CISCO Engage | Tech Day

Identity is the New Perimeter

Why SGT-Based Access Matters for Today's Campus Network

Lou Norman CCIE CISSP
Cyber Security Architect,
linkedin.com/in/lounorman

March 17th, 2026

Lou Norman

- 37 years of networking and security experience
- 29 years at cisco Systems
- CCIE for 27 years
- CISSP for 22 years
- First Security Hack – Spoofed Email from the President of the university to the CIO
- Installed my first firewall in (Pix 535) 2003
- Installed the first Firewall Service Module in production that same year.
- Helped install and test NAC solutions since the early 2000's.
- Hobbies: Biking, boating, archery, anything that takes me outdoors.

Agenda

1. Why Zero Trust Matters
2. Zero Trust platform
3. Secure Networking
4. SGT Basics
5. Cisco ISE
6. Catalyst Center
7. Meraki
8. Where to Start
9. Closing thoughts

Why Zero Trust Matters

Section title placeholder

Why Zero Trust Matters

Security tools are not perfect

Having a security tool for every vulnerability is not possible

Users are not perfect

cisco

Section title placeholder

Why Zero Trust Matters

Sooner than later, it will be required

What it takes to get Zero Trust right

Zero Trust requirements

Establish Trust

- User / device / service identity
- Posture + context
- Risk-based authentication

Enforce Trust-Based Access

- Micro-segmentation
- Unified access control
- Least privilege + explicit trust

Continuously Verify Trust

- Re-assessment of trust
- Indicators of compromise
- Shared signals
- Behavior monitoring – threat and non-threat activity
- Vulnerability management

Respond to Change in Trust

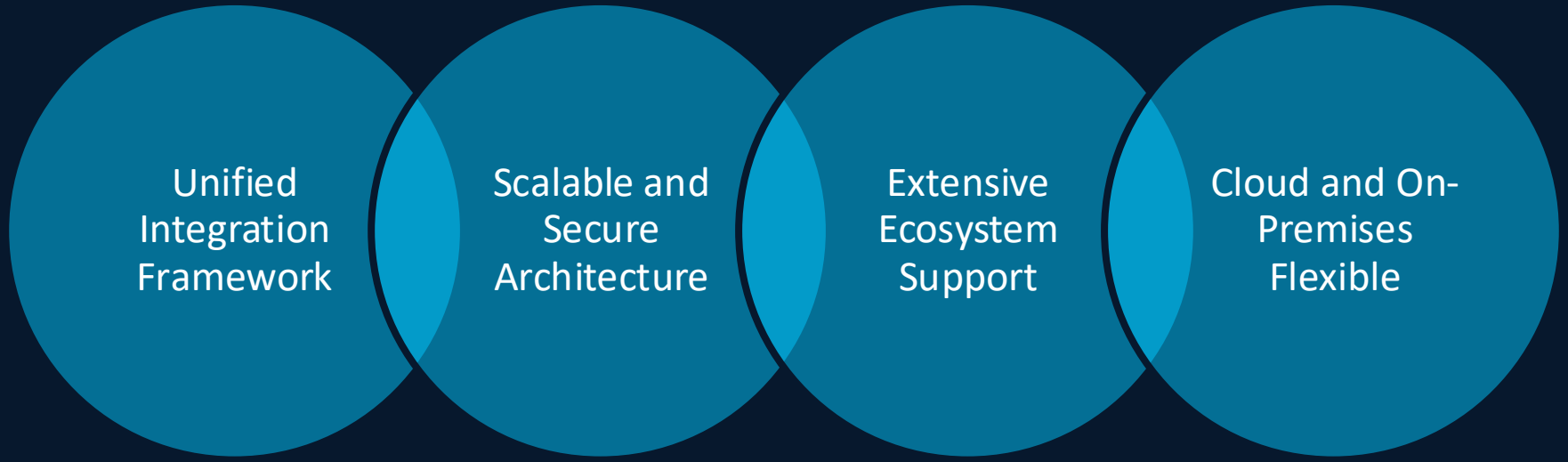
- Prioritized incident response
- Orchestrated remediation
- Integrated + open workflows

Section title placeholder

Why Zero Trust Matters

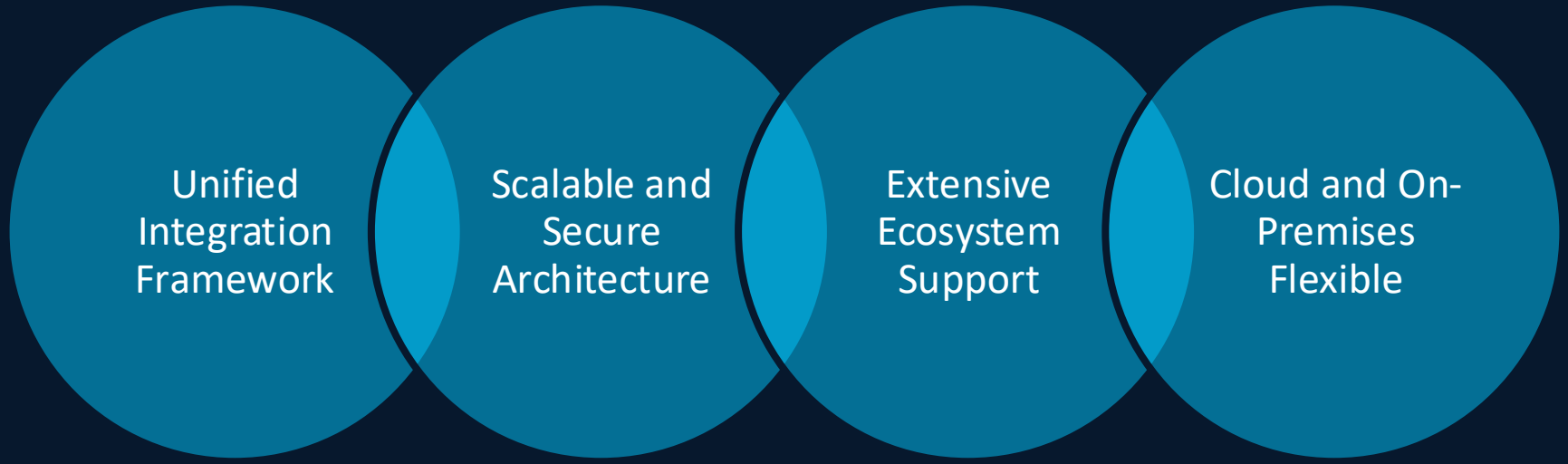
Sounds like something for a security platform?

Unified Architecture & Ecosystem Integration



- Enables seamless, bi-directional sharing of contextual information across solutions
- Eliminates the need for platform-specific APIs for network and security tools
- Supports a wide range of products and third-party security product integrations
- Utilizes open architecture with WebSocket and REST APIs for communication
- Provides secure, scalable, and customizable connections between clients and identity
- Offers deployment flexibility across on-premises and Cloud environments
- Enables deep security analysis through integration with cloud-based SaaS applications

Cisco Identity Service Engine (ISE) the First Security Platform

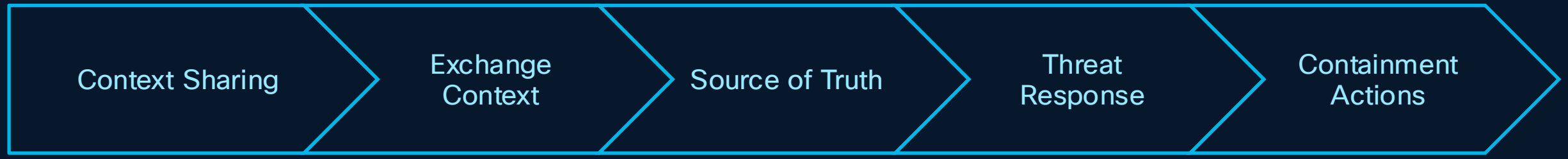


- Enables seamless, bi-directional sharing of contextual information across platforms
- Eliminates the need for platform-specific APIs for network and security tools
- Supports a wide range of Cisco and third-party security product integrations
- Utilizes pxGrid 2.0 architecture with WebSocket and REST APIs for communication
- Provides secure, scalable, and customizable connections between clients and ISE
- Offers deployment flexibility across on-premises and pxGrid Cloud environments
- Enables deep security analysis through integration with cloud-based SaaS applications

241

Cisco ISE

Contextual Intelligence & Automated Response



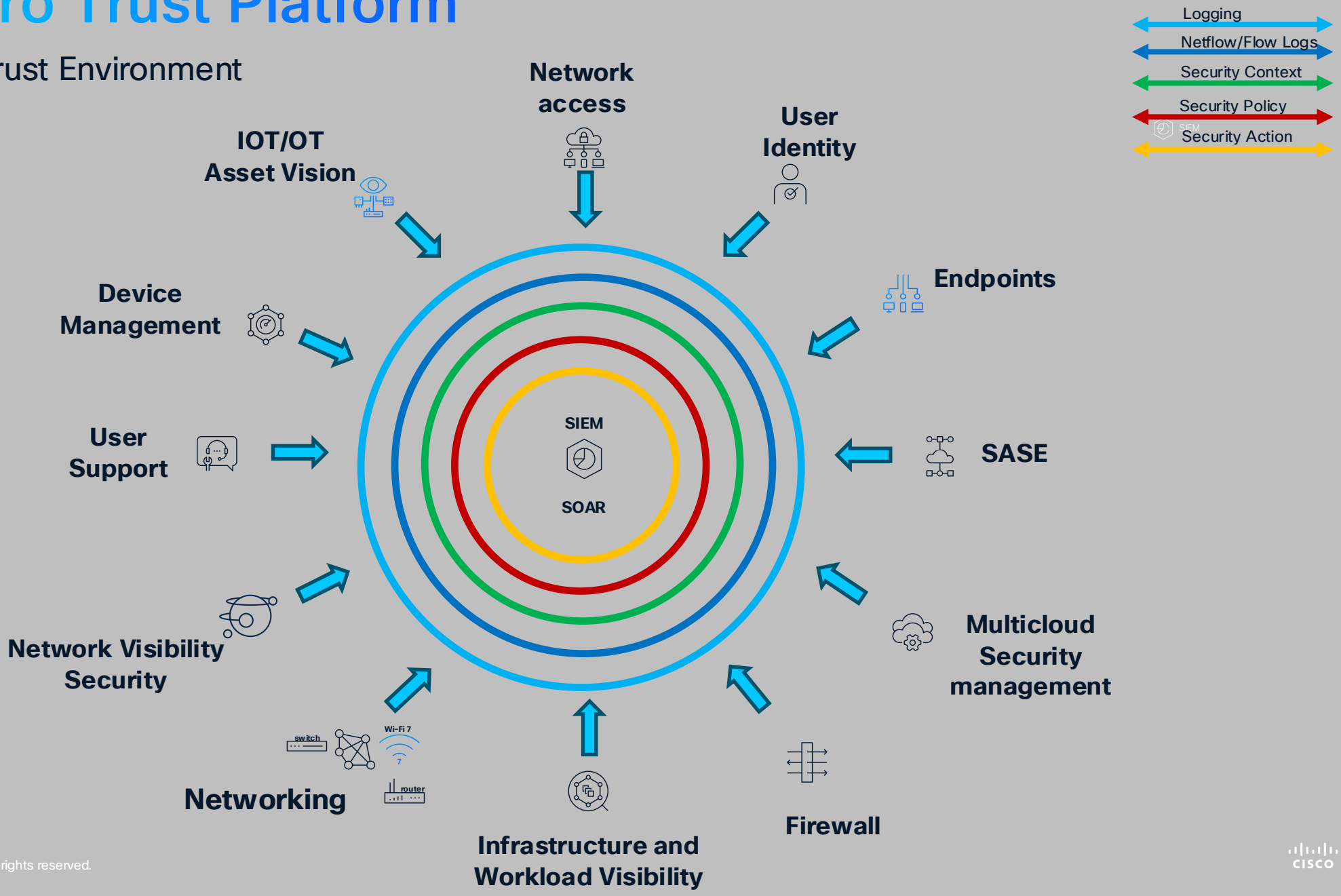
- Facilitates near real-time exchange of endpoint, user, and network context
- Enhances overall security visibility and enforcement across the network
- Establishes Cisco ISE as the authoritative 'Single Source of Truth' for identity
- Ensures consistent and accurate data sharing for security context
- Enables rapid threat containment actions like quarantining or isolating endpoints
- Leverages shared contextual data to drive automated response mechanisms
- Supports adaptive network control to mitigate risks across the ecosystem

