and authorization

Identity Services Engine Context visibility

← Profile Policy

### Add Profile Policy

**Details**

Policy name

Status  Enable  Disable

Type

Custom  
Define endpoint profiling conditions and apply Multi Factor Classification (MFC) labels below.

Direct mapping  
Map the values from authoritative sources (i.e. MDM, CMDB, SNMP) to assign as the selected Multi Factor Classification (MFC) label for an endpoint

**Conditions**

And

OR

dhcpClassIdentifier: operator Matches DHCP

userAgent Matches IP

DHCP: hostname Start with win

**Result**

The endpoints match this profile policy will be profiled with the following 4 Multi Factor Classification (MFC). Please fill in at least 1 MFC.

MFC: Manufacturer

MFC: Endpoint type

MFC: Model

MFC: OS

# New Context Visibility UI

## Problem

Information most needed by admins was either hard to find or not available in UI

## Solution

Streamlined UI with updated charts, analytics, customizations, and endpoint data

The screenshot displays the Cisco Identity Services Engine (ISE) Context Visibility interface. The top navigation bar includes the Cisco logo, 'Identity Services Engine', and 'Context visibility'. The main content area is divided into several sections:

- Endpoints Summary:** Shows 5000 Total, 3900 Connected, 1000 Disconnected, and 100 Rejected endpoints.
- Analytics:** Four bar charts showing top failed authentication, top authorization profiles, top reject reasons, and top locations.
- Endpoint Data Table:** A table with columns for MAC address, Auth Status, IP address, Username, Location, Authentication policy, and Authorization policy.

A 'Customize analytic view' dialog box is open on the right, allowing users to select or deselect graphs to display. The dialog includes sections for 'Selected analytic view', 'Authentication', 'Compliance', 'Classification', and 'Guest'.

MAC address	Auth Status	IP address	Username	Location	Authentication policy	Authorization policy
00:00:00:00:00:01	✓	10.0.10.155	john.smith	San Jose - Floor 1	EAP-PEAP Corp	Corp → Employee

# Improved Profiling Policy Management

ISE 3.5

## Problem

Need to know how many endpoints match a profiling policy, which policies are enabled or disabled, and which attributes define a policy

## Solution

New profiling policy management enables insights into endpoints per policy, better policy creation workflow, and endpoint filtering

The screenshot shows the Cisco Identity Services Engine (ISE) Profiling Policies management interface. The top navigation bar includes the Cisco logo, "Identity Services Engine", and "Work Center / Profiler". The main navigation menu on the left lists: Bookmarks, Dashboard, Context Visibility, Operations, Policy, Administration, and Work Centers. The main content area is titled "Profiling Policies" and includes a sub-section for "MFC Profiling Policies" and "Certainty Factor & Logical Profiling Policies". A summary bar shows: 30 Policies enabled (with a green checkmark), 3 Policies disabled (with a grey circle), and 36 Enabled policies with no matched endpoints (with a yellow warning icon). Below this, a table lists individual policies with columns for Rank, Name, Status, Type, MFC: Endpoint type, MFC: Manufacturer, MFC: Model, MFC: OS, and Endpoints. The table includes a search bar, filters for Status and Type, and buttons for Export, Import, and Add profiling policy. A note states: "Policies will be processed sequentially based on the rank you set here".

Rank	Name	Status	Type	MFC: Endpoint type	MFC: Manufacturer	MFC: Model	MFC: OS	Endpoints
1	Name	Enabled	Custom	—	—	—	Linux	120 matched
2	Name	Enabled	Direct mapping	Value from JAMF: Endpoint type	Value from JAMF: Manufacture	Value from JAMF: Model	Value from JAMF: OS	180 matched
3	Name	Disabled	Custom	dhcpDeviceType	App manufacturer	—	—	589 matched
4	Name	Enabled	Custom	Printer	intune manufacture OS	Lexmark-Printer E260dn	iOS	287 matched
5	Name	Enabled	AI	—	—	—	Linux	749 matched
6	Name	Disabled	Direct mapping	Value from JAMF: Endpoint type	Value from JAMF: Manufacture	Value from JAMF: Model	Value from JAMF: OS	358 matched
7	Name	Disabled	Custom	dhcpDeviceType	App manufacturer	—	—	976 matched

