CISCO Connect

Unlocking Segmentation: How Cisco Delivers With ISE, TrustSec, Firewalls, Secure Workload & ACI

Jacob Schneider
Segmentation SE

Chase Abrams
Segmentation Advisor

March 24, 2026

Cisco Segmentation Specialists

Chase Abrams –

Principal Advisor, Segmentation

- 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

Jacob Schnieder–

Segmentation Solutions Architect

- 22+ years of experience designing & deploying Cisco Security & Networking solutions
- 12 years @ Cisco
- Cisco Live Distinguished Speaker
- Deep Background in Service Provider, Enterprise Networking and Security
- CCIE (#24940)
- 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 is a **patchwork**

The World Has Changed

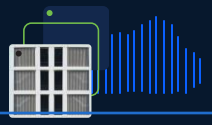
New Applications, Infrastructures, and Work Styles are changing the rules!

IoT is coming of age

IoT devices might be smart, but they are not secure. **How do I protect them?**

Cyber attacks are on the rise

Attackers somehow find a way. **How do I limit the threat radius?**



Applications are cloud-powered

Perimeter is gone. It's not your data center, but it's your problem. **How do I implement end to end segmentation across domains?**

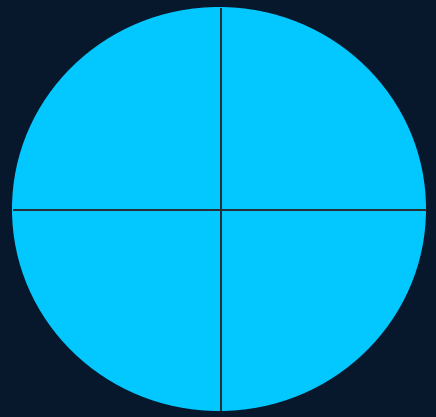
The workplace has gone hybrid

Users need to connect from anywhere on anything. **How do I enforce consistent Access Policy?**

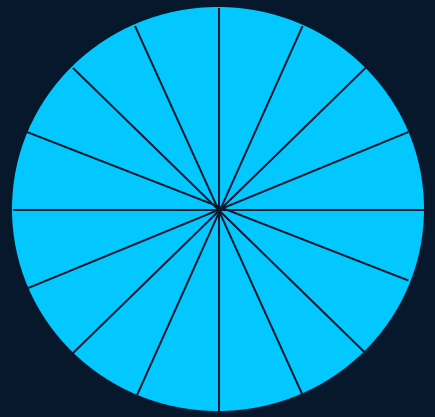
What is Segmentation?

"*Segmentation is the practice of dividing a larger system into smaller, isolated parts to improve control, security, and performance.*" -> Thanks AI ChatBot!!

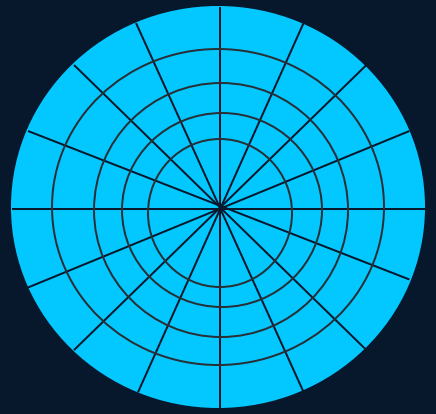
No Segmentation



Macro Segmentation



Micro Segmentation



Nano Segmentation??

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

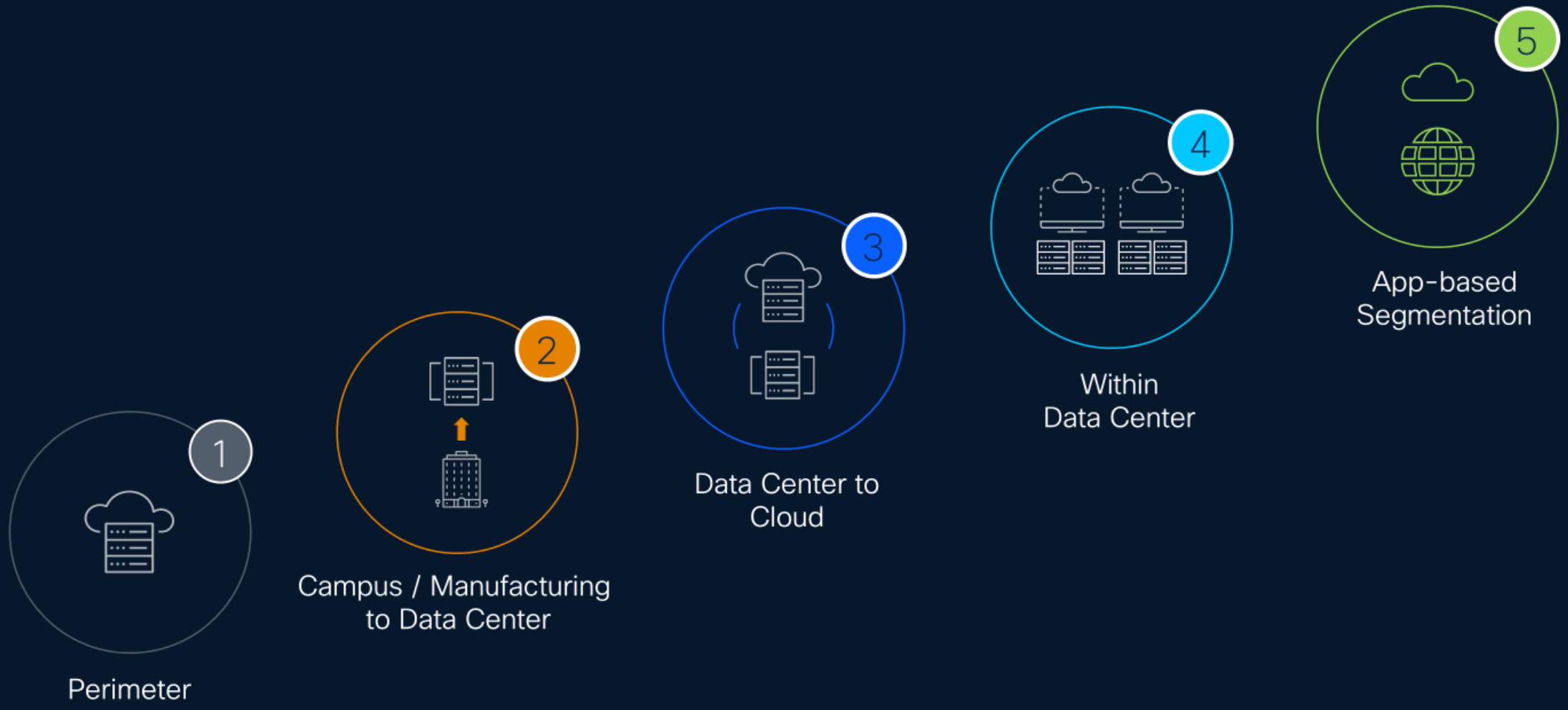
Why it matters to our customers

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

Cisco innovations

1998	2008	2014	2016	2022	2023	2024
VRF, PVLAN	Cisco TrustSec (SGT)	Cisco ACI and VXLAN – EVPN	Cisco Secure Workload (Tetration)	Cisco Multicloud Defense (Valtix)	Cisco Secure Access	Cisco HyperShield

Segmentation that meets you where you are



Enterprise Segmentation Outcomes We Deliver **Today**

From identity to workload enforcement. One architecture across campus and data center.

- Identity & Visibility – ISE as the control plane
- Campus Segmentation – SGT based policy enforcement
- Data Center Micro-segmentation – Application mapping and policy simulation
- Unified Policy Enforcement – consistent policy across domains
- Operationalization and Simplification – One policy model. No tool sprawl.

Zero Trust Realized

Cisco's Zero Trust Platform

Security Cloud Control

Securing Users (Universal ZTNA)

Securing Apps (Hybrid Mesh Firewall)