cisco

Cisco Zero Trust Platform

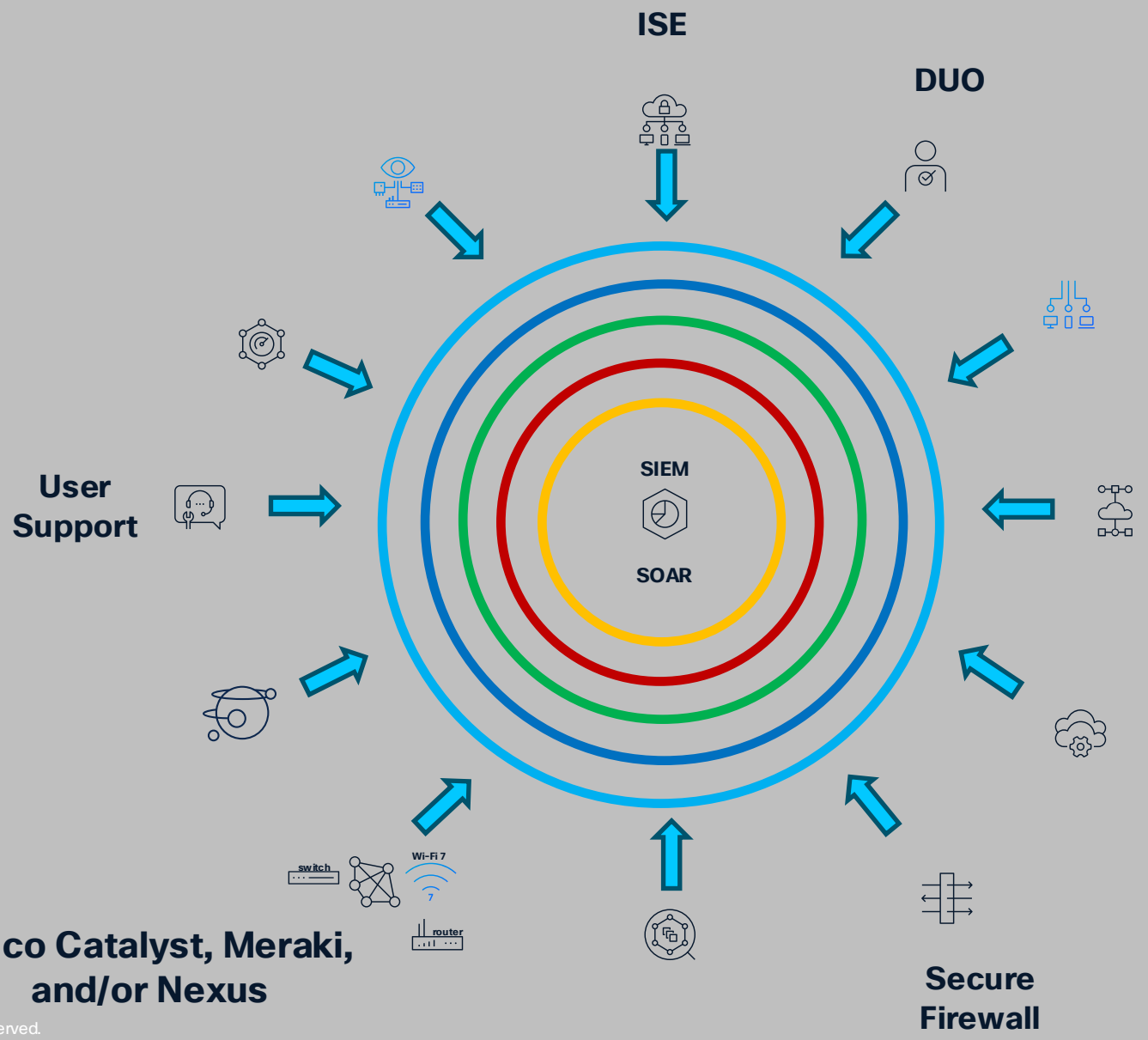
Cisco Zero Trust Platform

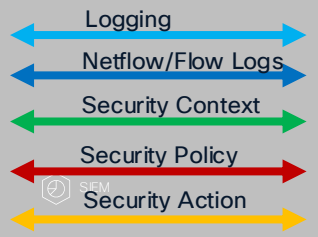
Universal Zero Trust Environment



Cisco Zero Trust Platform

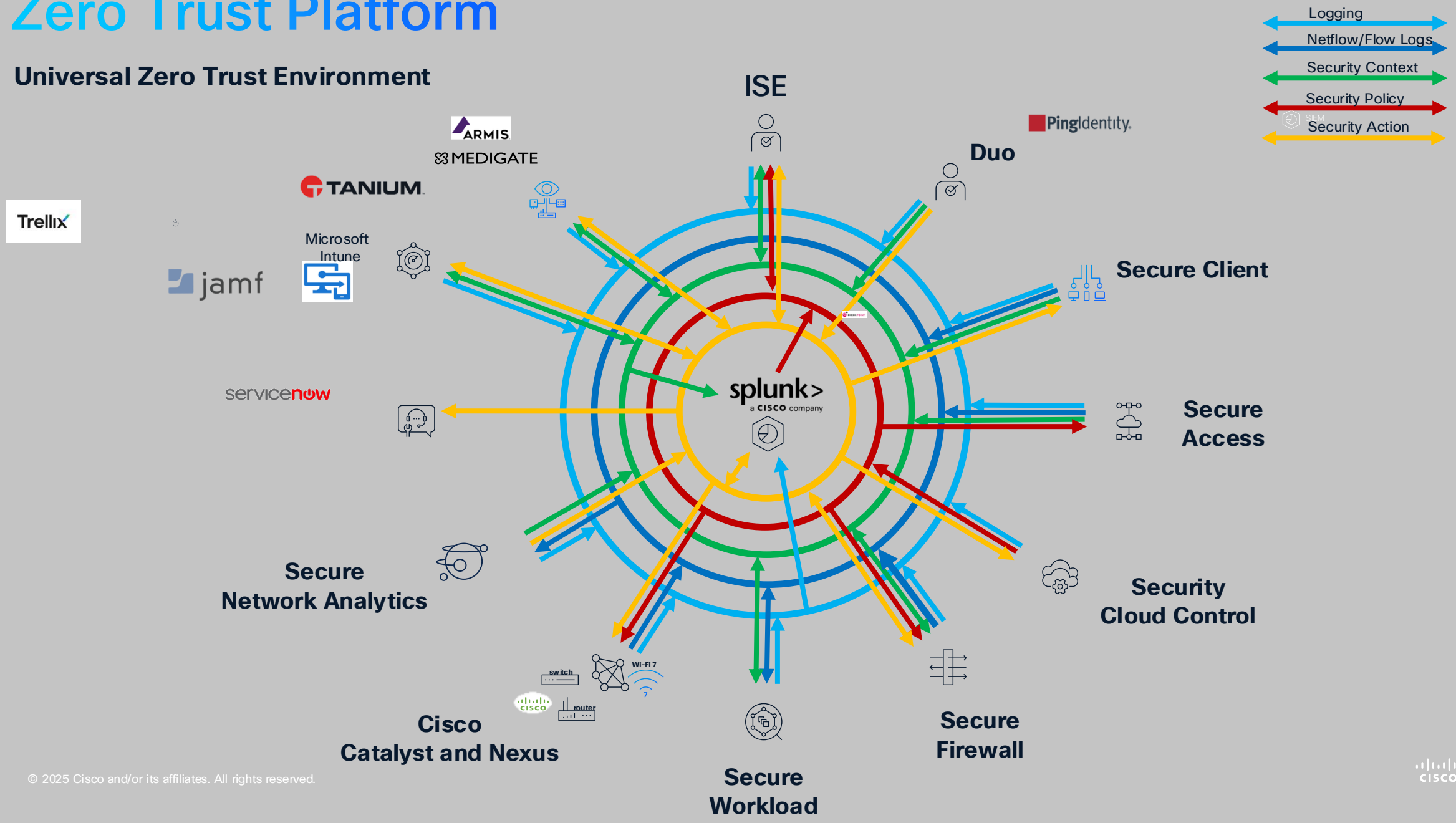
SGT Environment





Zero Trust Platform

Universal Zero Trust Environment



Secure Networking

What is Secure Networking?

Secure networking is a modern network infrastructure design that fuses advanced security and deep visibility into the network to protect the confidentiality, integrity, and availability of data and resources—ensuring digital resilience across the future-proofed workplace and the AI-ready data center.

In an increasingly AI-driven world, a Cisco Secure Networking architecture is the most effective safeguard against unauthorized access, misuse, and attacks.

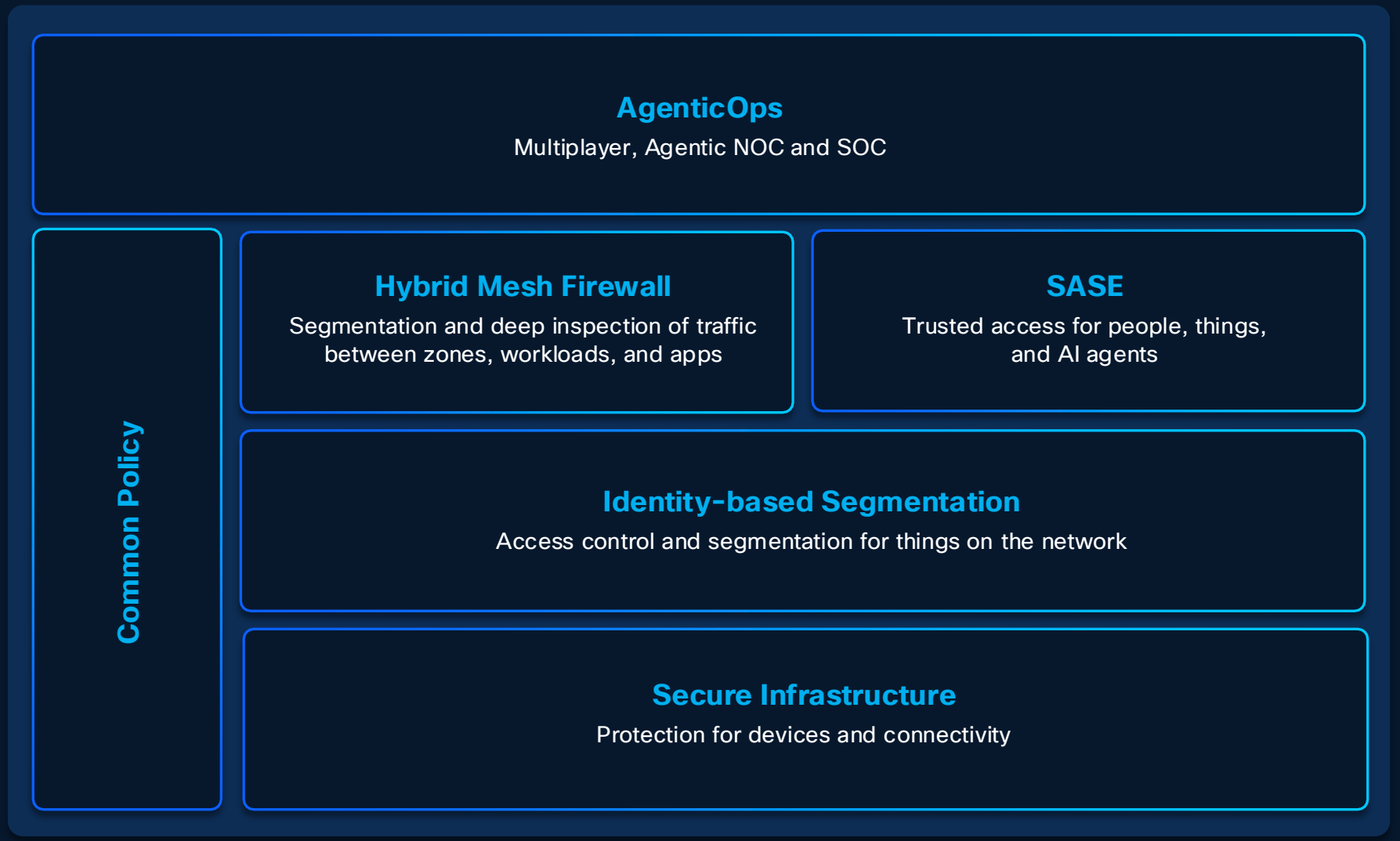
Differentiation

The Cisco Secure Networking Architecture is:

- AI-native
- Identity and threat-aware
- Hyper distributed and deeply embedded

Secure Networking

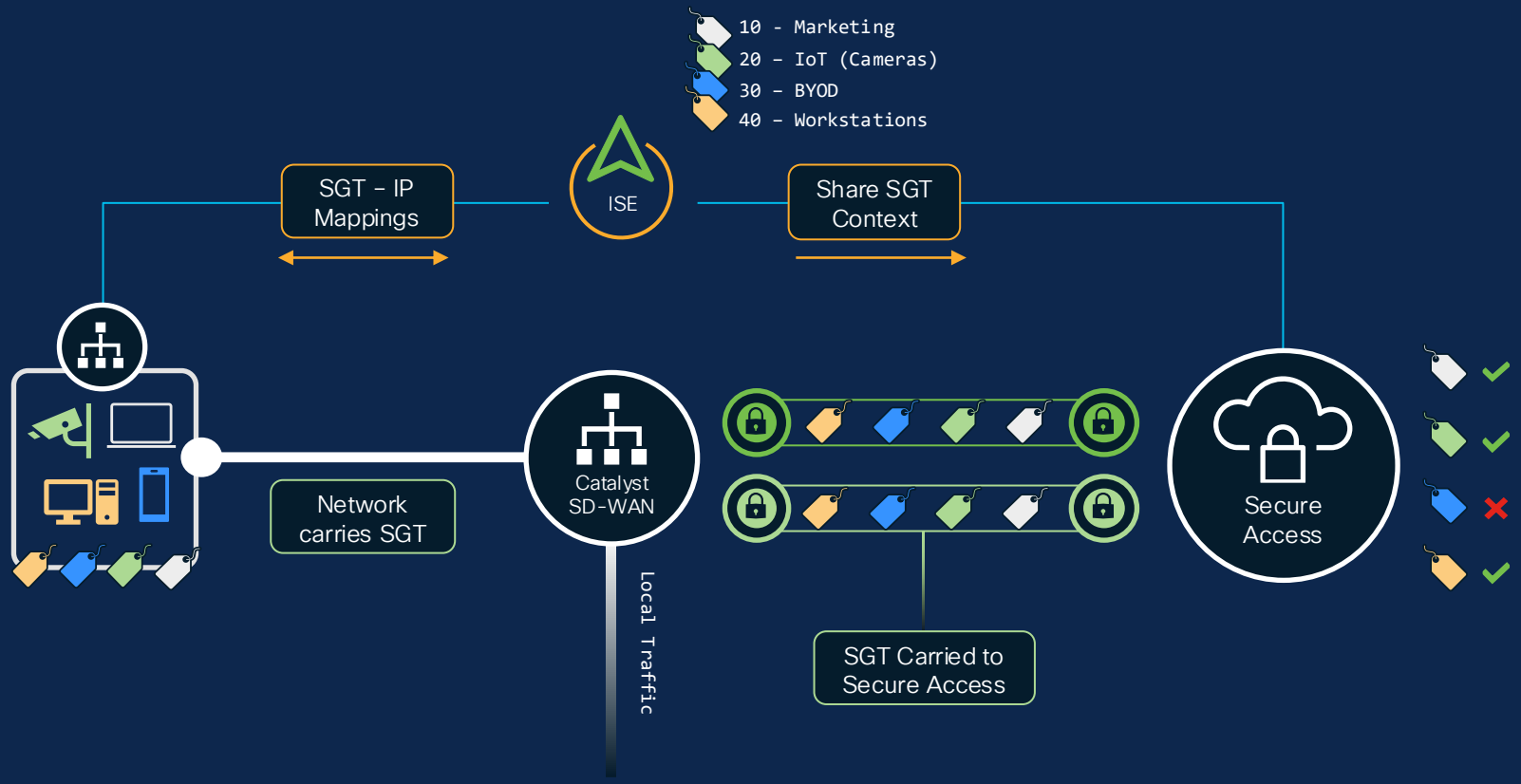
Reference design for fusing security into the network



Security Group Tags (SGTs) Basics

Identity Services Engine

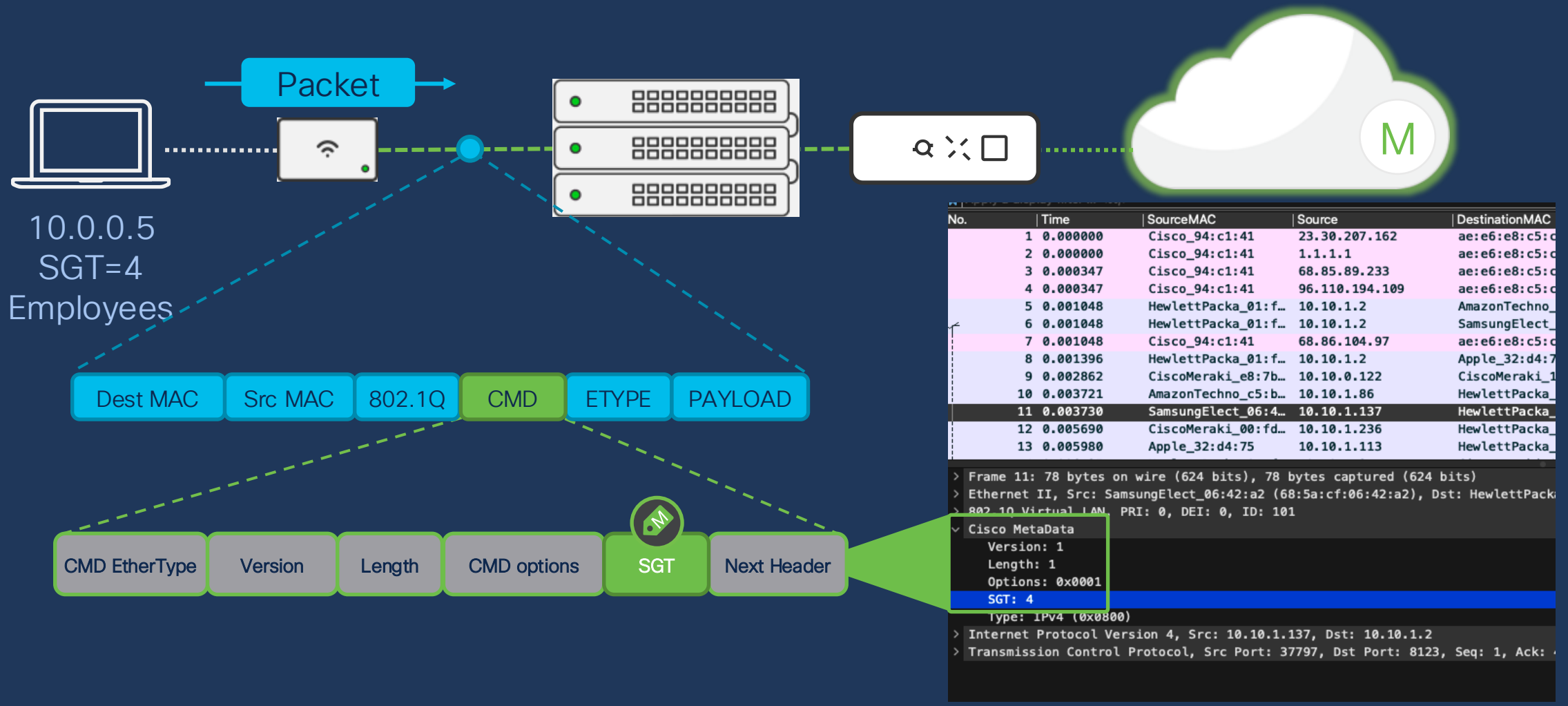
SGT Support for consistent policy and enforcement



Consistent Policy

- SGT Based Policy across network & Cloud
- Maintain micro segmentation through Secure Access
- Uniquely identify devices and traffic based on context from ISE
- Apply policy to SGT Based Identity

How are SGTs Transmitted in Adaptive Policy?



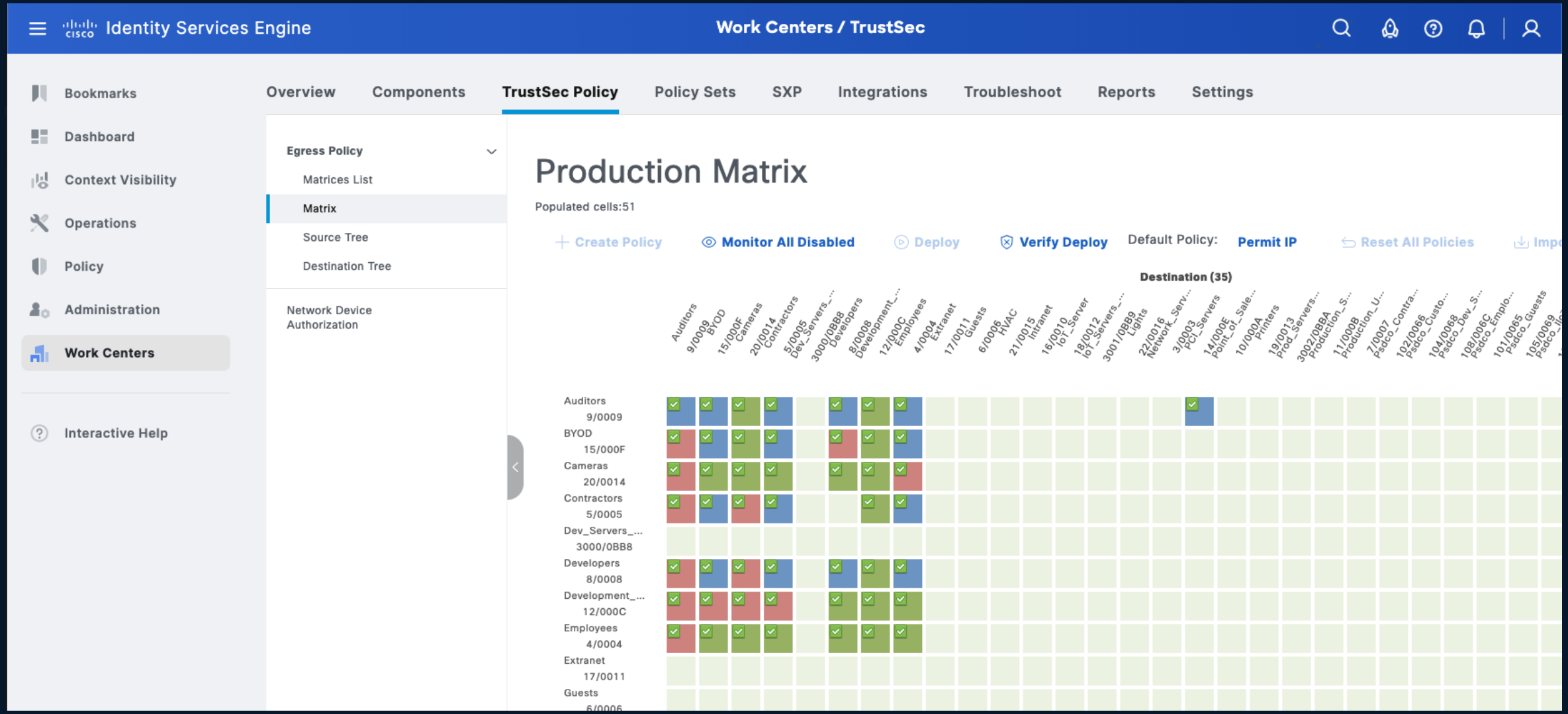
TAG Scaling Limits

Category	Limit
Theoretical (16-bit)	65,535
Cisco ISE Recommended	4,000
Catalyst Center Cluster	4,000
Hardware Enforcement (Typical)	255
Reserved Tags	0–15

Fewer is better

The first 16 tags (**0–15**) are reserved by Cisco for internal and system functions. Common examples include:
SGT 0: Unknown (Default for unclassified traffic)
SGT 2: TrustSec Devices (Used for network infrastructure devices)
SGT 15: Any (Used in policy to match all tags)