# Posture and Compliance

# Seeing beyond who and what your are with Posture

ISE Posture with  
Cisco Secure Client/  
Agentless



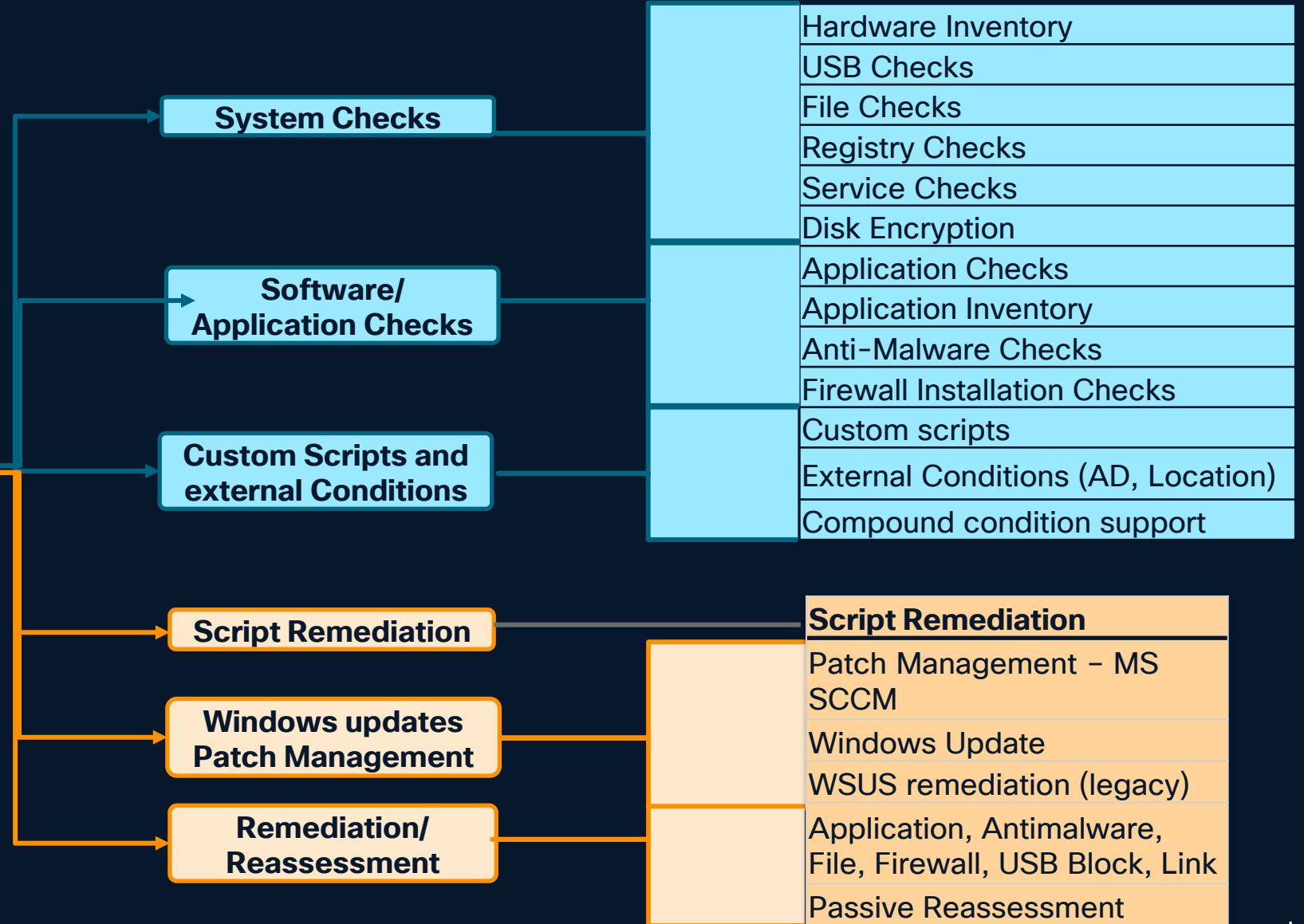
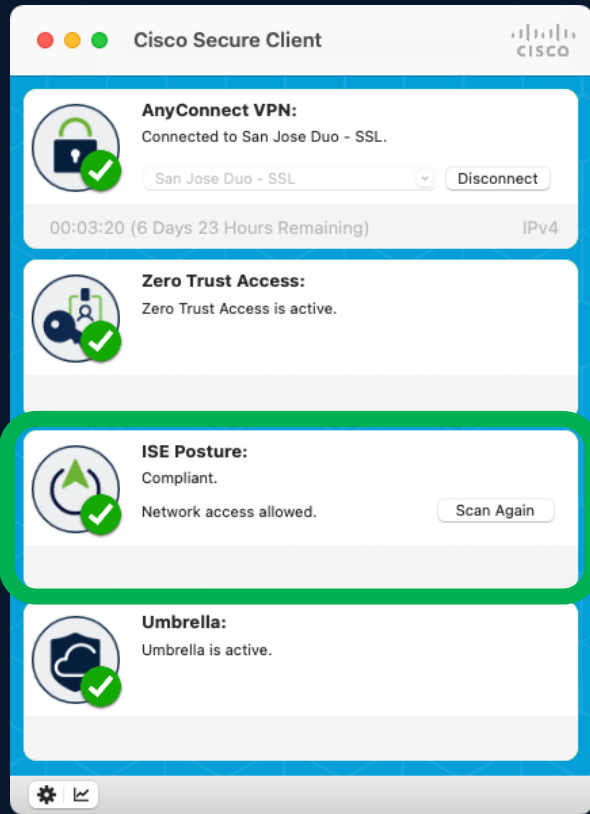
EMM/MDM Integrations