Access Control

AI Access

North South Segmentation

AI Model Protection

East West Macro/ Microsegmentation

Distributed Exploit Protection

One Integrated Architecture

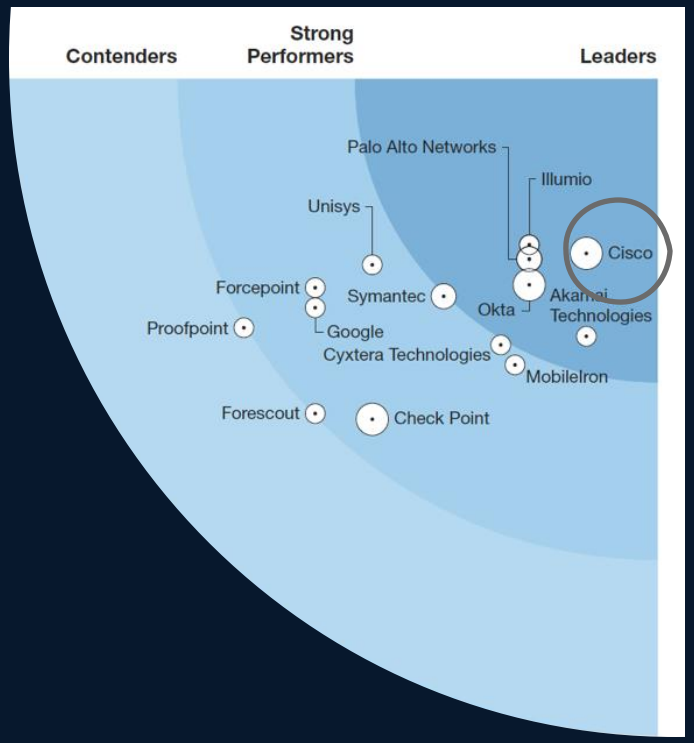
Cisco TALOS, Cisco XDR & Splunk

cisco

Segmentation in the Campus

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

45%
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

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

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-tcnac

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

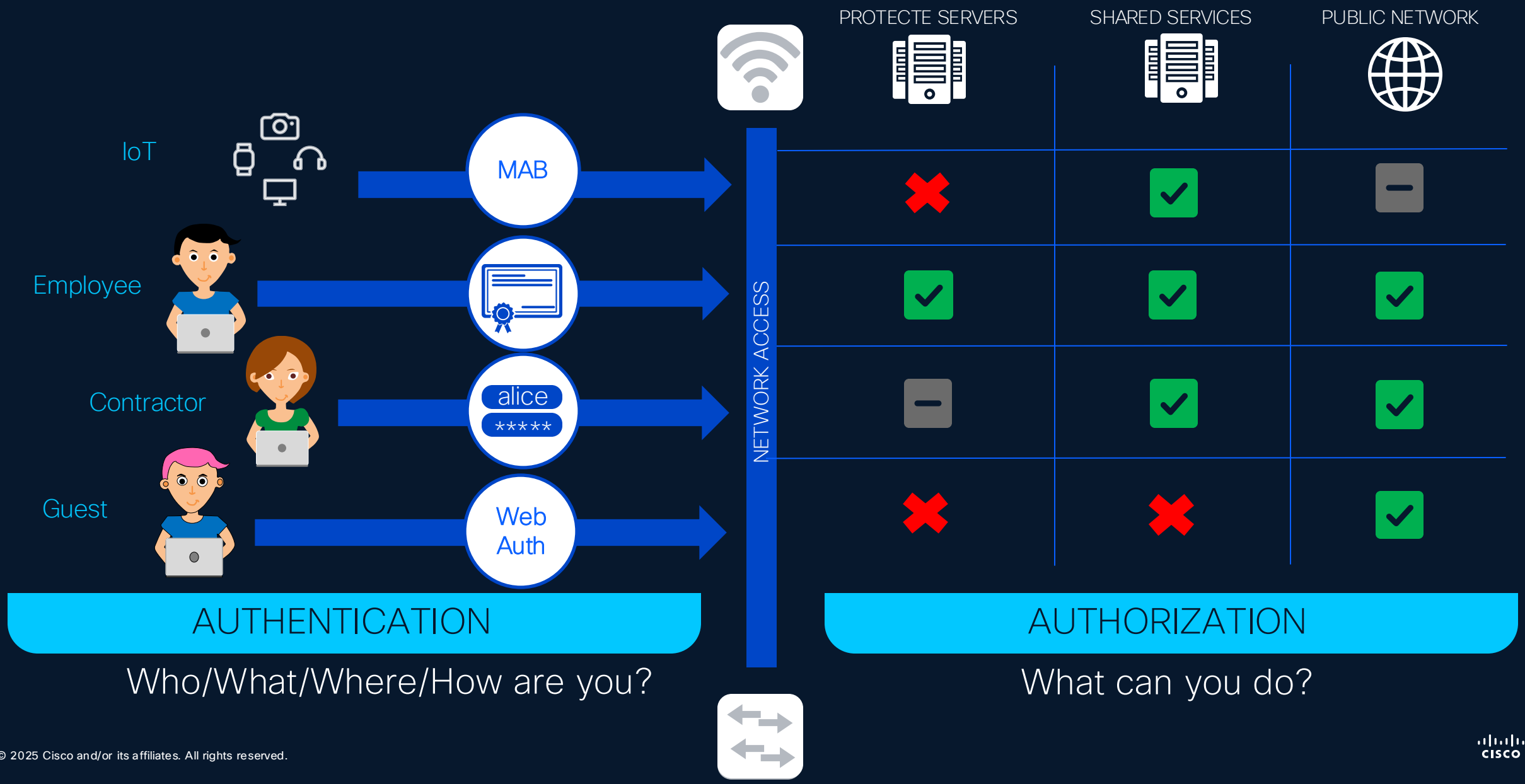
- Entra, AD
- LDAP, ODBC
- MDM
- SAML/MFA

Security Services

- Cloud Analytics
- Secure Firewall
- Partners

Visibility → **Segmentation** → **Containment**

Least Privilege Access

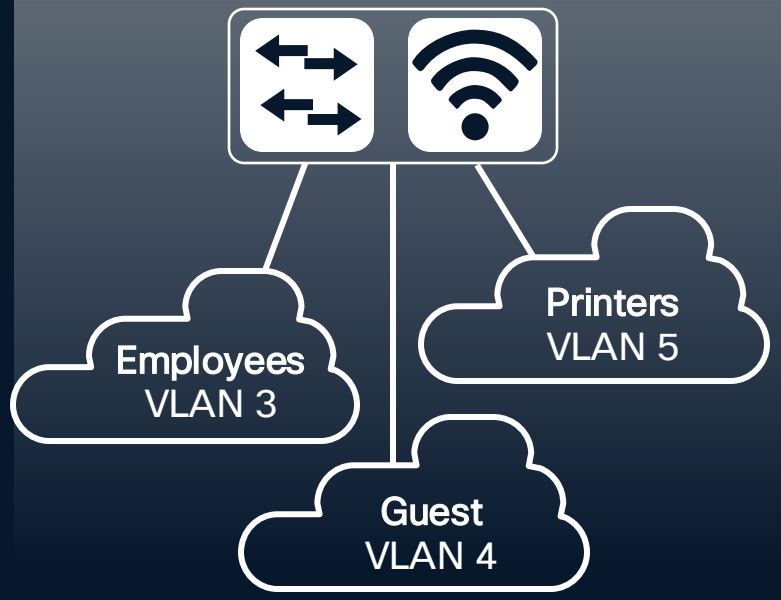


Network Segmentation Options

Beyond RADIUS Access-Accept / Access-Reject

VLANs

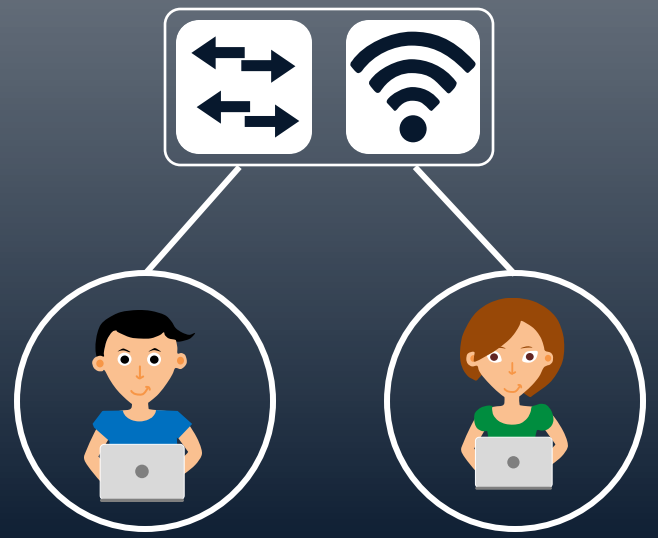
Dynamic VLAN Assignments



Per port / Per Domain / Per MAC

ACLs: DL, Named, DNS

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



Employee

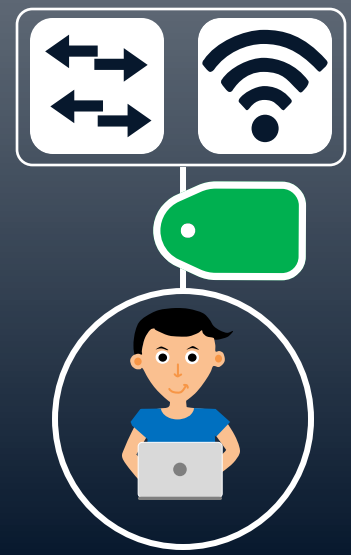
```
permit ip any any
```

Contractor

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

Security Group Tags

Cisco Group-Based Policy



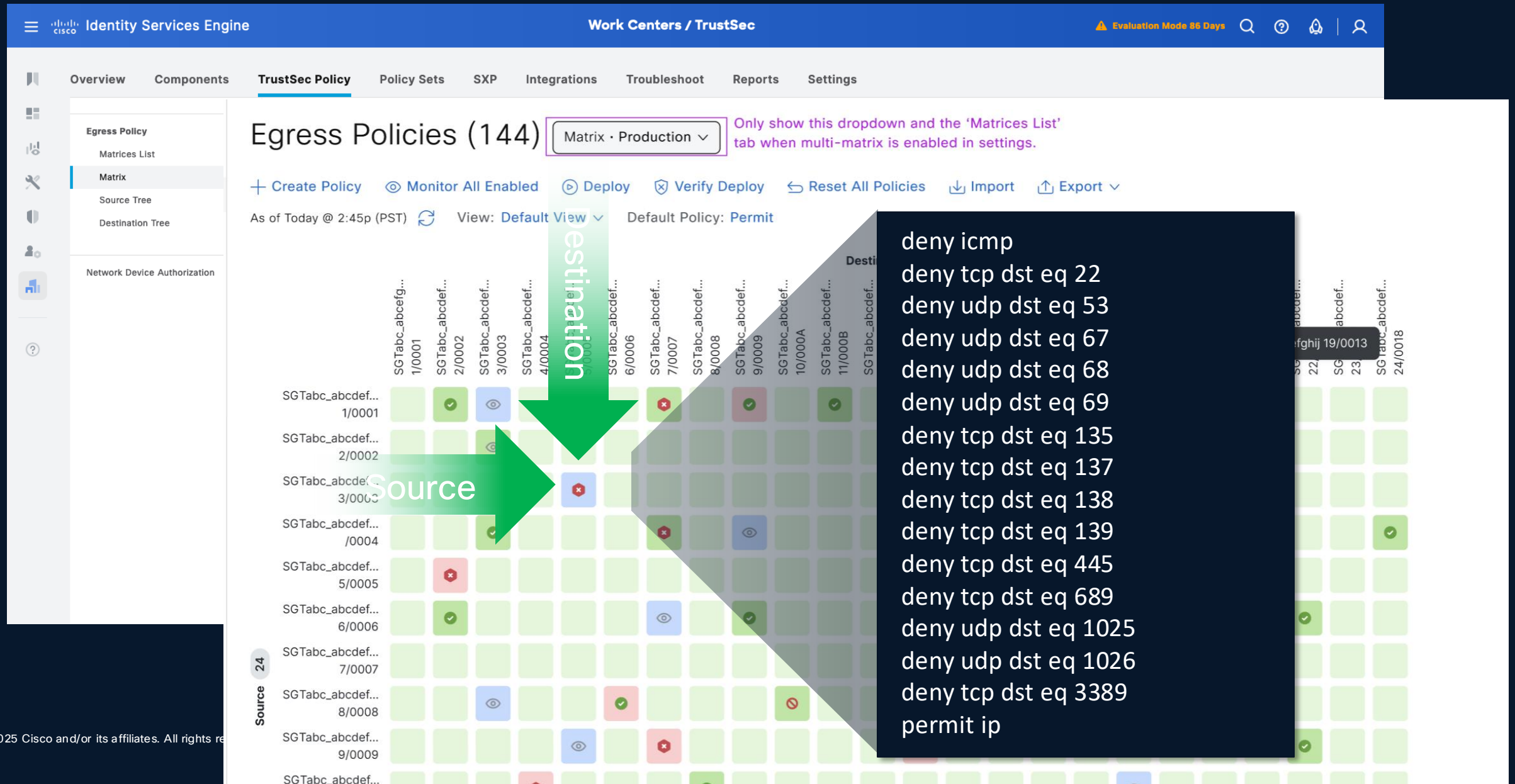
16-bit SGT assignment and
SGT based Access Control