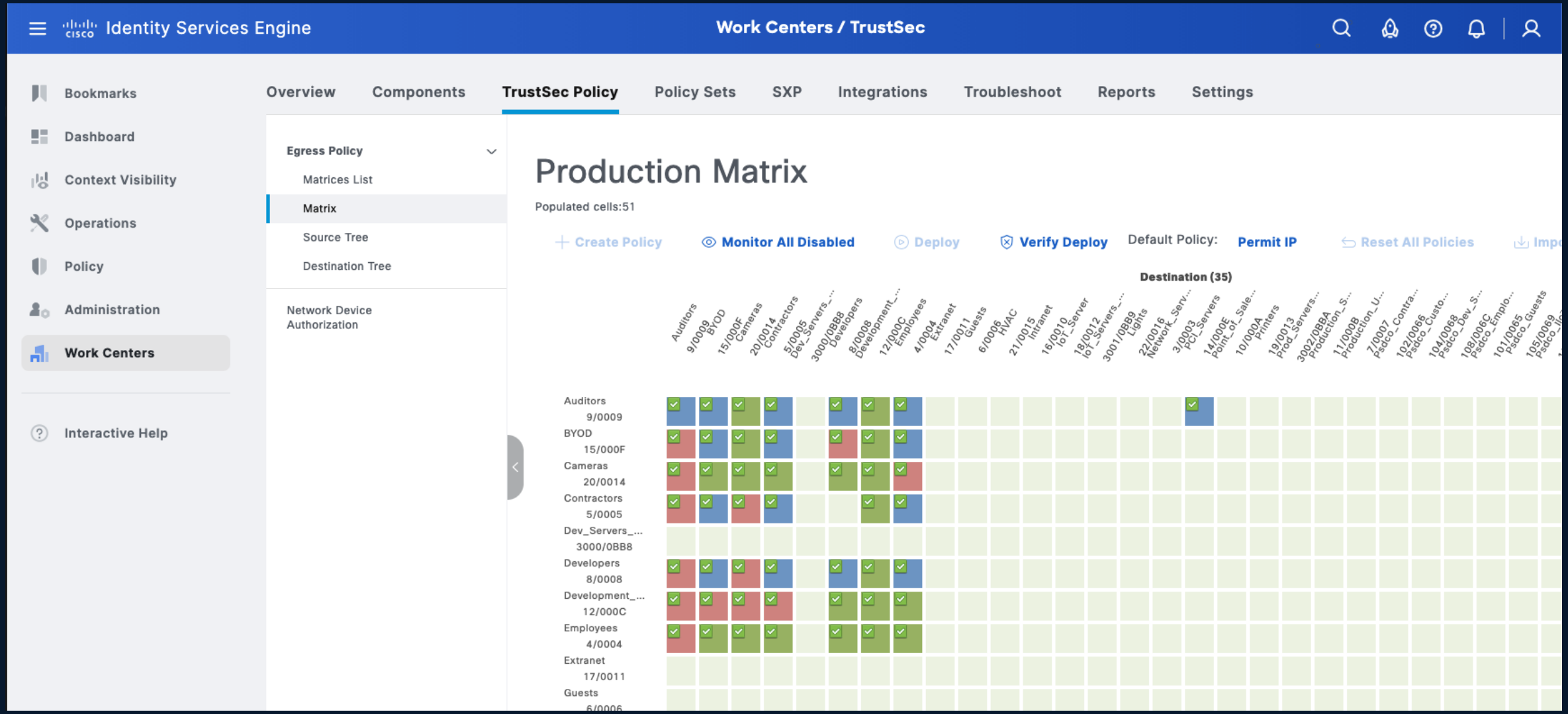
TrustSec Policy Matrix



Or is this better

```
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
```

Business Intent is clear



Cisco ISE

Cisco Identity Services Engine

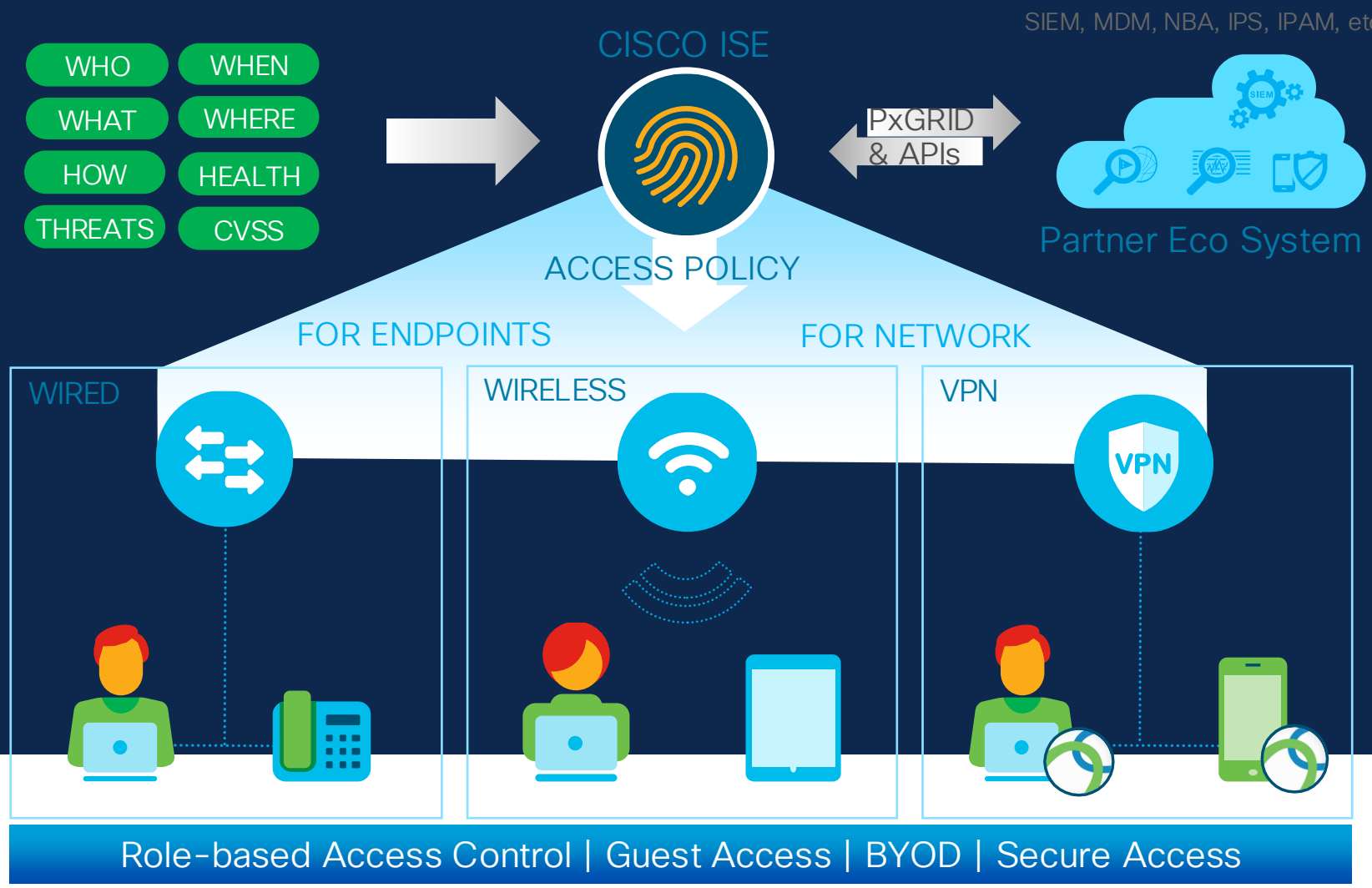
Cisco ISE

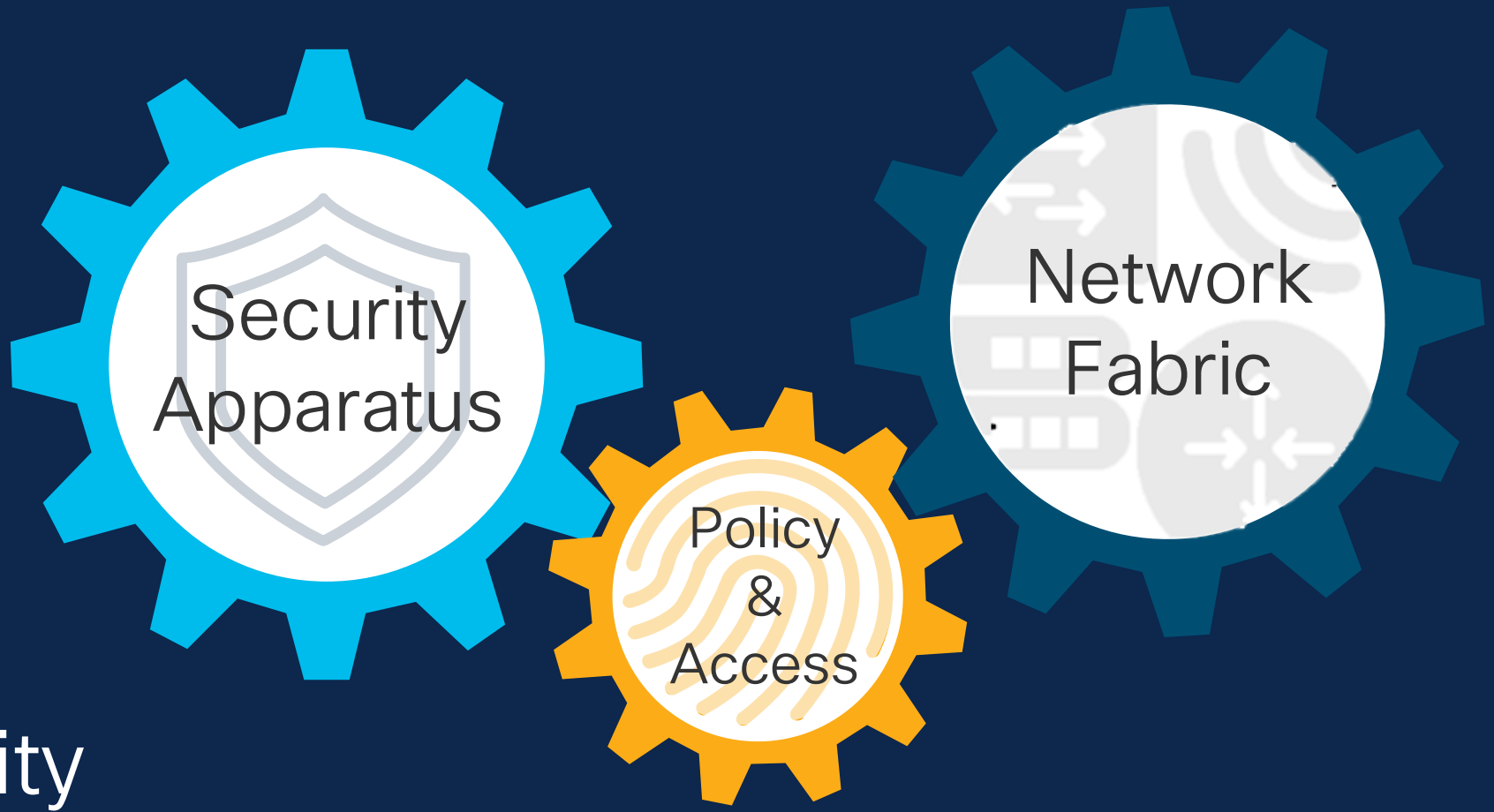
Cisco Identity Services Engine (ISE) is an industry leading, Network Access Control and Policy Enforcement platform

Visibility
Context about everything touching the network

Control
Network access control and segmentation

Compliance
Enterprises comply to industry regulations





Driving security intelligence through the Network Fabric

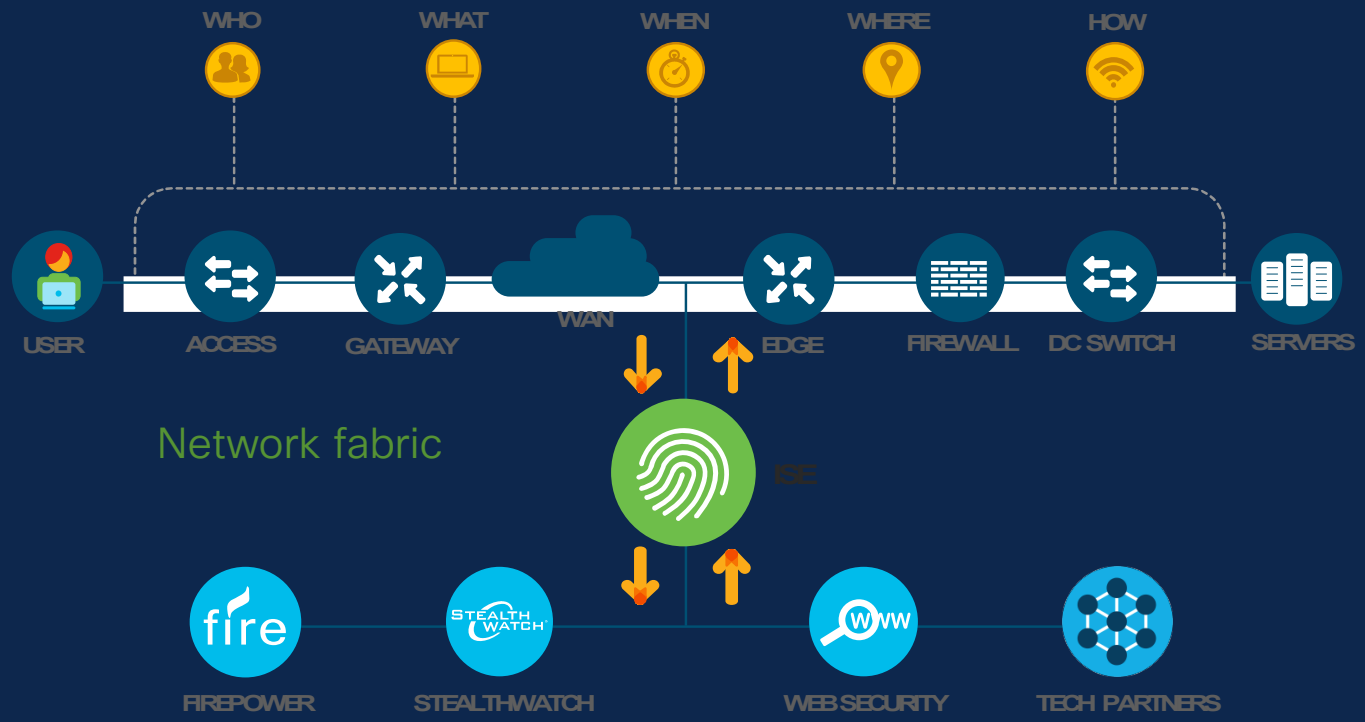
ISE is the center-piece of Secure Networking