Threat Centric NAC -  
Integration with Vulnerability  
Scan/Threat Collection



# ISE Posture with Cisco Secure Client



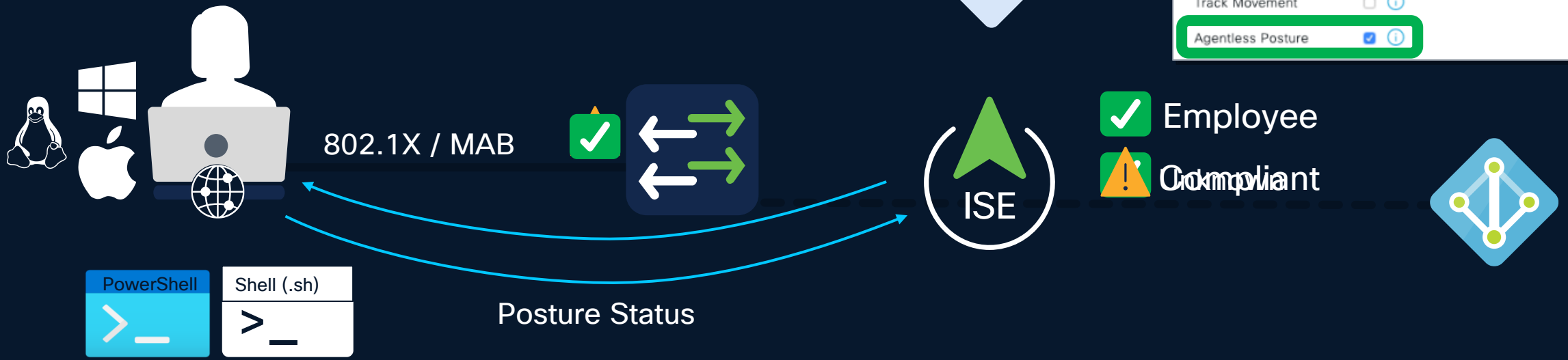
# Agentless Posture

ISE 3.0+

Status	Rule Name	Conditions	Profiles	Security Groups
Unknown		AND Network_Access_Authentication_Passed Compliance_Unknown_Devices	Agentless_Posture	Network_Services
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	<input type="checkbox"/>
Track Movement	<input type="checkbox"/>
Agentless Posture	<input checked="" type="checkbox"/>