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
```


cisco

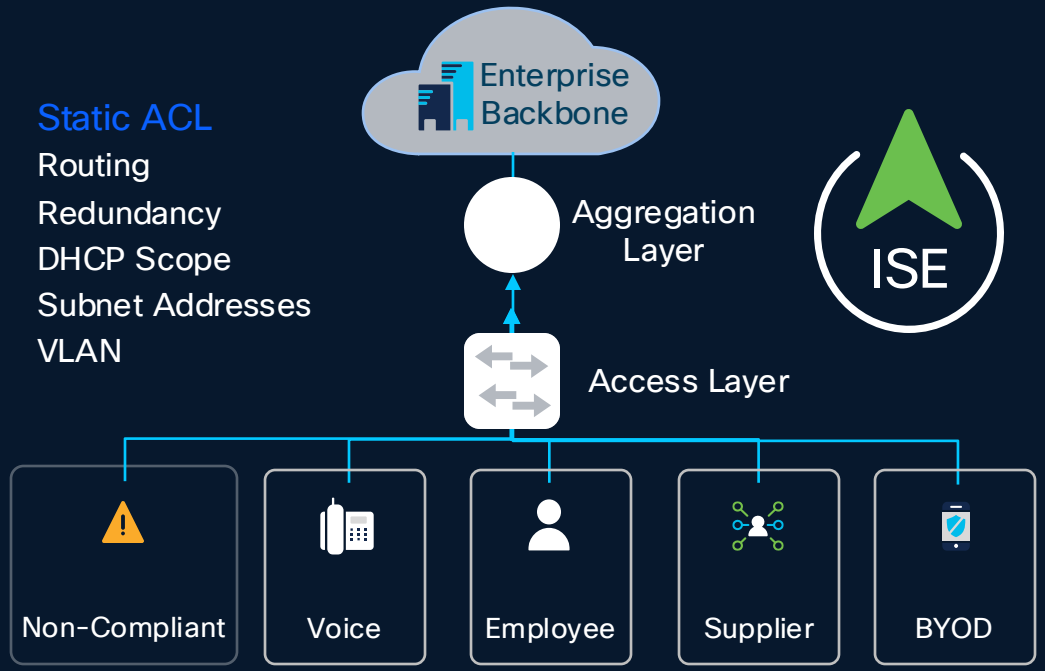
Business Intent Is Clear With TrustSec



Group Based Policy Simplifies Segmentation

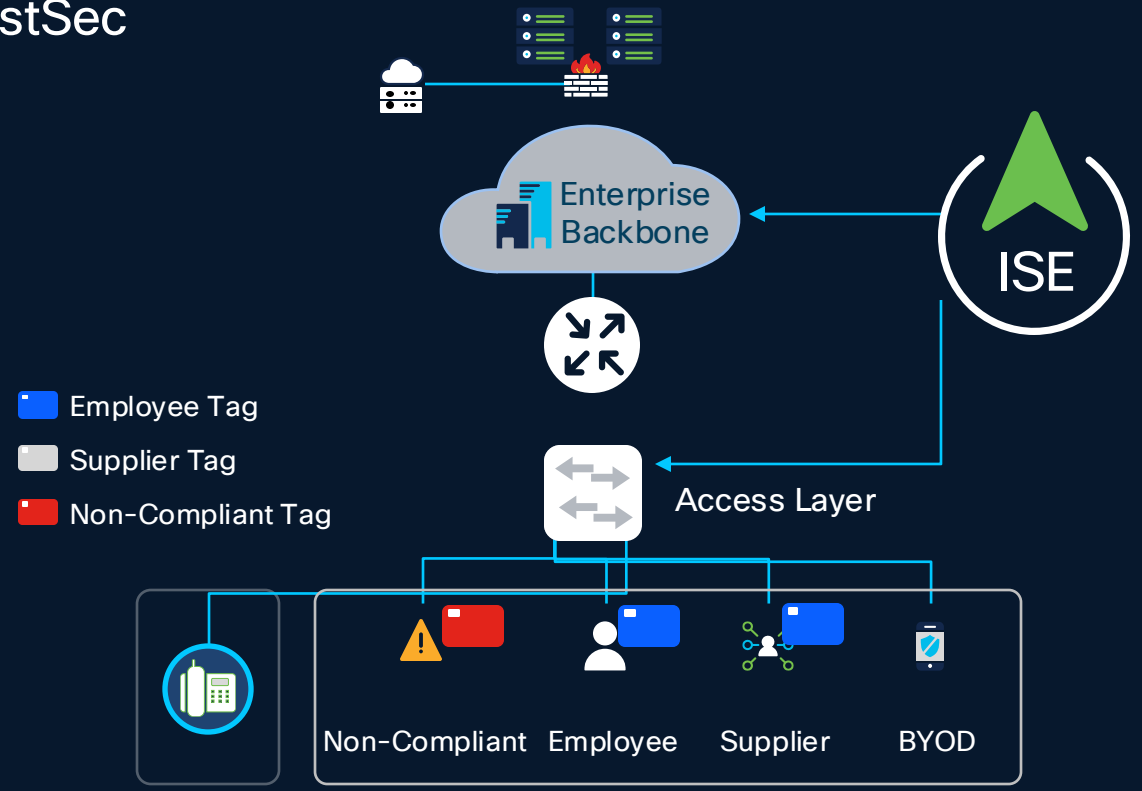
Traditional Segmentation

Static ACL
Routing
Redundancy
DHCP Scope
Subnet Addresses
VLAN



Security Policy based on Topology
High cost and complex maintenance

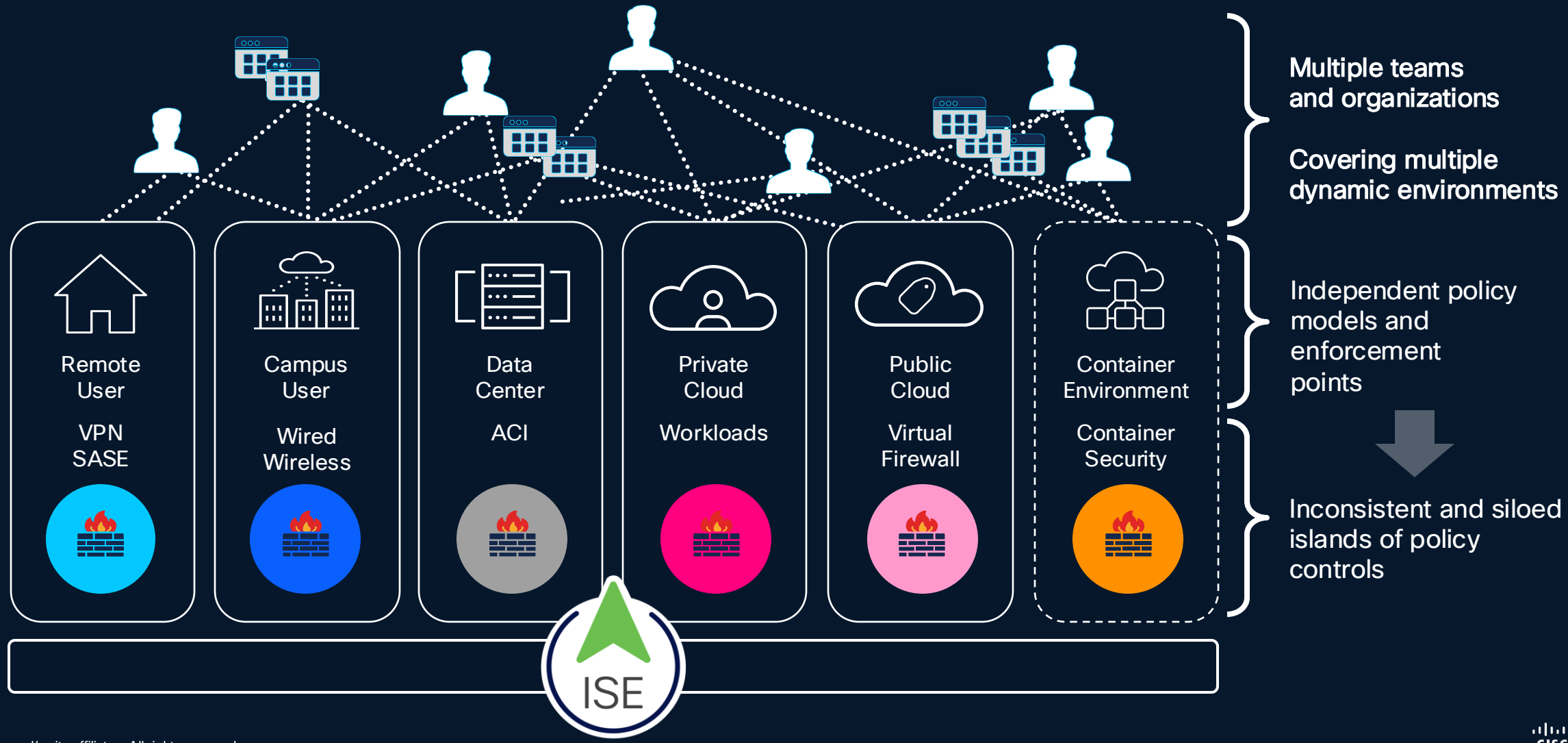
TrustSec



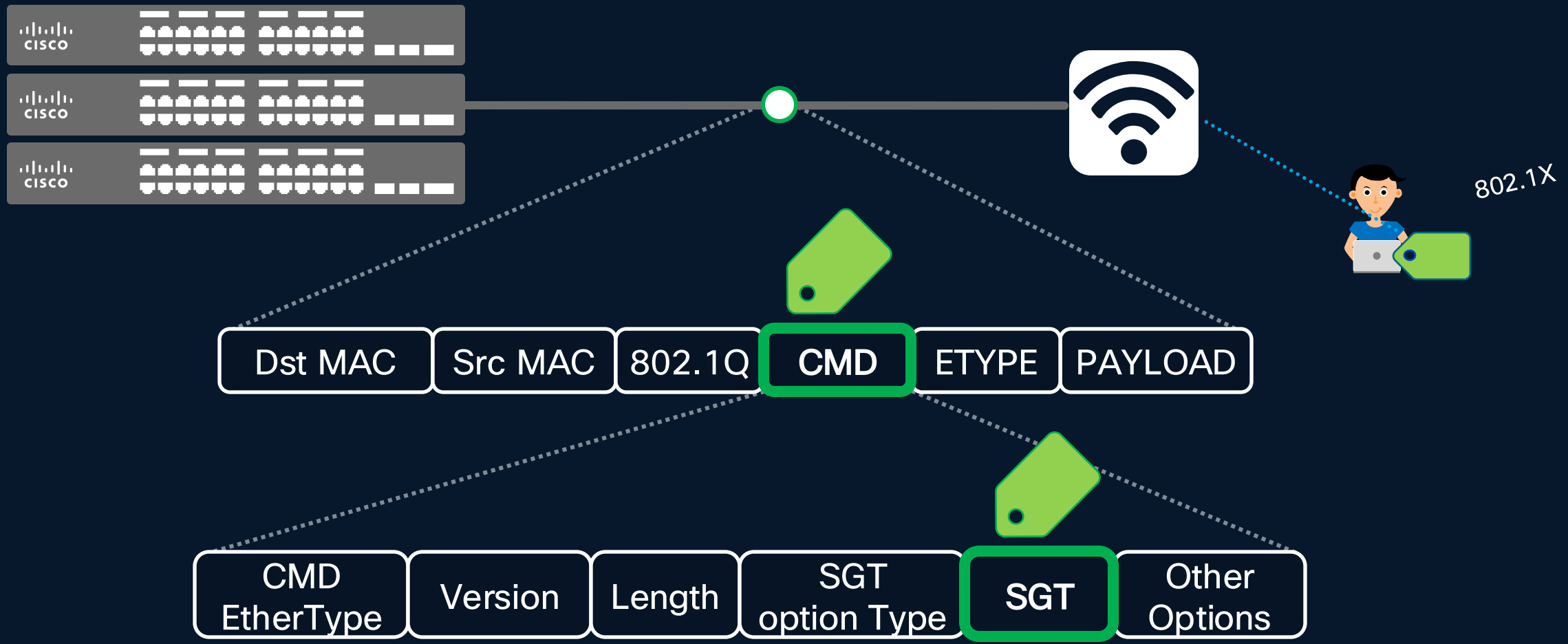
Use existing topology and automate
security policy to reduce OpEx

Common Policy with Security Group Tags (SGTs)

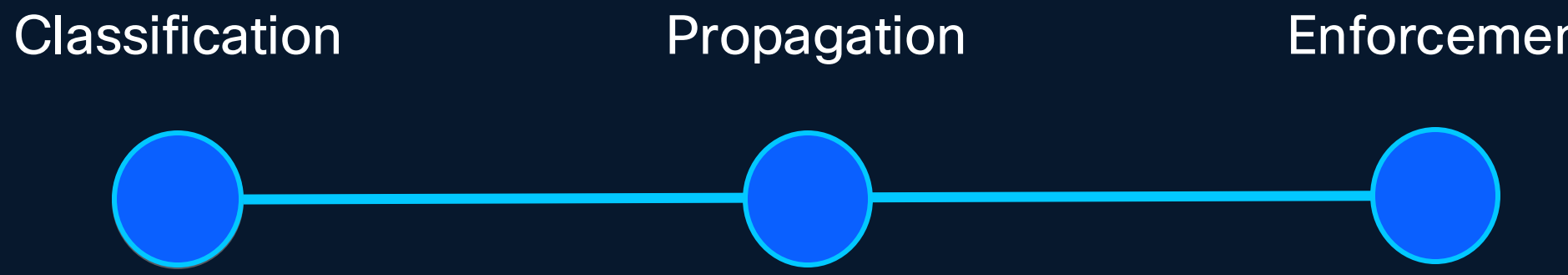
The common language across network industry products



TrustSec Security Group Tags (SGTs)



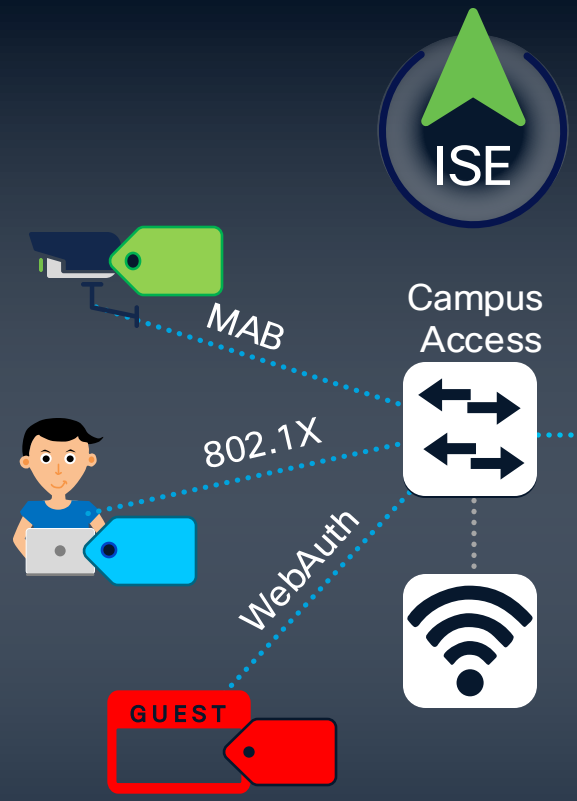
TrustSec Mechanisms



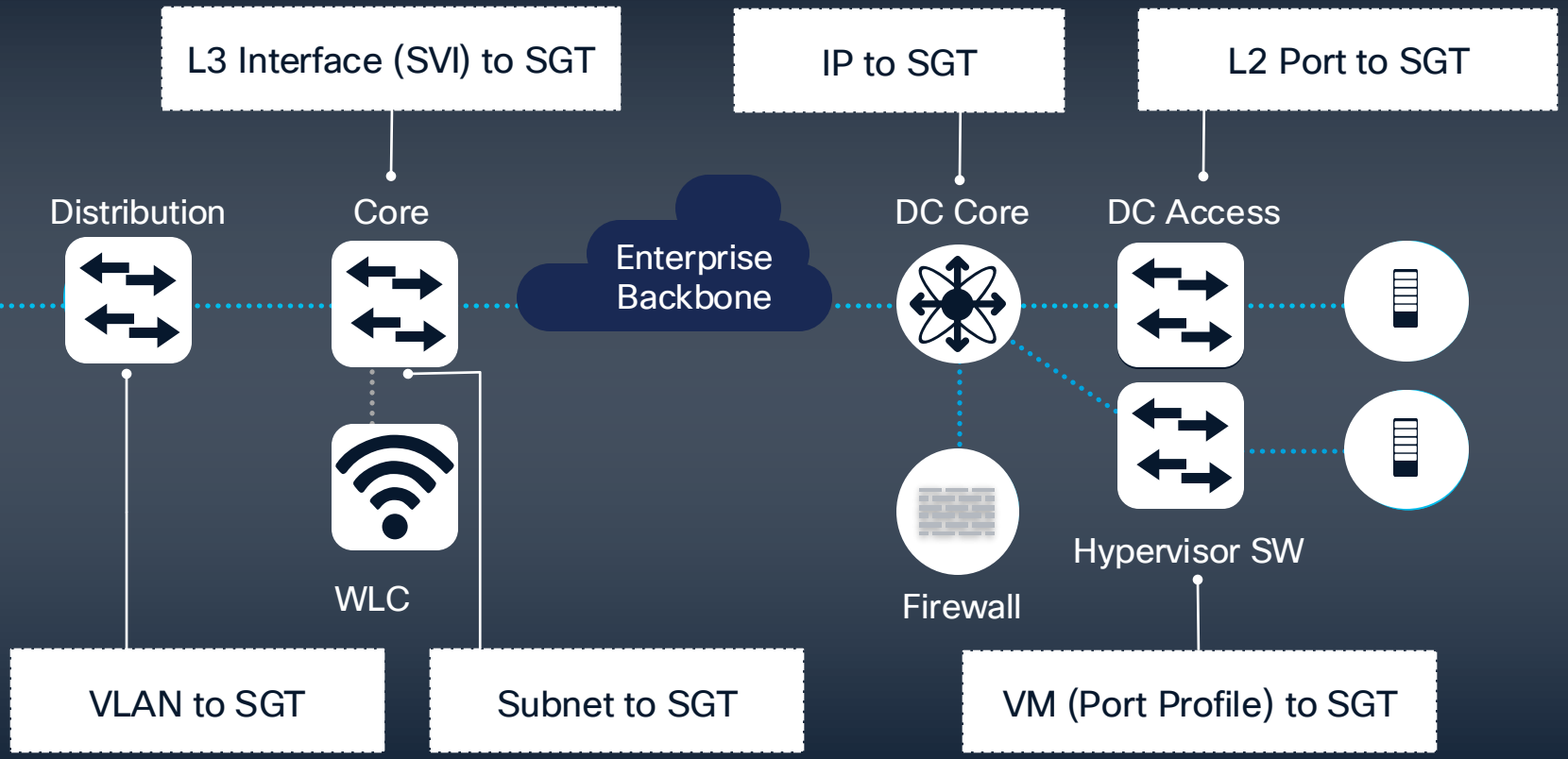
Classification Mechanisms

Classification Propagation Enforcement

Dynamic Classification

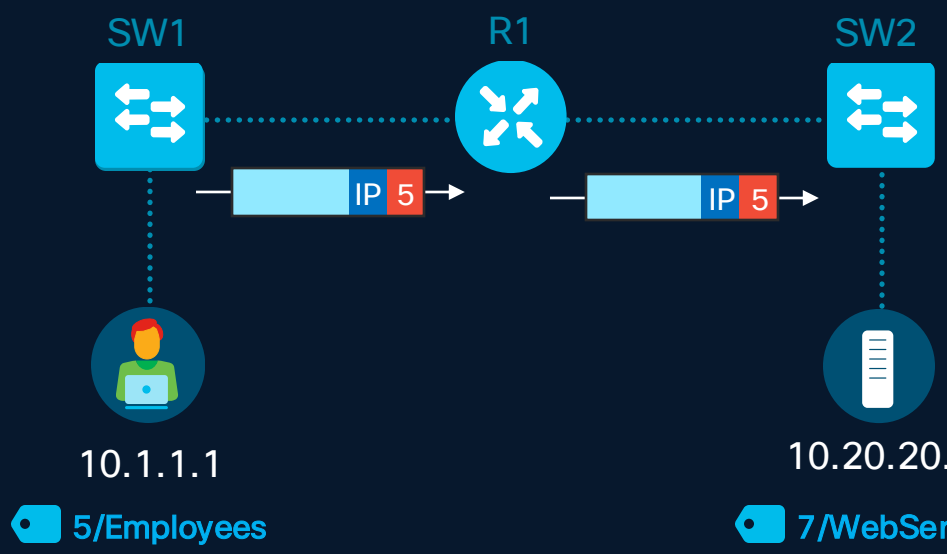


Static Classification



TrustSec Propagation

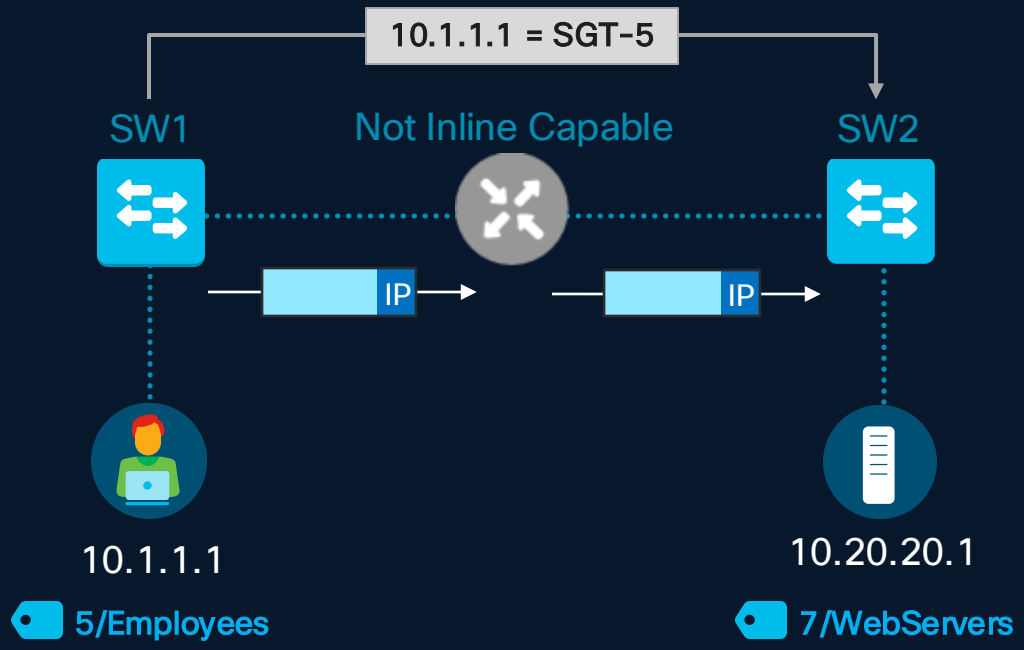
DATA PLANE PROPAGATION (INLINE TAGGING)