ISE Capabilities

Enhances visibility by providing contextual information on who and what is on your network

Creates security policy used to automatically block malicious users or devices and remediate or mitigate threats

Accelerates threat identification by sharing intelligence with Cisco security and technology partner platforms



Business outcomes of ISE

In the Enterprise

Asset Visibility

See and share user and device details and consolidate security solutions with pxGrid

Access Control

Streamline enterprise network access policy over wired, wireless, & VPN access

Guest Access

Easily provide visitors secure guest internet access

BYOD & enterprise mobility

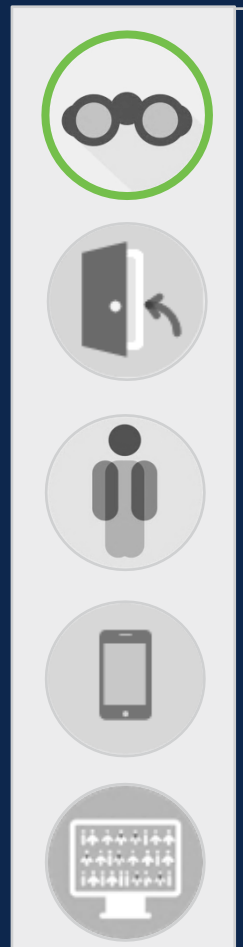
Seamlessly classify and securely onboard non-corporate devices

Segmentation

Segment network without VLAN and IP subnet. Simplify role-based access control

Make fully informed decisions

With rich contextual awareness



UNKNOWN

Without ISE

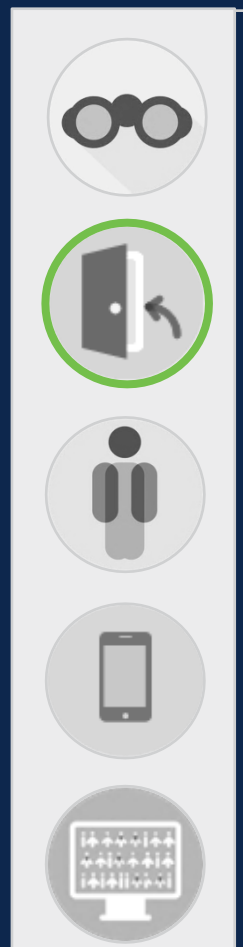
Poor context awareness		Rich context awareness
IP ADDRESS: 192.168.2.101	WHO	Bob (Employee)
Unknown	WHAT	Apple iPad/iOS/11.0.1
Unknown	WHEN	10:30 AM PST
Unknown	WHERE	Floor-1, San Jose, Building 19
Unknown	HOW	Wireless
Unknown	APPS	Firefox, MS Word, AnyConnect
Unknown	SPEC	Serial number, CPU, memory
Access to any device/user 	RESULT	Authorized network access 

KNOWN

With ISE

Control all access from a single location

Connect trusted devices to trusted services



Secure access from any location regardless of connection type

Apply access and usage policies across the entire network

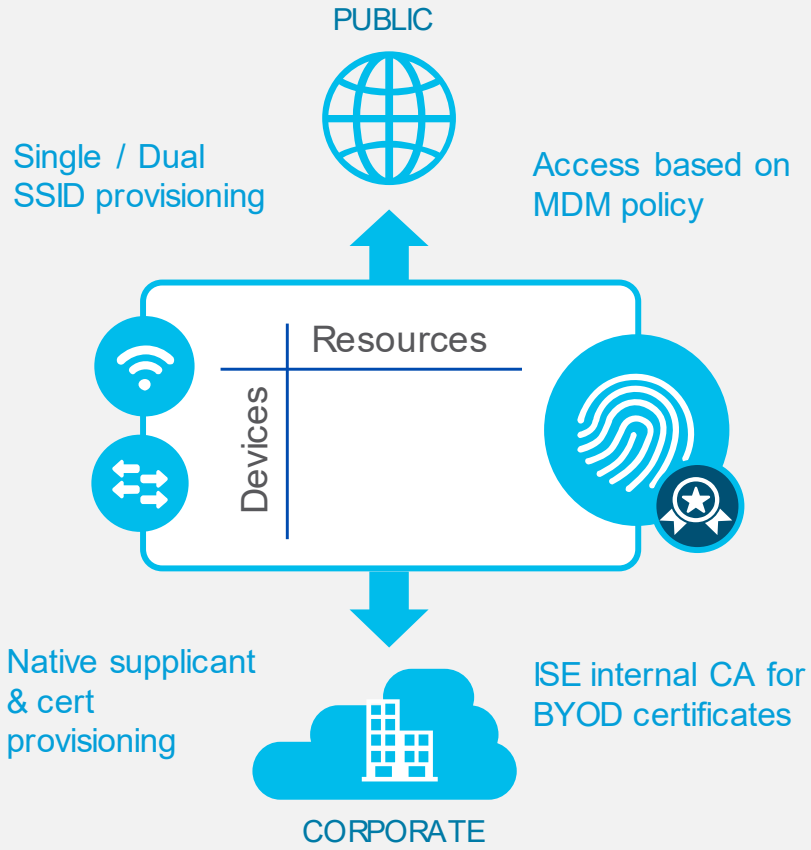
Monitor access, activity, and compliance of non-corporate assets

BYOD has never been so easy

Self served, flexible, secure

Device Support

- iDevice
- Android
- MAC OSx
- Windows
- ChromeOS



EMM integrations

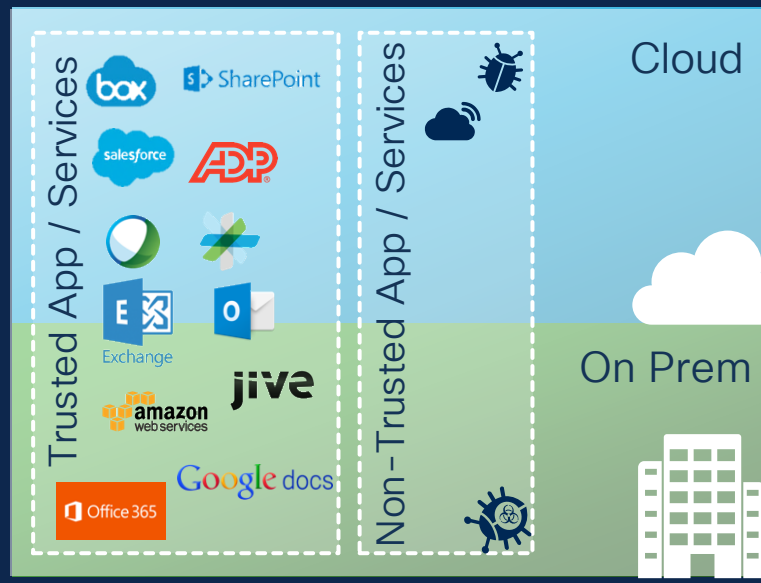
MaaS360 by Fiberlink
airwatch
SAP
IBM
CITRIX
MobileIron
Good
cisco Meraki

EMM: Enterprise Mobility Management | MDM: Mobile Device Management

Managing policy based on ‘Trust’