# Posture Deployment Options

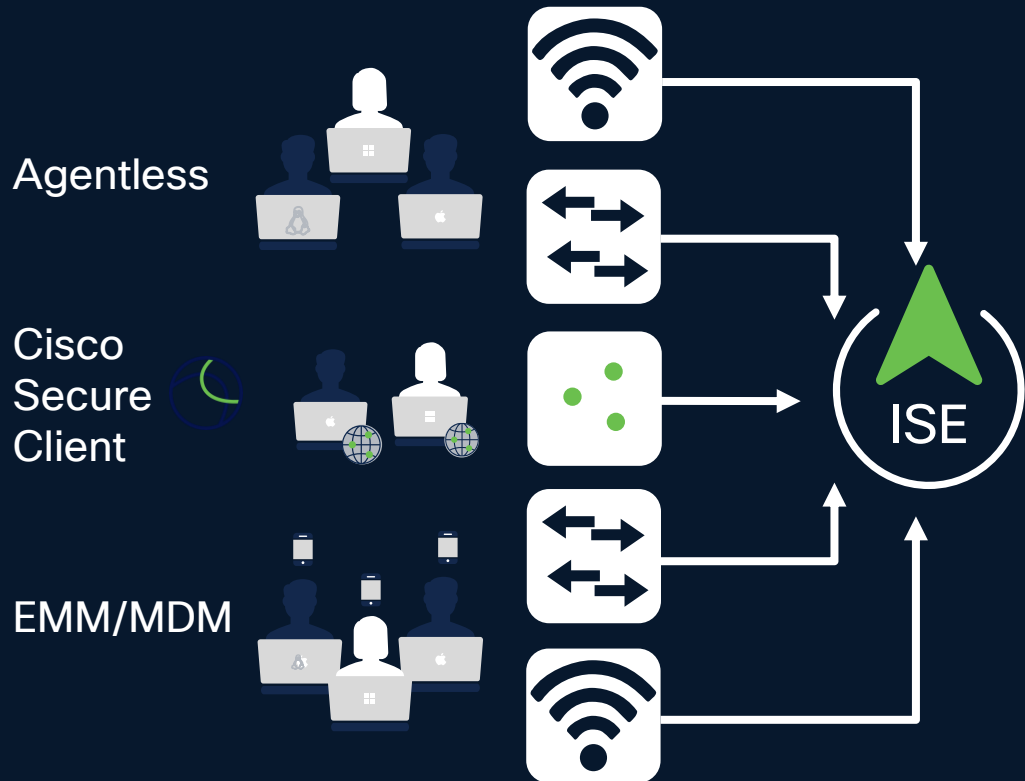
- ✓ Supported
- ! Limitations
- ✗ Not Supported

ISE 3.3

Capability	Cisco Secure Client			AC Stealth		Temporal		Agentless		
	Windows	Mac	Linux	Windows	Mac	Windows	Mac	Windows	Mac	
Anti-Malware Checks	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Firewall Installation Checks	✗	✗	✗	✓	✓	✓	✓	✓	✓	
Application Inventory	✗	✗	✗	<b>Visibility (Less Effort)</b>						✓
Hardware Inventory	✗	✗	✗	✓	✓	✓	✓	✓	✓	
Process Checks	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Dictionary Conditions	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Application Checks	✓	✓	✗	✓	✓	✓	✓	✓	✓	
File Checks	✓	✓	!	<b>Experience (Less Time)</b>						✗
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	<b>Security (More Protection)</b>						✗
Remediation	Auto, Manual	Partial	Partial	Part Auto	Partial	Text	Text	✗	✗	
Reassessment	✓	✓	✓	✓	✓	✗	✗	✗	✗	

# 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

# Integrations

# Power of pxGrid Integration

Enabling a platform approach into the Cloud

## ISE Context OUT



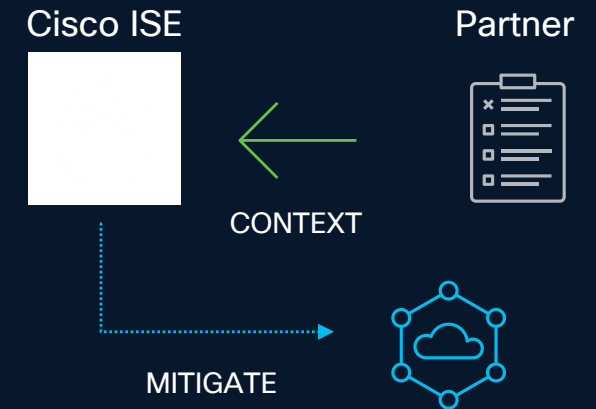
ISE makes Customer IT  
Platforms User/Identity, Device  
and Network Aware