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

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

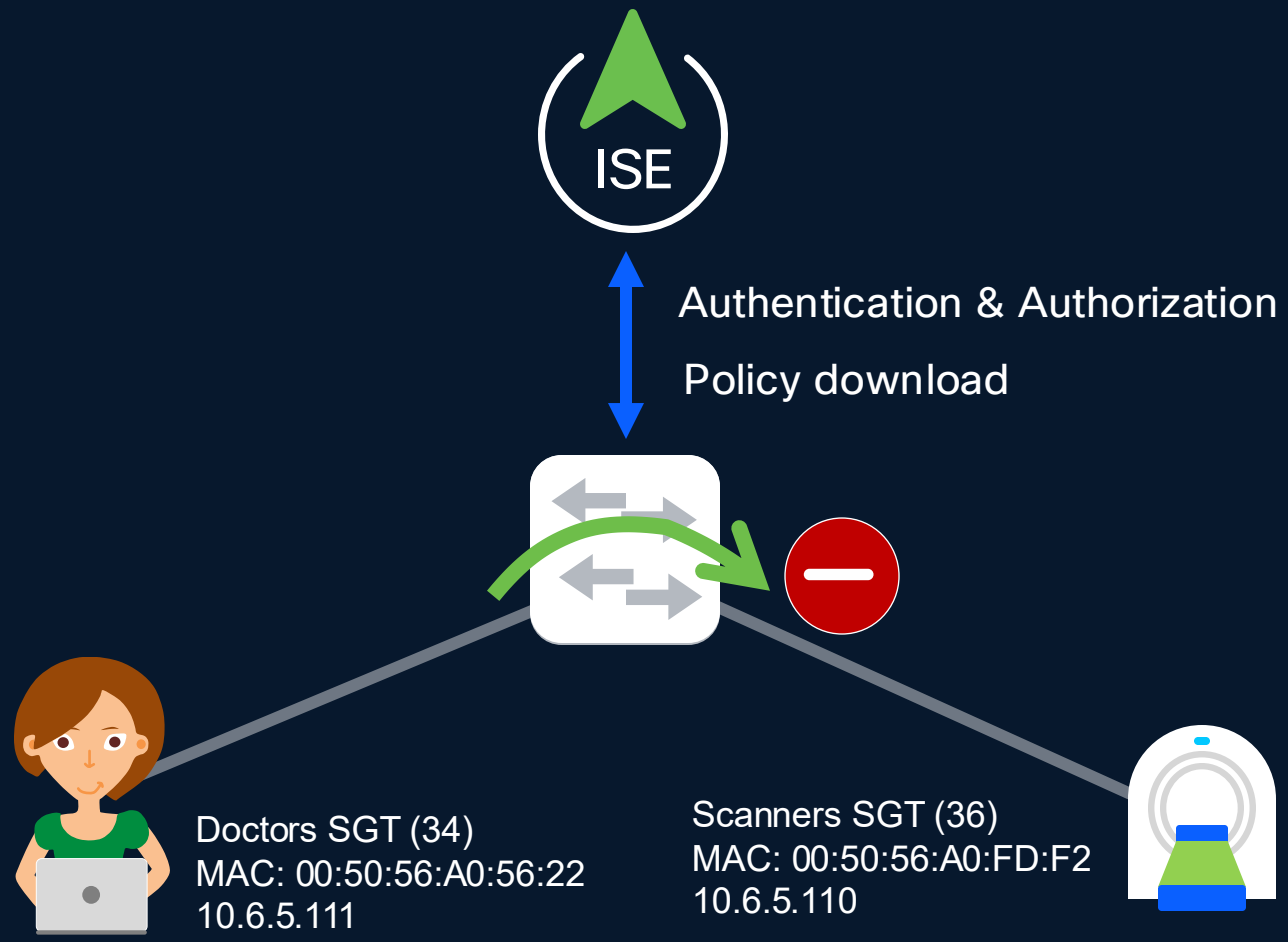
CONTROL PLANE PROPAGATION (SXP)



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

- SXP
- pxGrid

Classification, SGT Lookup and Enforcement



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

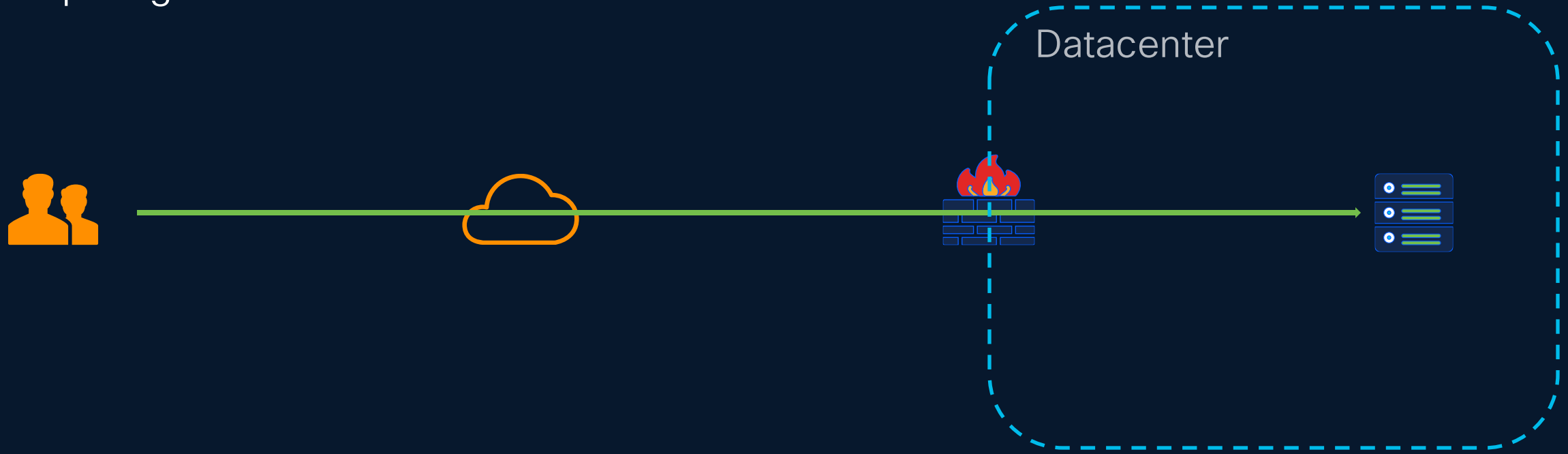
		Destination	
	Egress Policy	Doctors	Scanners
Source	Doctors	Permit All	Deny All
	Guests	Deny All	Deny All
	Scanners	Deny All	Permit All

Segmentation for Application Workloads

Securing Application Workloads – Threat Landscape

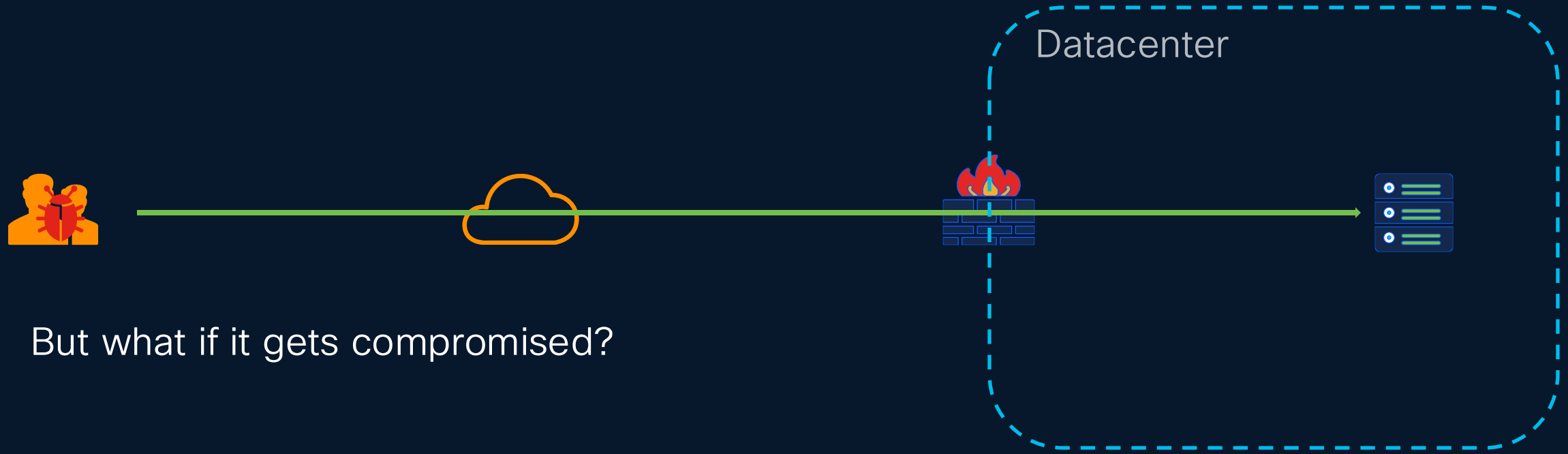
Using Network Security Controls

Simple right?



Securing Application Workloads – Threat Landscape

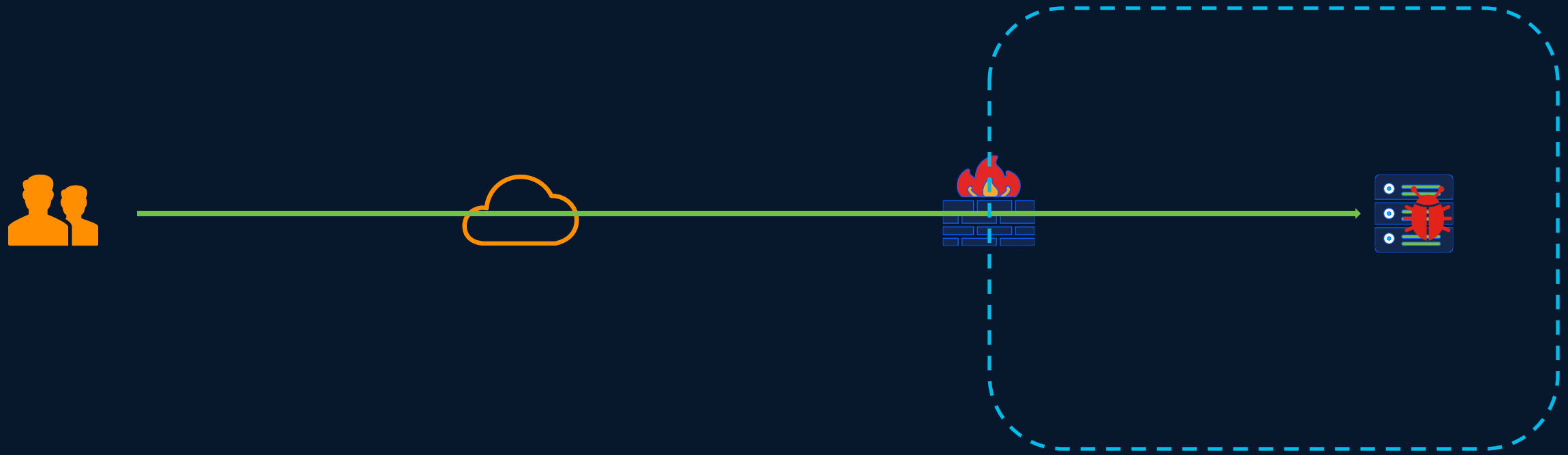
Using Network Security Controls



But what if it gets compromised?

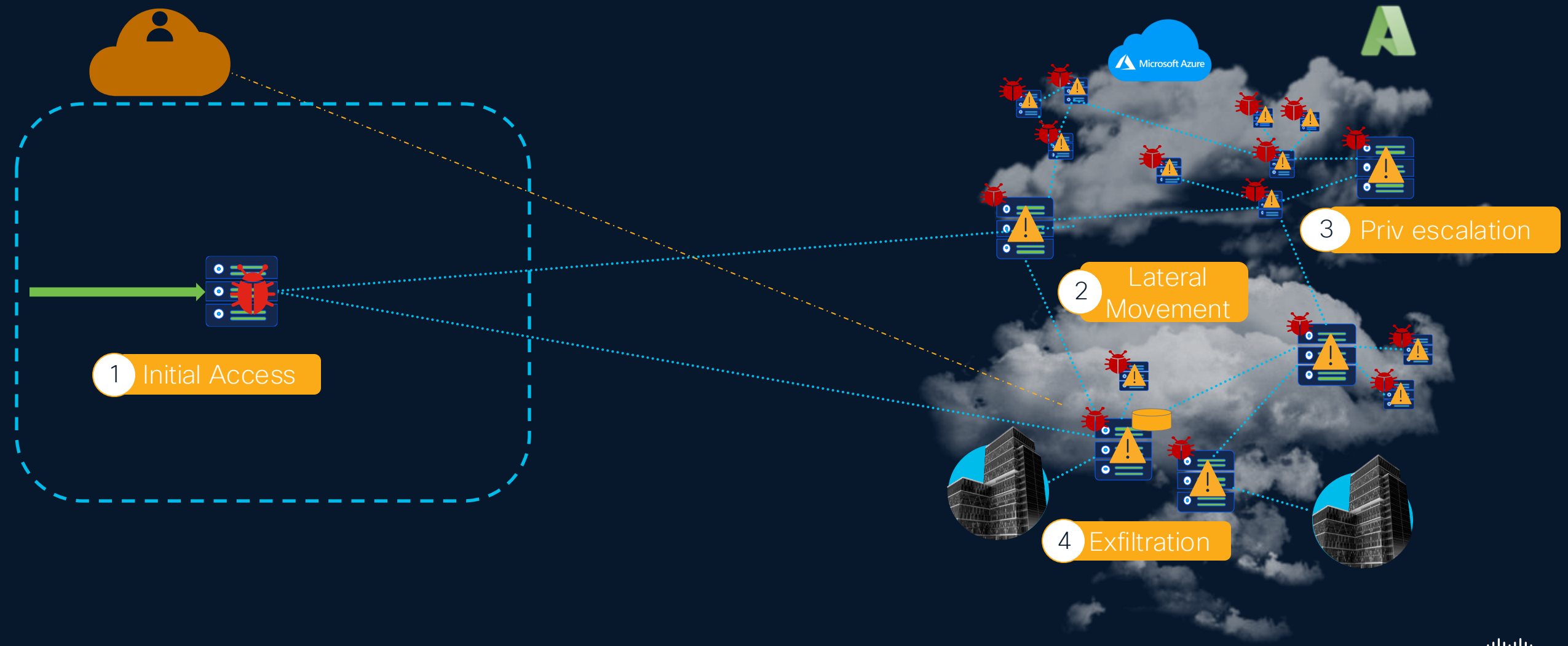
Securing Application Workloads – Threat Landscape

Using Network Security Controls



And this is only a part of the story.....