Connecting trusted users and devices to trusted services

CISCO IDENTITY SERVICES ENGINE



Improved Visibility and Decision

Software-Defined Segmentation, Service Access & Entitlement

Location-Free App/Service Access

Software Defined Access

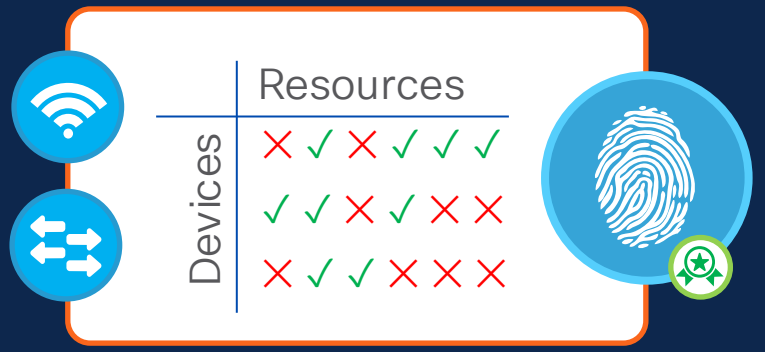
Traditional Networks Challenges

Network deployment challenges

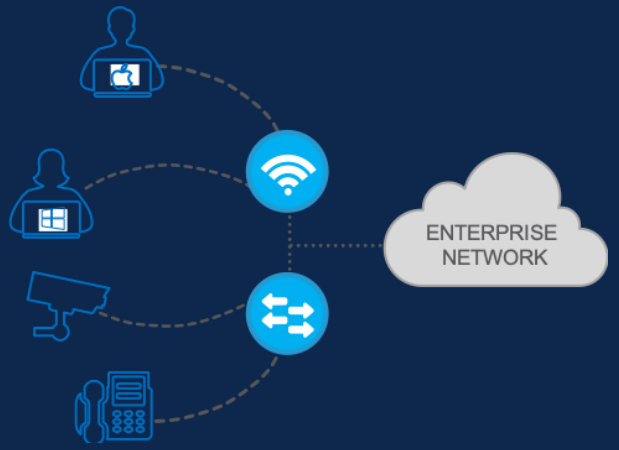
Network Infrastructure

Switching Routers Wireless

Network security challenges



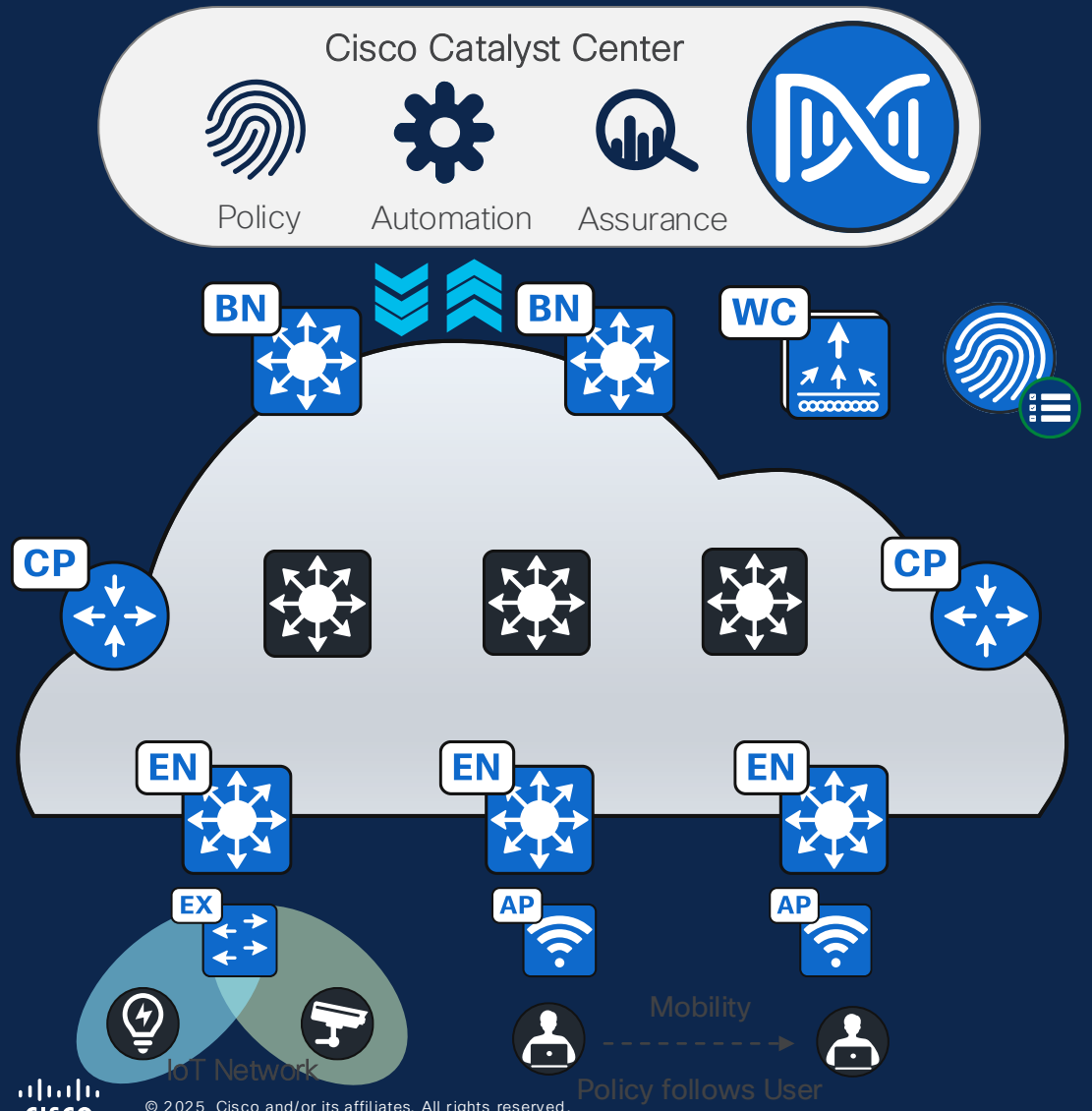
Wireless & wired network challenges



Network operations challenges

Cisco Software Defined Access

The Foundation for Cisco's Intent-Based Network



One Automated Network Fabric

Single Fabric for Wired and Wireless with full automation

Identity-Based Policy and Segmentation

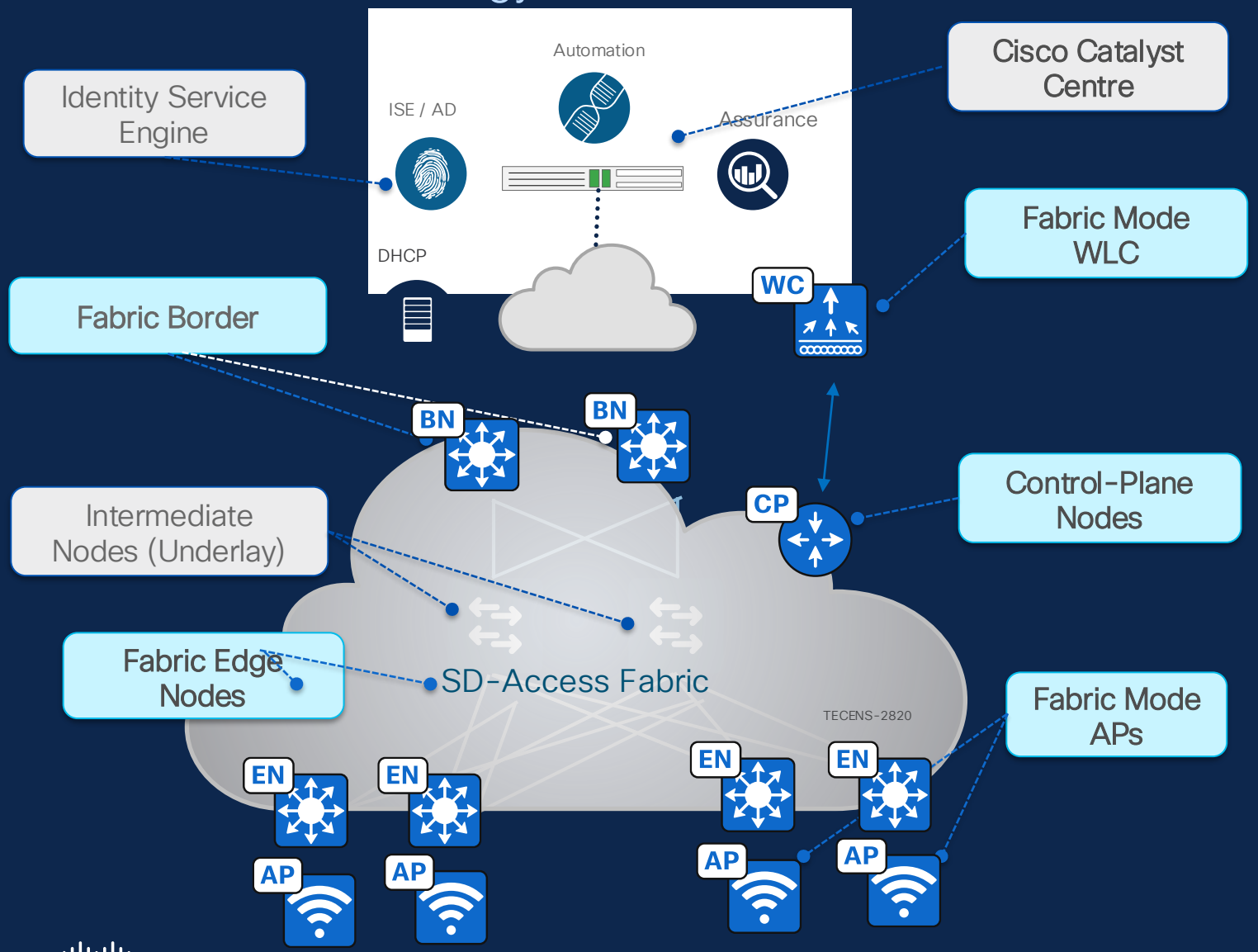
Policy definition decoupled from VLAN and IP address

AI-Driven Insights and Telemetry

Analytics and visibility into User and Application experience

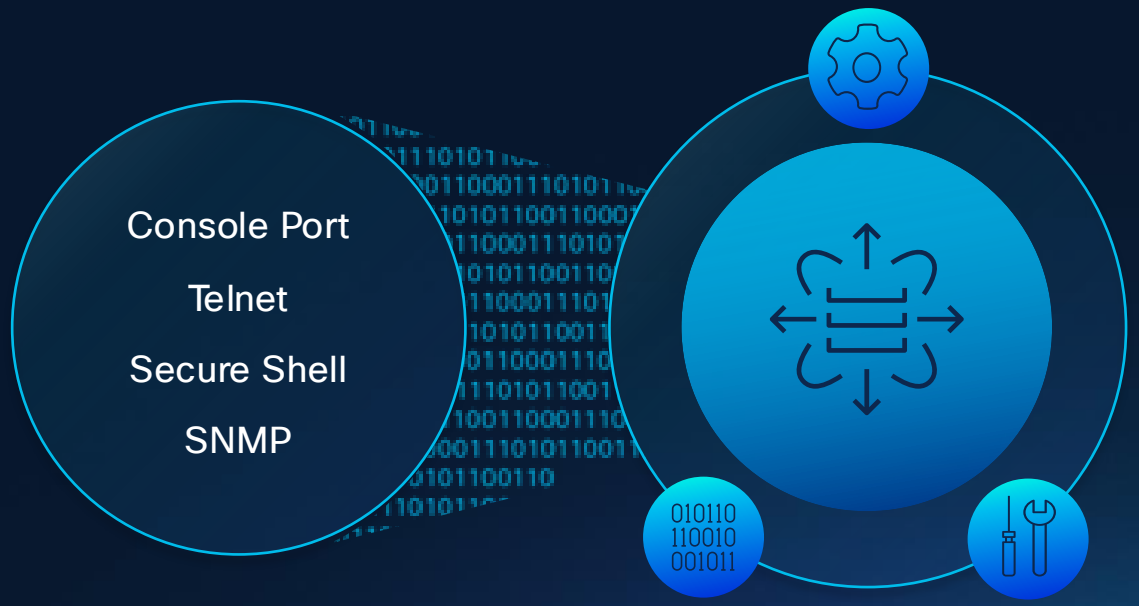
SD-Access Fabric Architecture

Roles and Terminology



- **Cisco Catalyst Center** – Enterprise SDN Controller provides GUI management abstraction via multiple Service Apps, which share information
- **Identity Service Engine** – External ID Services is leveraged for dynamic User or Device to Group mapping and policy definition
- **Control-Plane (CP) Node** – Map System that manages Endpoint ID to Location relationships. Also known as Host Tracking DB (HTDB)
- **Border Nodes** – A Fabric device (e.g.. Core) that connects External L3 network(s) to the SDA Fabric
- **Edge Nodes** – A Fabric device (e.g.. Access or Distribution) that connects wired endpoints to the SDA Fabric
- **Fabric Wireless Controller** – Wireless Controller (WLC) fabric-enabled, participate in LISP control plane
- **Fabric Mode APs** – Access Points that are fabric-enabled. Wireless traffic is VXLAN encapsulated at AP

Modern networks are exposing the limits of traditional tools



- Scalability limitations due to device-by-device access, time-consuming deployments, and manual troubleshooting
- Security risks stemming from delayed threat protection and response, human error, and lack of policy-based segmentation.
- Lack of visibility and delayed response driven by siloed, manual monitoring and limited traffic analysis.

As connected users and devices grow, traditional management methods struggle to keep pace

SD-Access Support

Fabric ready platforms for your digital ready network

Switching

Catalyst 9200

Catalyst 9200CX

Catalyst 9500

Catalyst 9300

Catalyst 9300LM

Catalyst 9300CX

Catalyst 9400

Catalyst 9400X

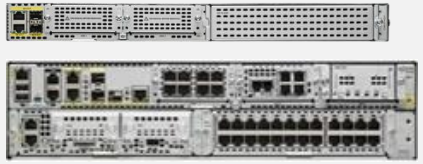
Catalyst 9500

Catalyst 9600

Catalyst 9500X

Routing

ASR-1000-X/HX



ISR 4300/4400

Catalyst 8000

CSRv/8000v

Wireless

Catalyst 9800

AIR-CT5520

AIR-CT8540

AIR-CT3504

Wave 2 APs (1800, 2800,3800/9100)

Extended

Cisco Digital Building

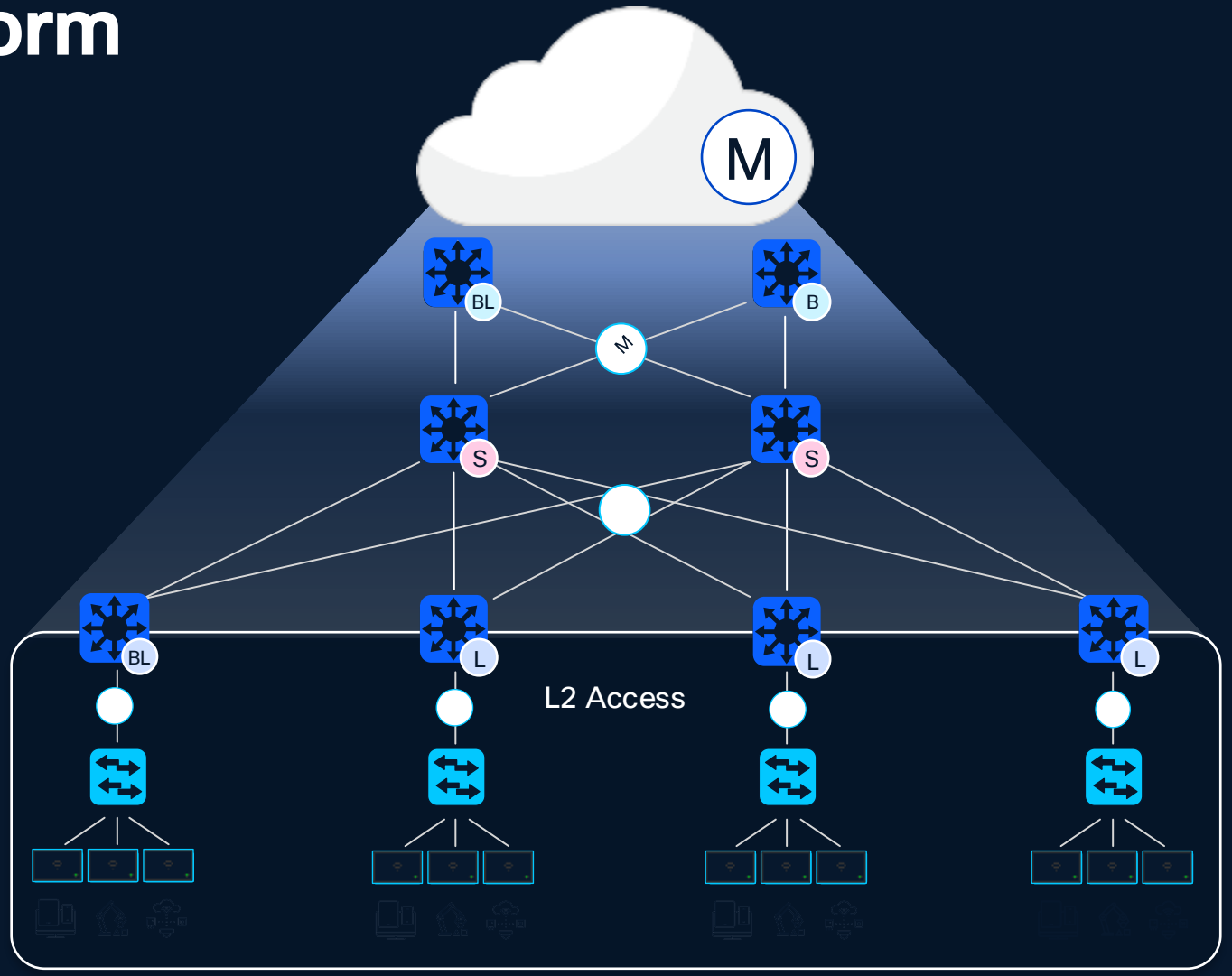
Catalyst 3560-CX

IE Series
(3K/4K/5K/9K)