## ISE Context IN



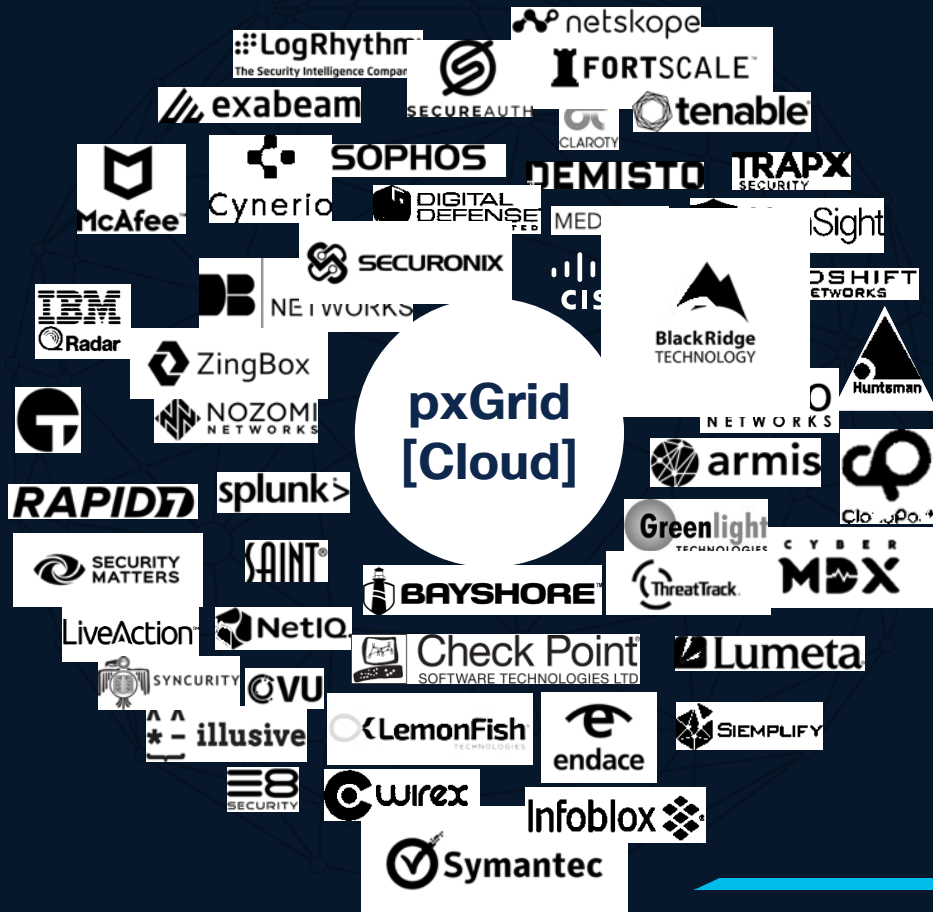
Enrich ISE context. Make ISE  
a better Policy Enforcement  
Platform

## Rapid Threat Containment



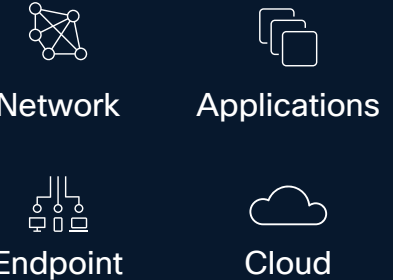
Enforce dynamic policies into the  
network based on Partner's  
request

# The power of integration with operational simplicity



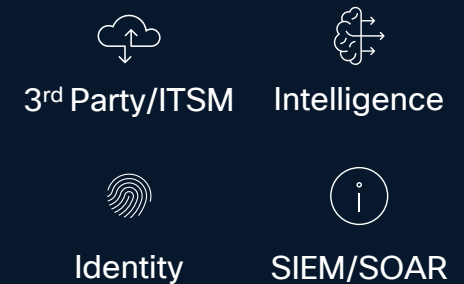
More Cross-Team  
Use Cases Simplified  
with Visibility and  
Automation