Securing Application Workloads – Threat Landscape



Segmentation and Policy Control Challenges

NetSec Admin | Server/VM Admin | Cloud Architect | DevSecOps

Organizational Challenges

Multiple teams, organizations and environments

Inconsistent islands of policy controls across environments

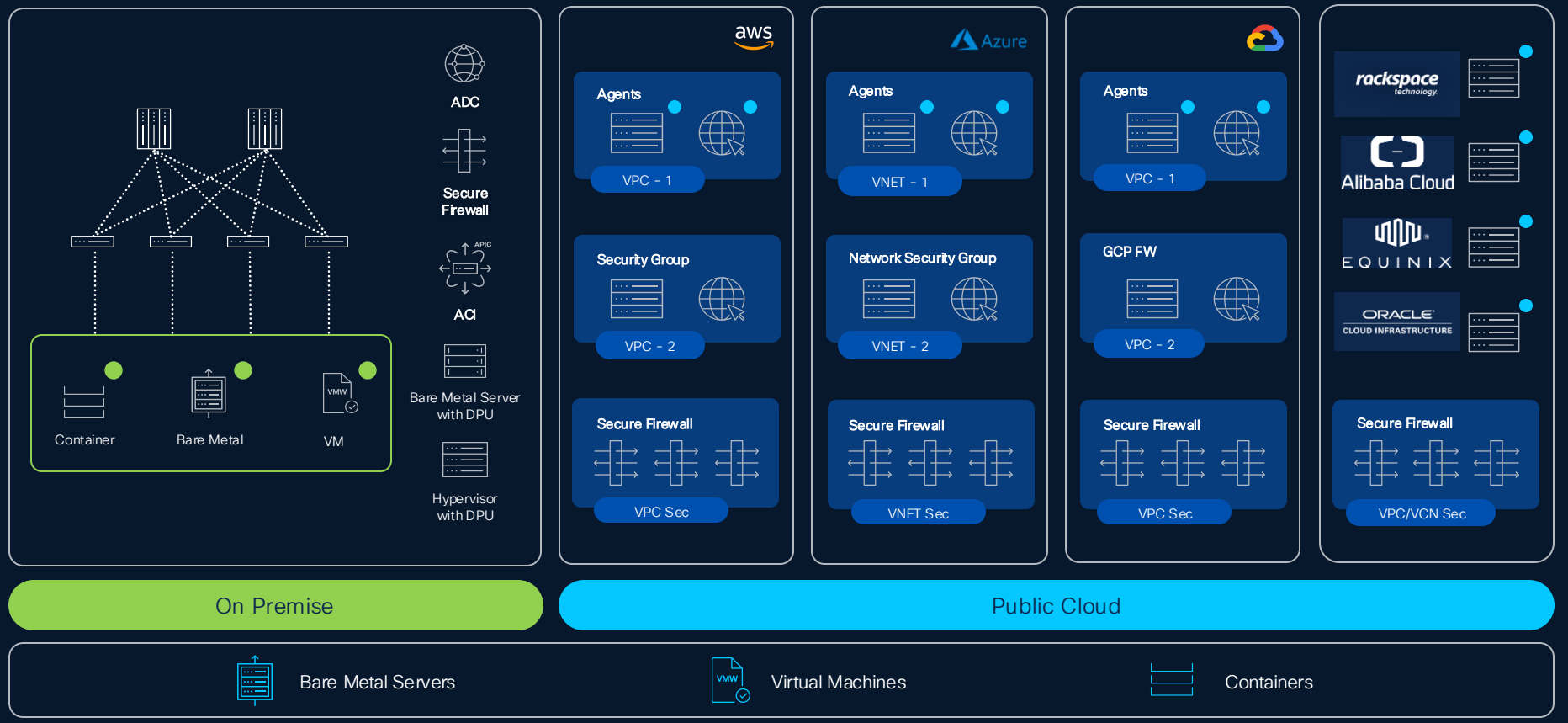
Cisco Secure Workload

Big picture for Applications

Agent

- Anywhere
- Windows Desktop
- Windows Server
- IBM AIX
- Oracle Solaris
- Oracle Linux
- Centos, Rocky, Alma Linux
- Ubuntu, Debian
- SUSE Linux
- RedHat Linux
- Amazon Linux
- OpenShift
- Kubernetes

Consistent microsegmentation from on-premises to the cloud



On Premise | Public Cloud

Bare Metal Servers | Virtual Machines | Containers

Agentless

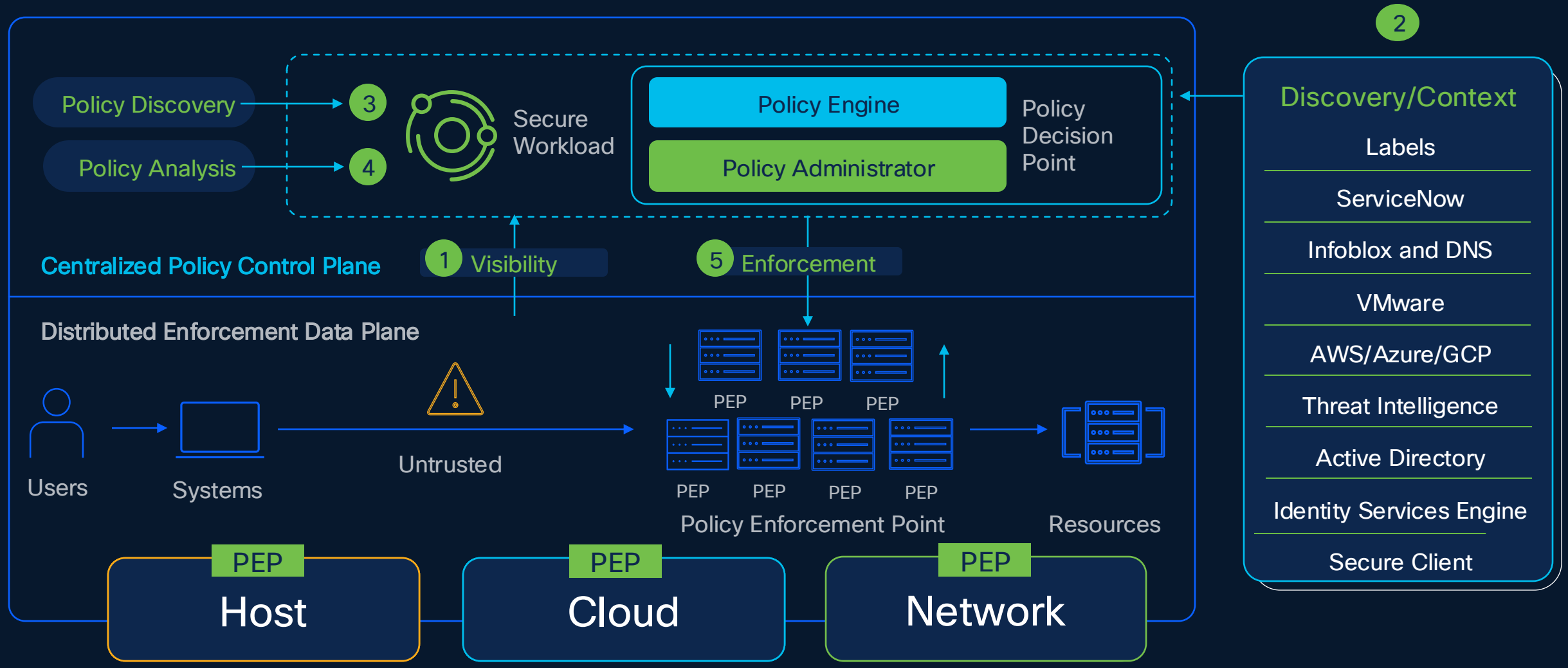
- On-Premise
- Load Balancer (ADC)
- Firewalls
- Data Center Fabric (SDN)
- NVIDIA Smart NIC (DPU)
- Public Cloud
- Security Group
- Network Security Group
- Cloud Network Firewall
- Multicloud Defense*
- NVIDIA Smart NIC (DPU)

User Identity | Tags and Labels | Vulnerability | Threat Feed | Application Encryption | Domain / FQDN | Cisco Security Risk Score