[Cisco Software-Defined Access Compatibility Matrix]

Intent-based fabric orchestration from a unified cloud platform

- Reduce the number of steps it takes to provision, manage, and troubleshoot sites
- Build and enforce segmentation policies that adapt to your network based on the intent of the user
- Deploy in a non-disruptive way on top of the devices you already own



Strategy to Intent-based Secure Networking

Aka How do We get there

Cisco Zero Trust Segmentation

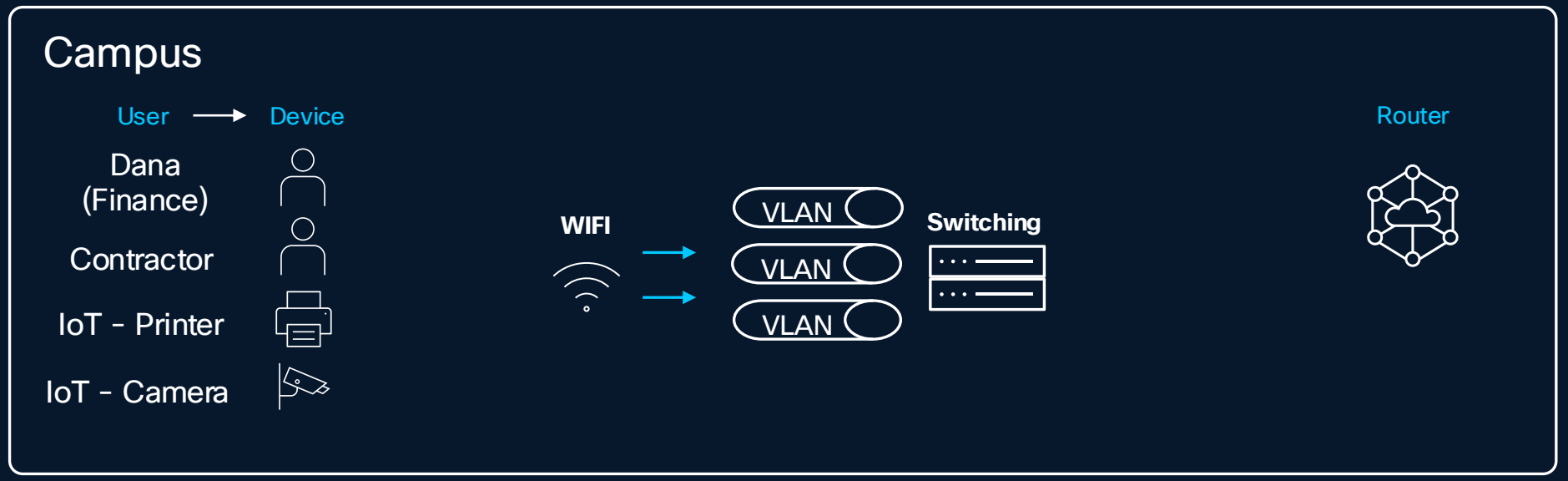
Campus and Unified Branch User to App

Dashboard

Config

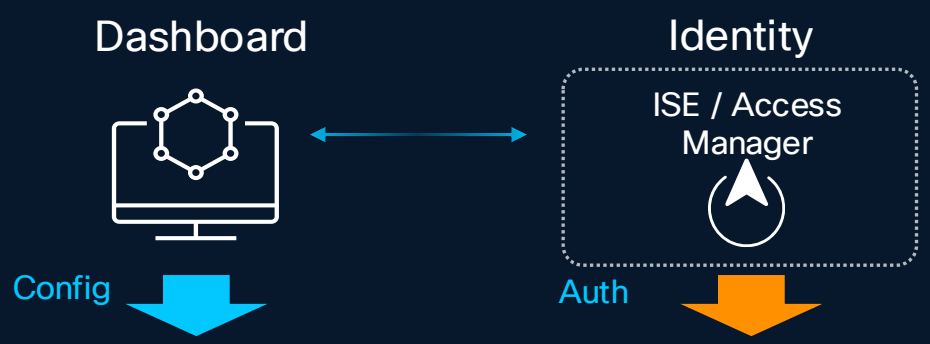
Current Network Infrastructure

- Basic VLAN segmentation only
- No user or device visibility or policies



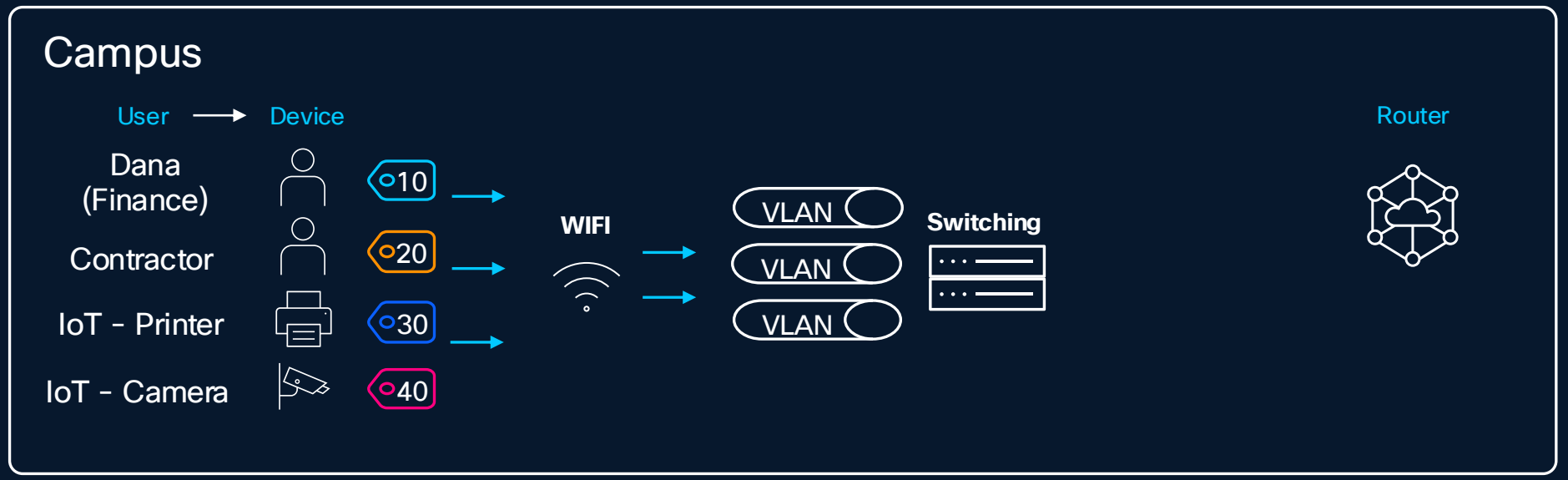
Cisco Zero Trust Segmentation

Campus and Unified Branch User to App



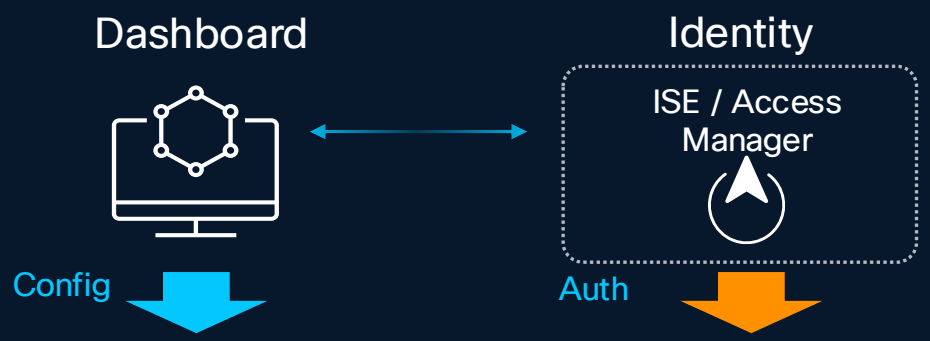
With Identity Services Engine or Access Manager:

- User and Device policies
- TrustSec SGT Tag Micro Segmentation



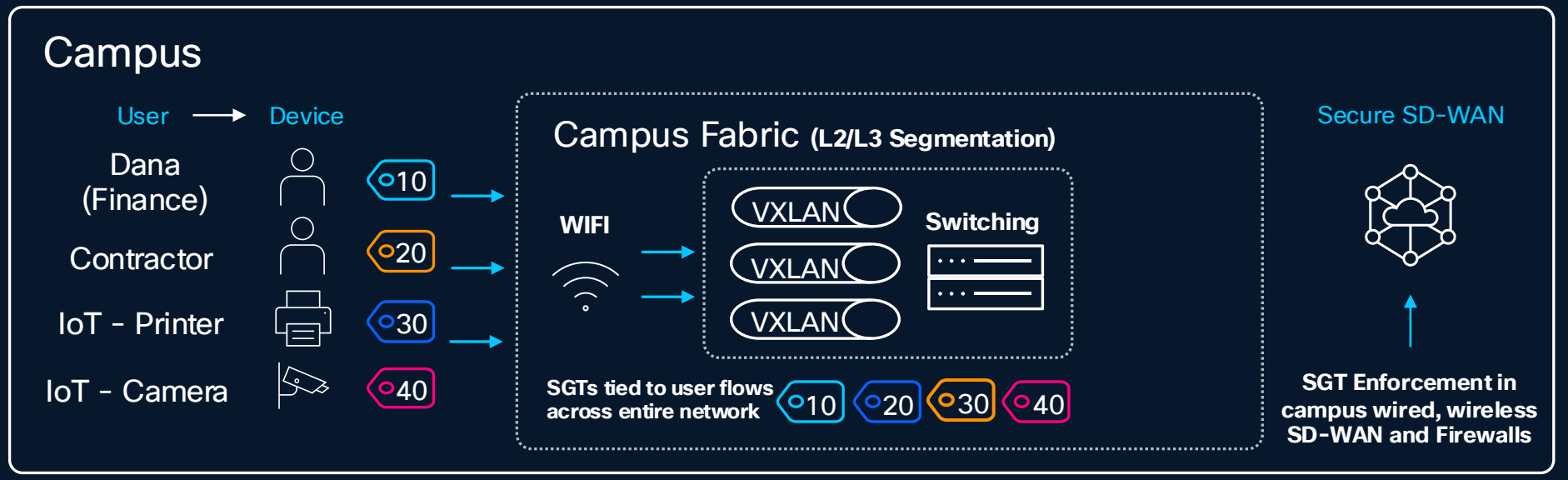
Cisco Zero Trust Segmentation

Campus and Unified Branch User to App



Campus Fabric:

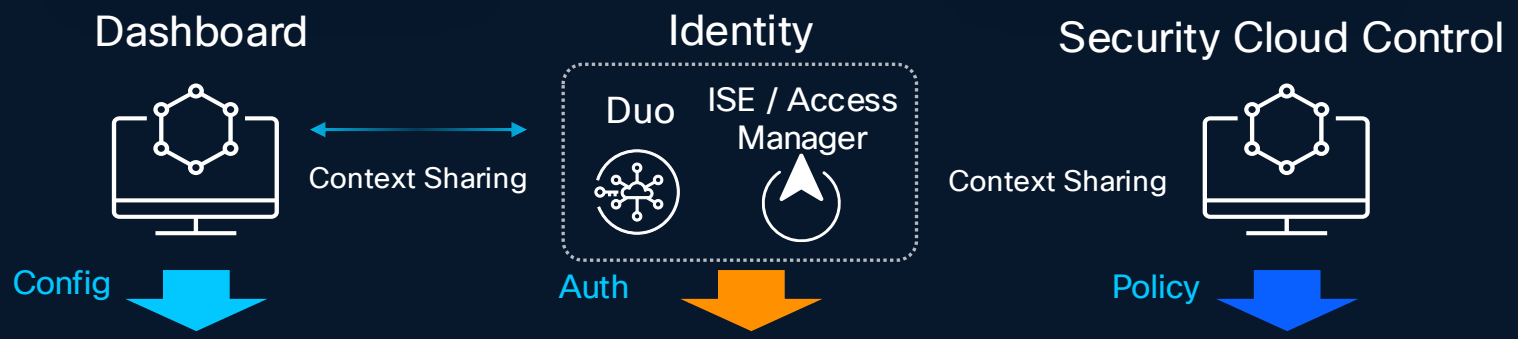
- Macro Segmentation with VRF / VXLAN
- Integrated Wired, Wireless and SD-WAN policies