## Cisco Security



## Your infrastructure

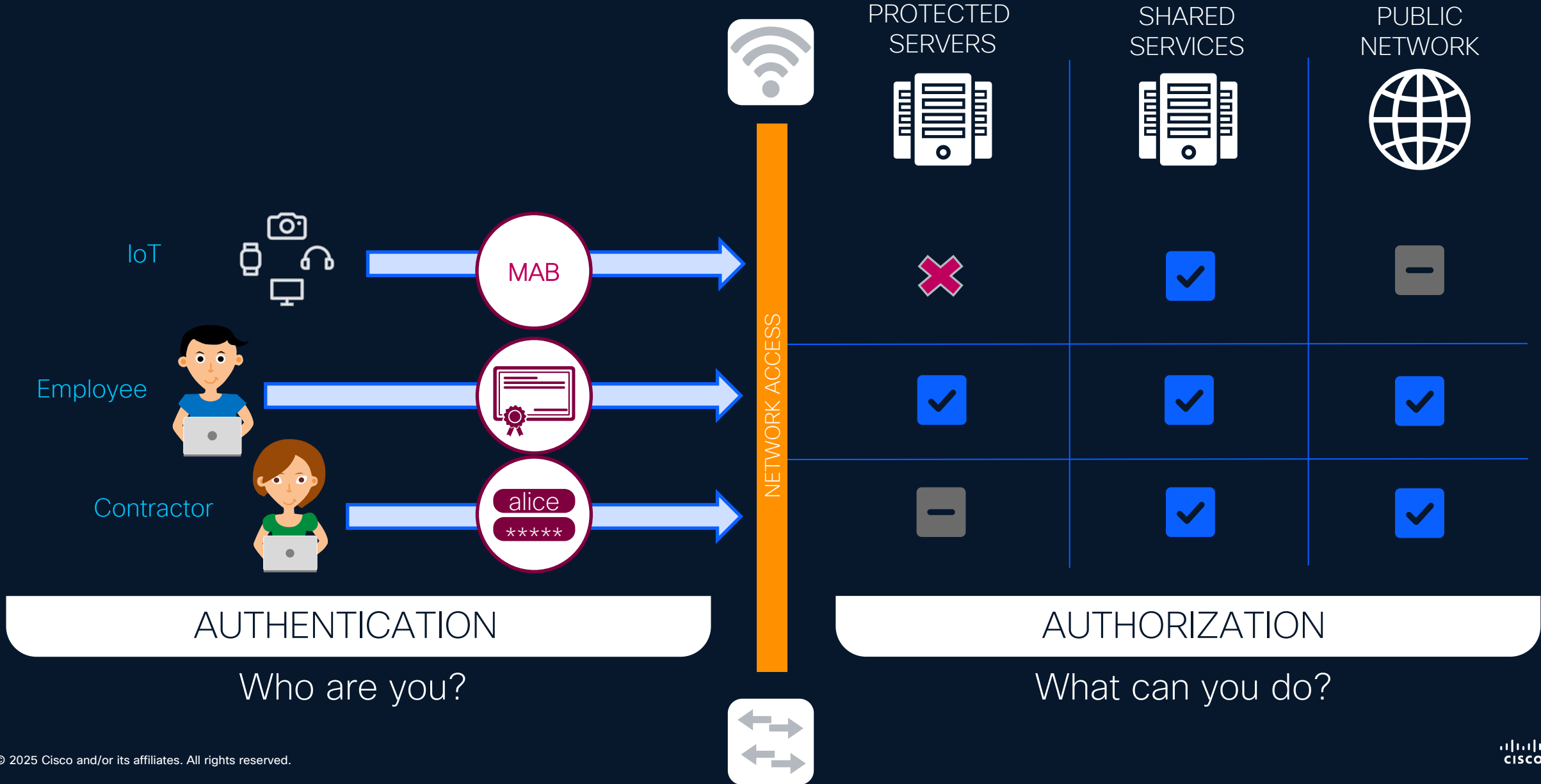
More Integrated  
Products Across  
Partner Ecosystem  
and Beyond





**Let's bring this home!!**

# Authentication and Authorization



**Get ready for part 2 –  
Segmentation Beyond the Campus**