* - In Roadmap

Secure Workload

Zero Trust Segmentation

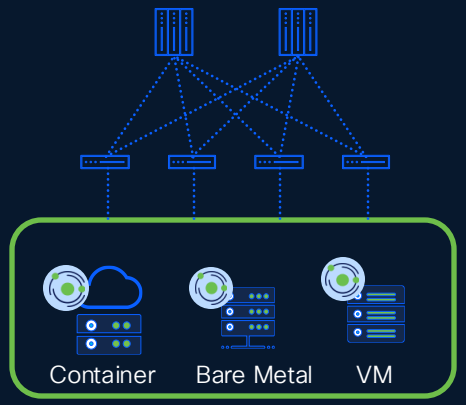


Microsegmentation Approach Evaluation

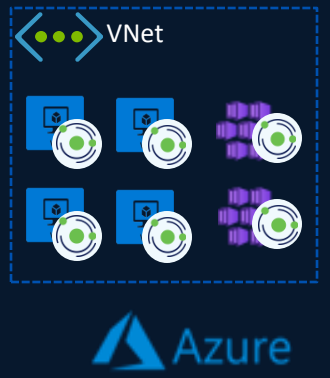
	Agent	Agentless
Pros	• Network Abstraction • In-depth visibility and protection • Flexible segmentation	• Less organizational dependencies • Leverage existing infrastructure • Faster time to deploy
Cons	• Organizational dependencies • OS dependency (legacy) • Agent fatigue	• Network/CSP infrastructure dependency • Segmentation granularity/scalability • Only network-flows visibility

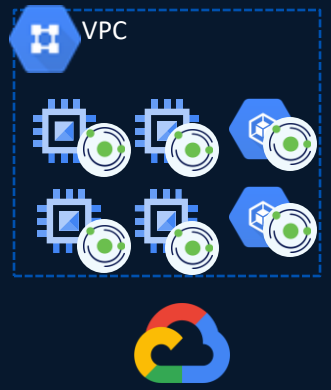
Host-Based Agent

Visibility and Enforcement



On-Prem





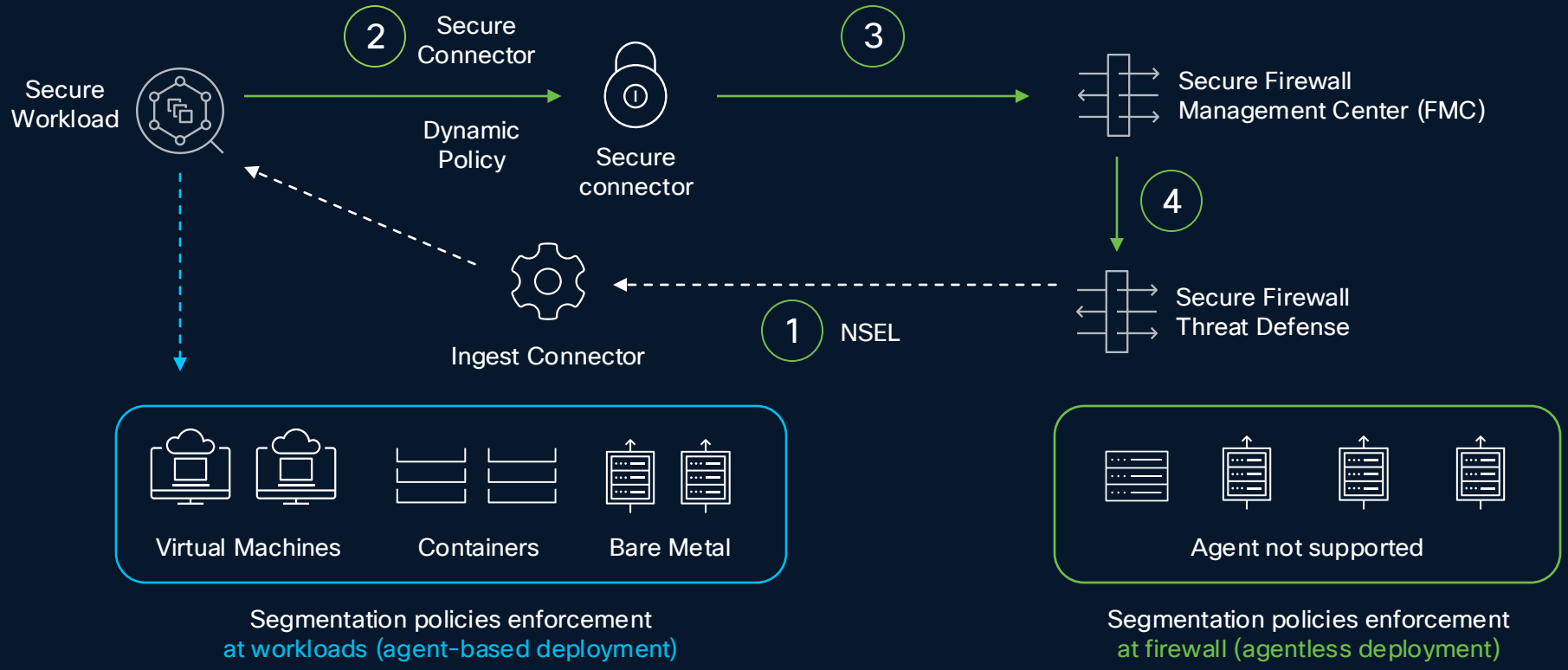
Any Location

Establish Policy Guardrails with Policies for your Application Workloads

cisco

Agentless - CSW-FMC Integration and Enforcement

Defense-in-depth use case



Benefits

- Faster time to value
- Agentless visibility & policy enforcement
- Flexible and scalable policy enforcement
- Reduce exposure to the known vulnerabilities