Cisco Zero Trust Segmentation

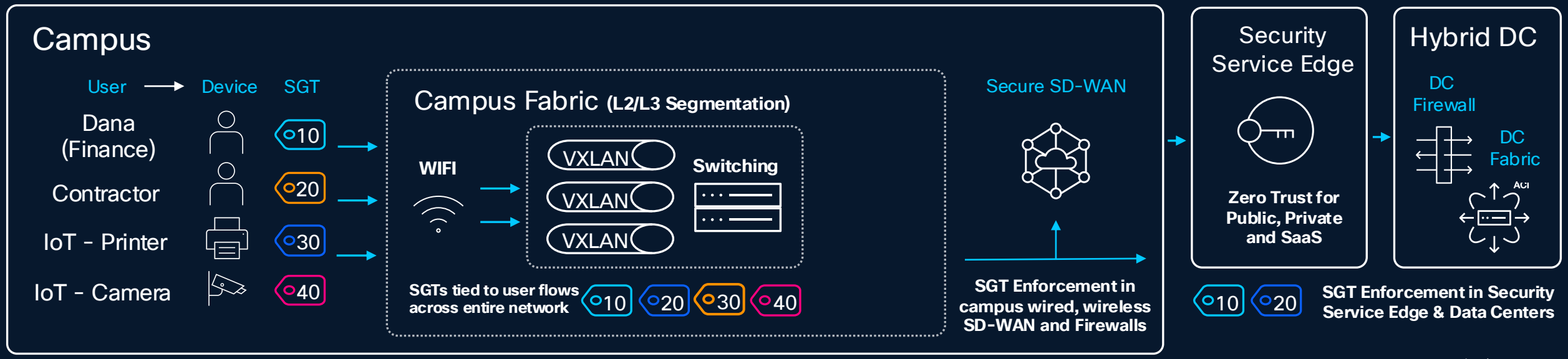
Campus and Unified Branch User to App

Unified policy



Security Cloud Control

- Unified policy between network, firewalls, SSE and Hybrid DC fabric
- User identity trust



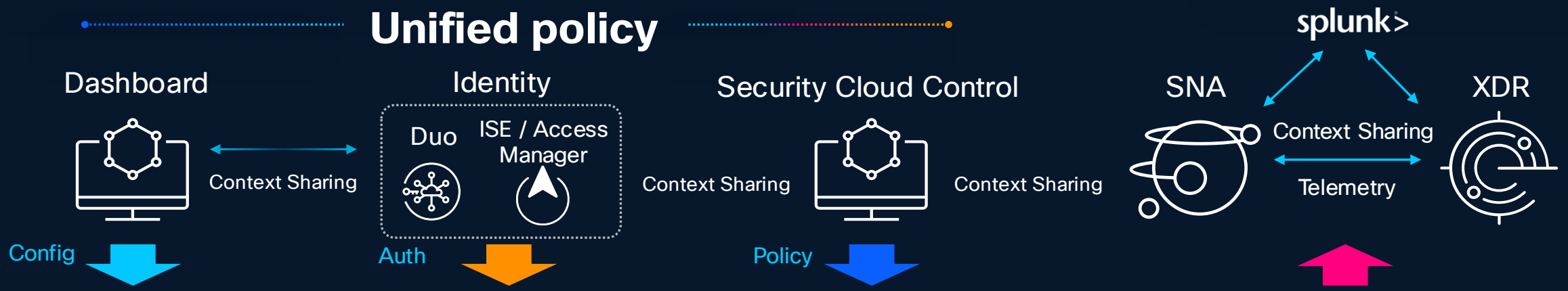
Cisco Zero Trust Segmentation

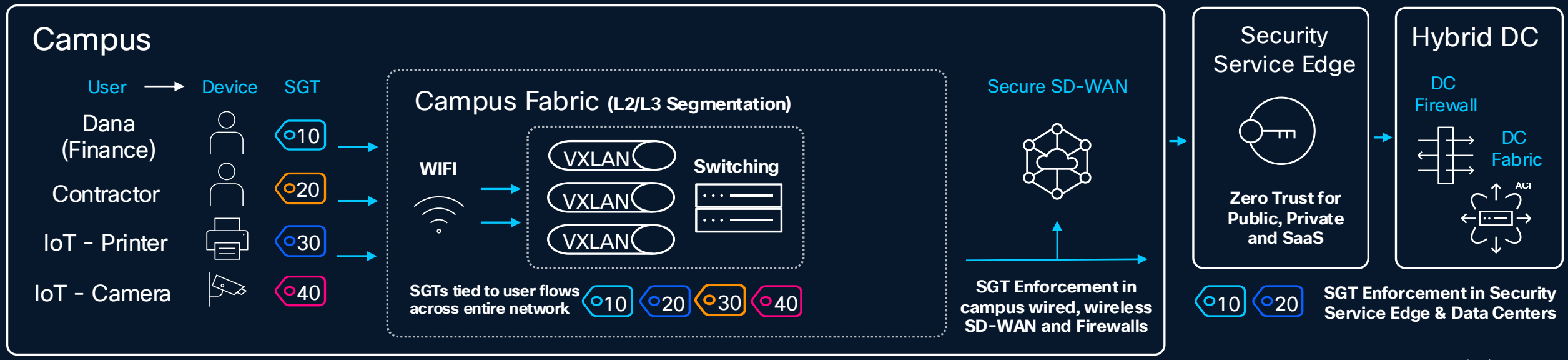
Splunk, XDR and Secure Network Analytics for SOC use cases

Campus and Unified Branch User to App

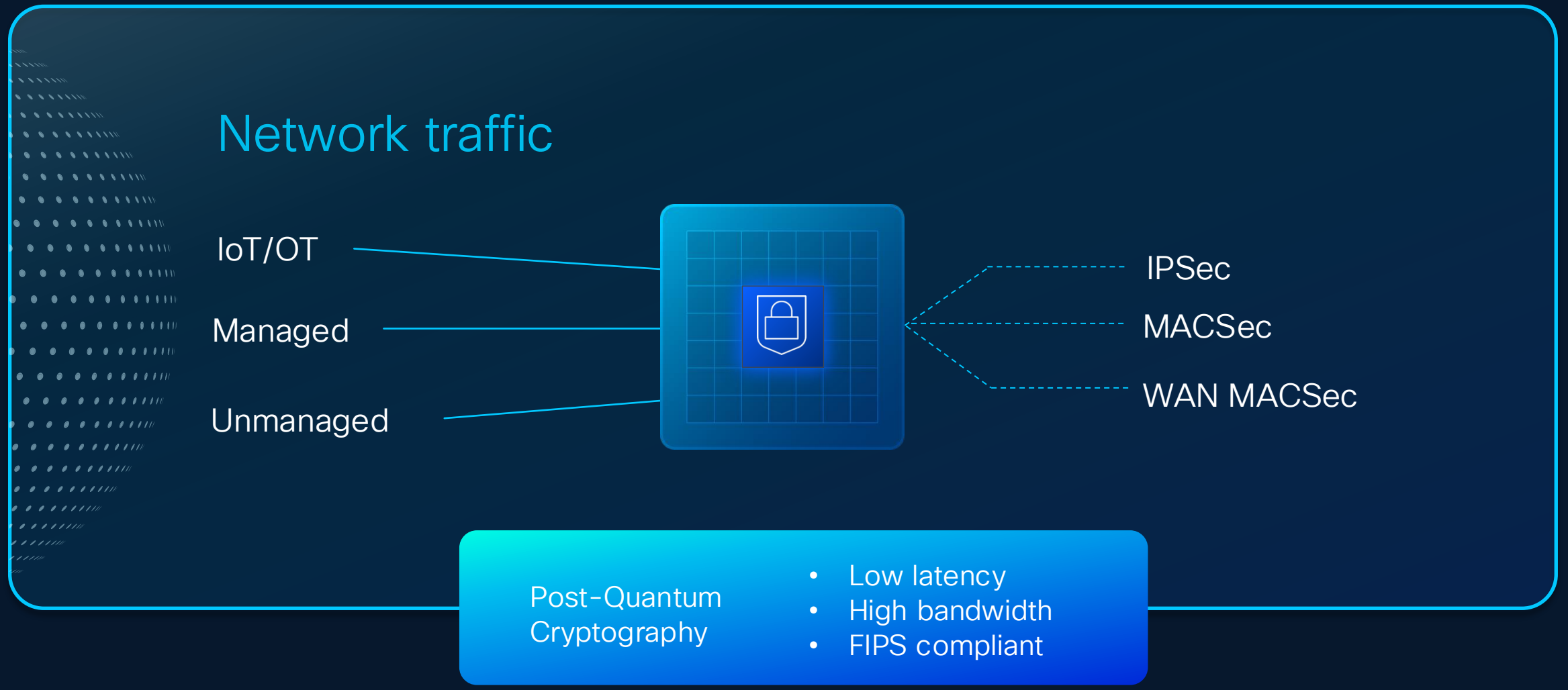
Unified policy

Unified security



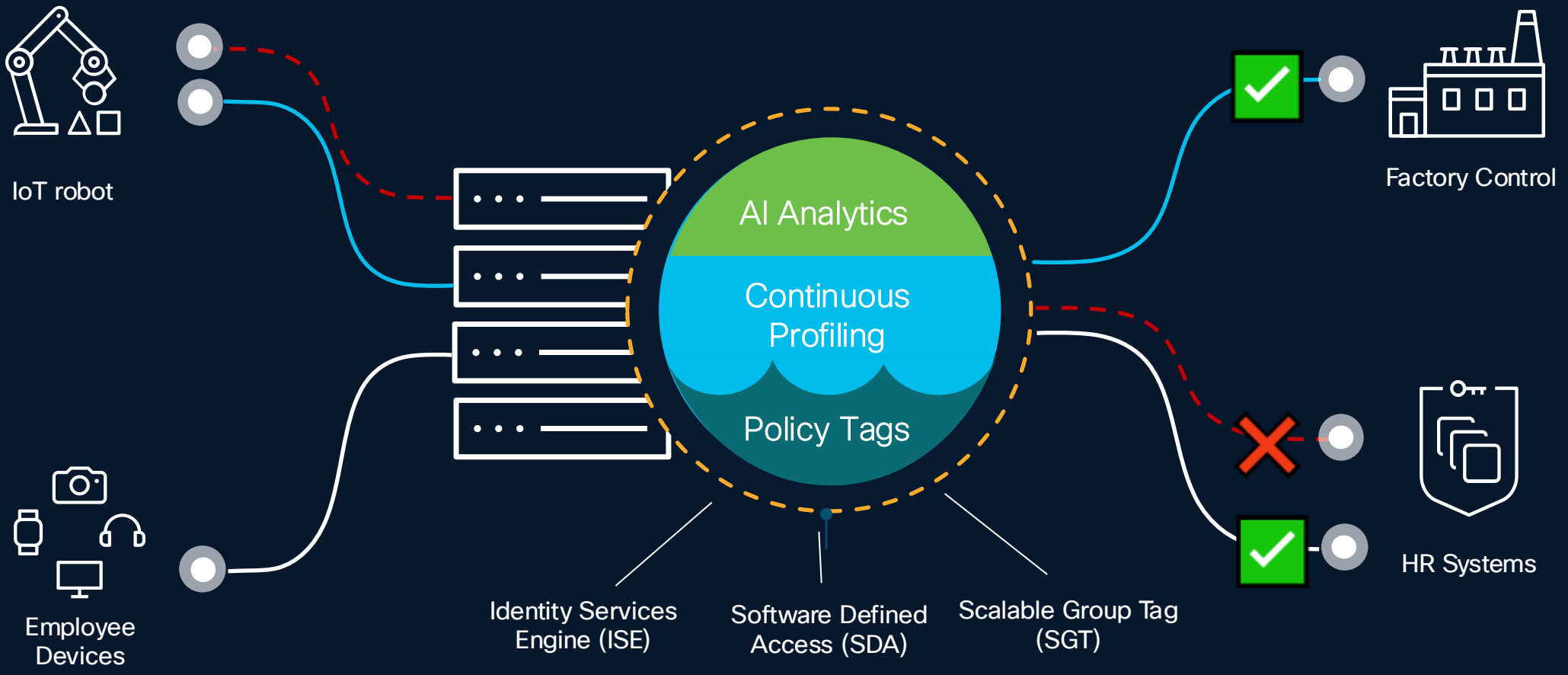


Securing network connectivity



Cisco as a Leader for Fabric Architectures

Scalable micro-segmentation to protect every connection



Thank you