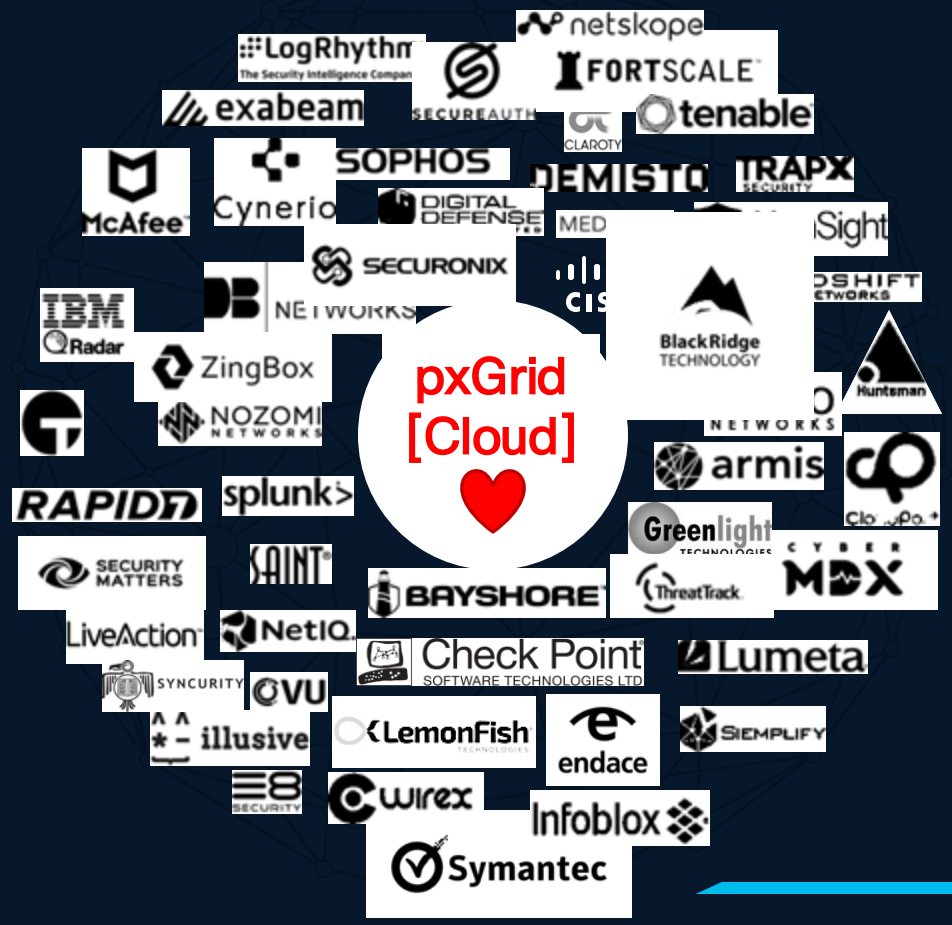
Cloud Service Provider Agentless

Protect the workloads – at the workload level!

- Centralized cloud-onboarding experience
  - Cloud connectors
  - Single point of management
- Visibility
  - Near real-time discovery of workloads and labels
  - Flow telemetry via VPC/VNets flow-logs
- Enforcement
  - Security Groups (AWS)
  - Network Security Groups (Azure)
  - Firewall (GCP)

Integrations

The Power of Integration With Operational Simplicity



More Cross-Team Use Cases Simplified with Visibility and Automation

Cisco Security

- Network
- Applications
- Endpoint
- Cloud

More Integrated Products Across Partner Ecosystem and Beyond

Your infrastructure

- 3rd Party/ITSM
- Intelligence
- Identity
- SIEM/SOAR

Power of pxGrid Integration

Enabling a platform approach into the Cloud

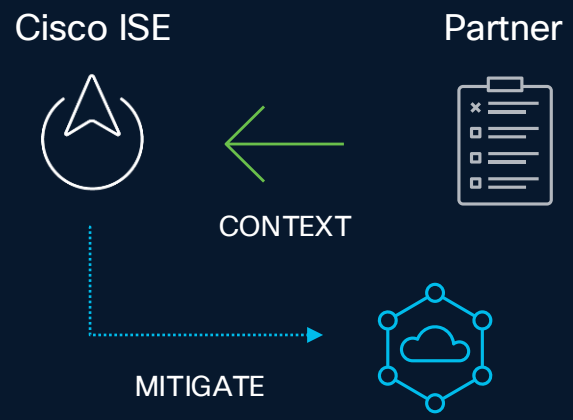
ISE Context OUT

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

ISE Context IN

Enrich ISE context. Make ISE a better Policy Enforcement Platform

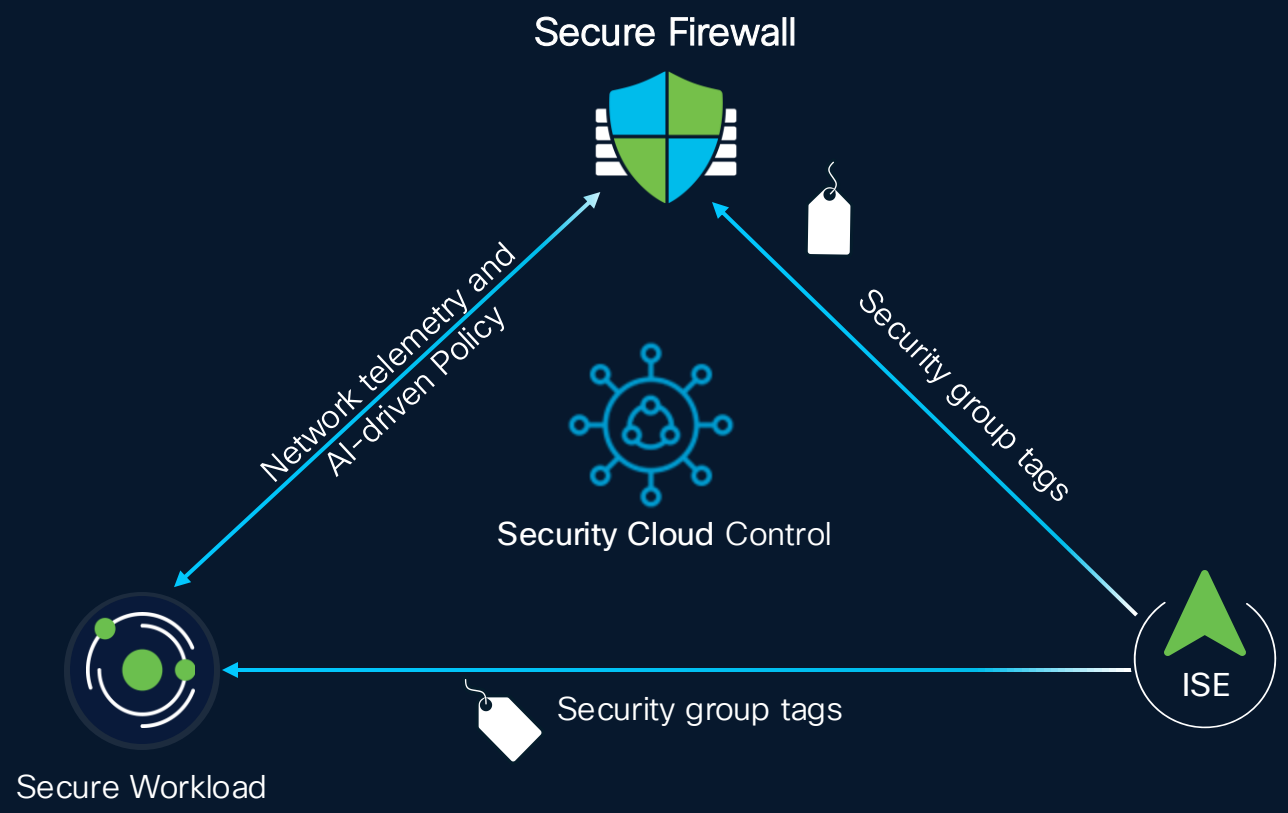
Rapid Threat Containment



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

Share Identity to Apply Consistent Policies

Native integration

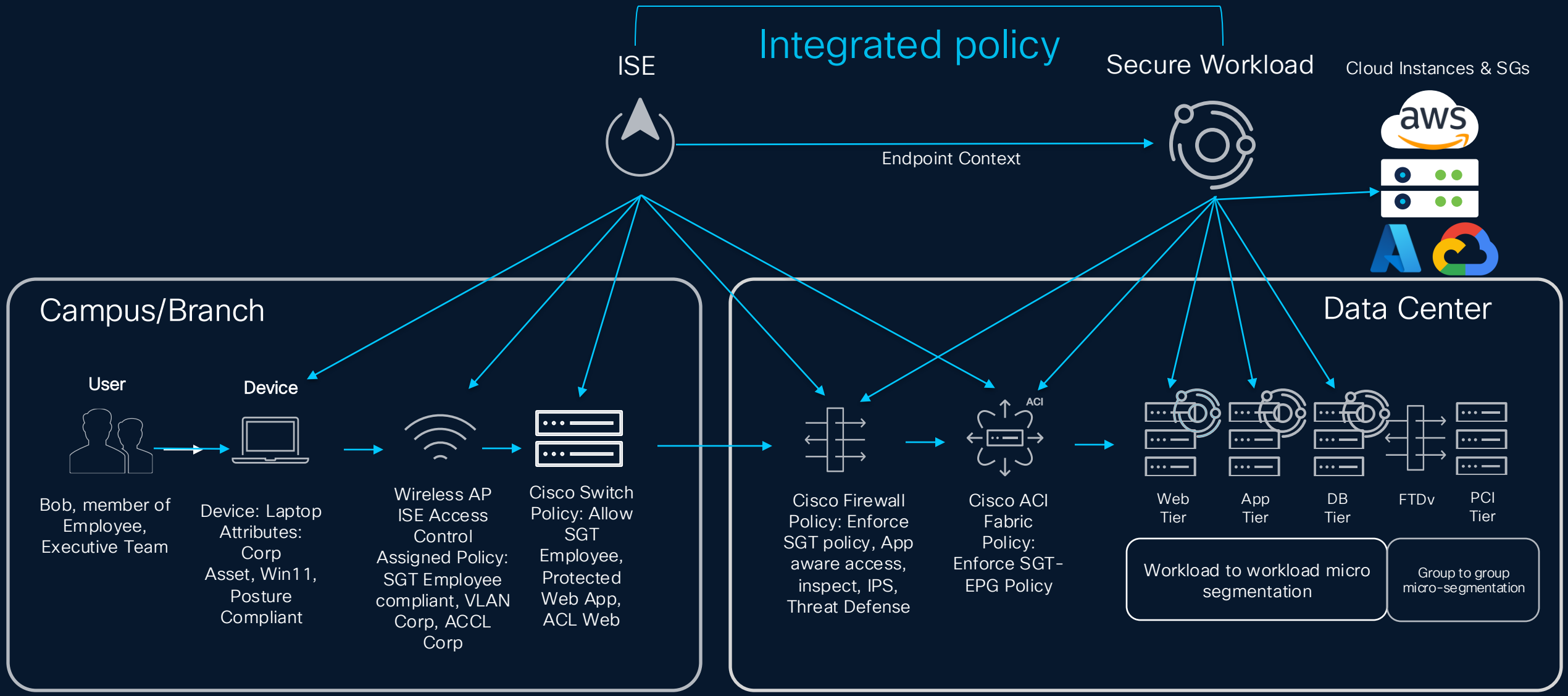


User based policy using ISE tags inline

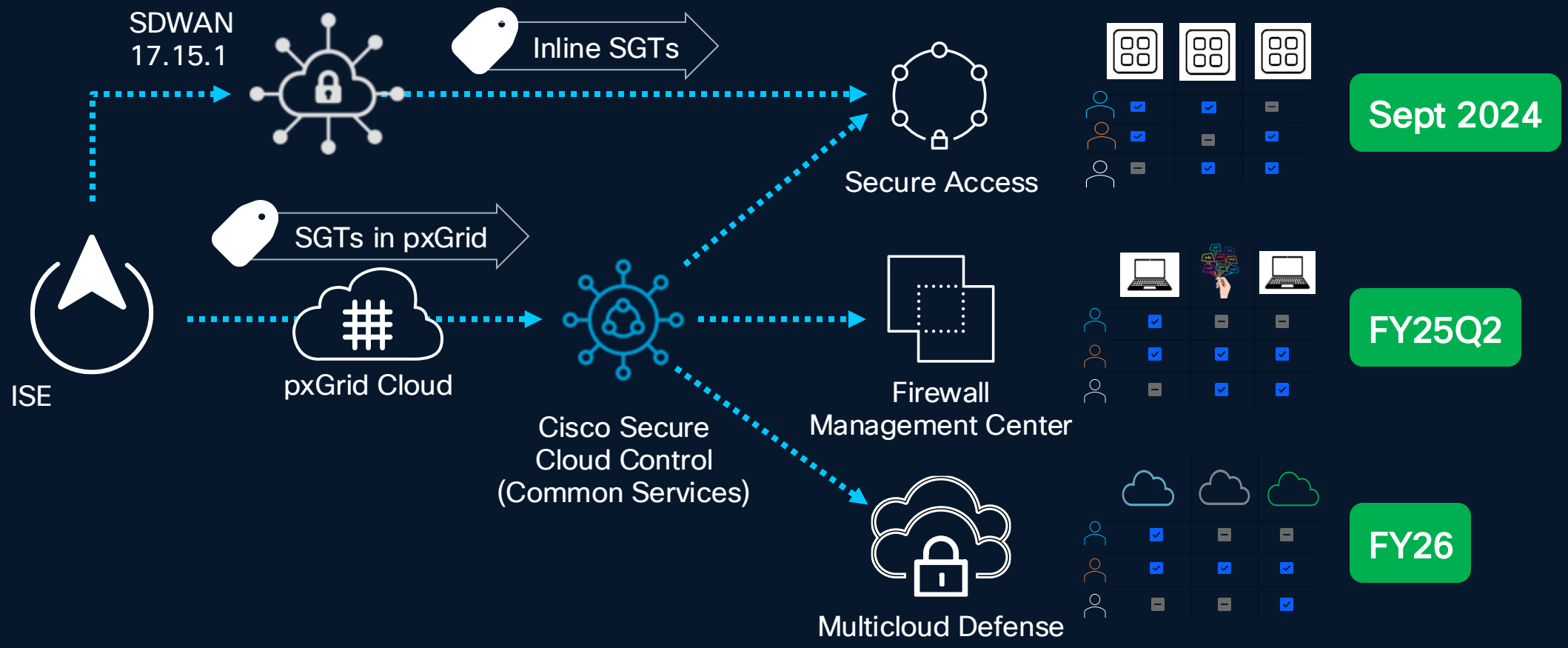
ML powered policy discovery

Policies evolve as users and apps change

Cisco's Zero Trust Segmentation Strategy

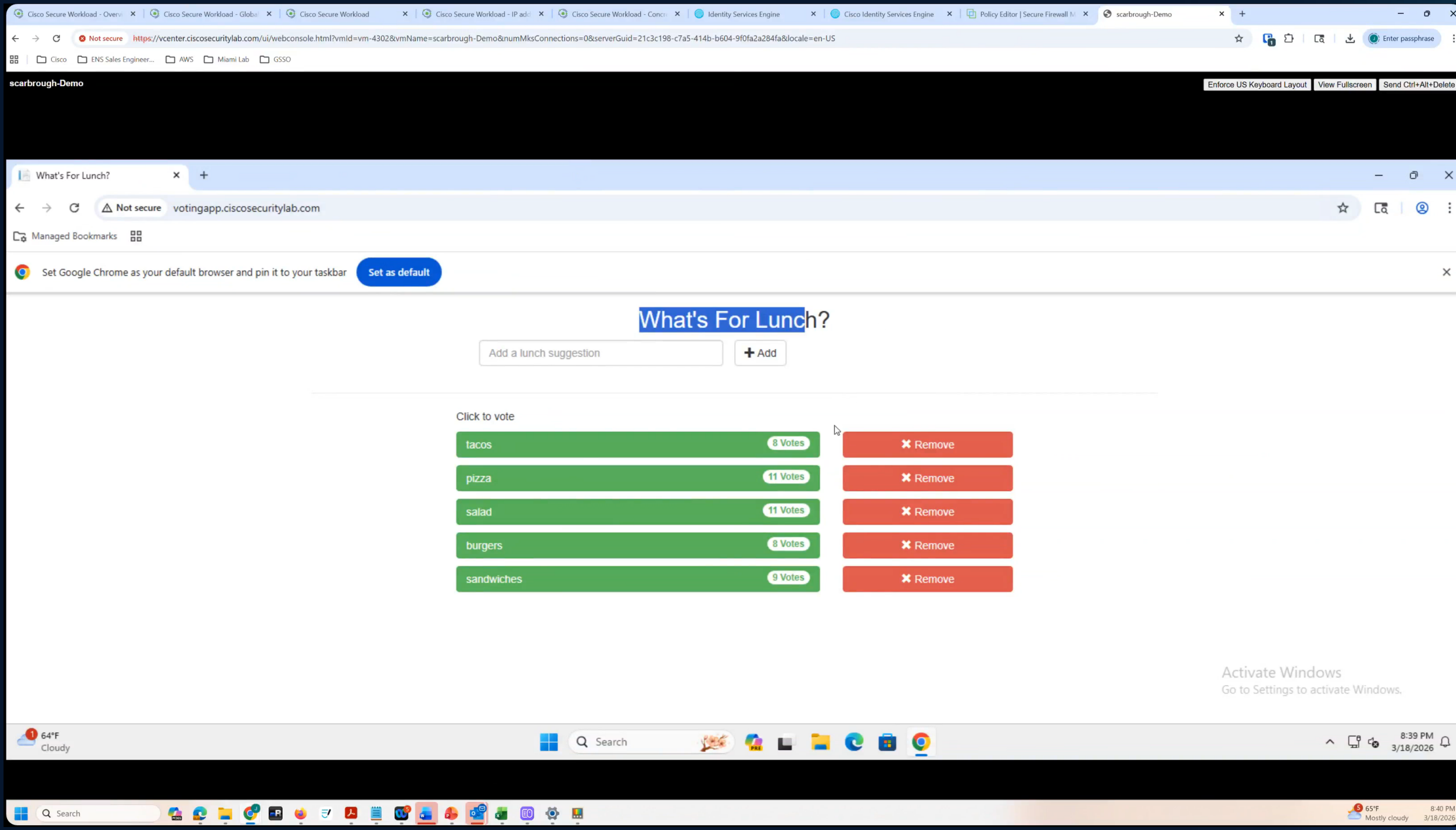


Context for Cisco Security Cloud Services



Security Group Tags (SGTs) are the common language used across campus, remote, cloud, and firewall policies

Demo


scarbrough-Demo
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
What's For Lunch?
Not secure
votingapp.ciscosecuritylab.com
Managed Bookmarks
Set Google Chrome as your default browser and pin it to your taskbar
Set as default
What's For Lunch?
Add a lunch suggestion
+ Add
Click to vote
tacos 8 Votes
pizza 11 Votes
salad 11 Votes
burgers 8 Votes
sandwiches 9 Votes
✖ Remove
Activate Windows
Go to Settings to activate Windows.
64°F
Cloudy
Search
8:39 PM
3/18/2026
65°F
Mostly cloudy
8:40 PM
3/18/2026

CISCO Connect

Thank you