
cisco Live!
Let's go
#CiscoLive

The bridge to possible

Who Ate My Packet

Challenges in Policy Management Across Domains

Jeremy Bowman - Solution Architect
Zaheer Aziz - Principal Architect

BRKXAR-3000

cisco Live!

Cisco Webex App

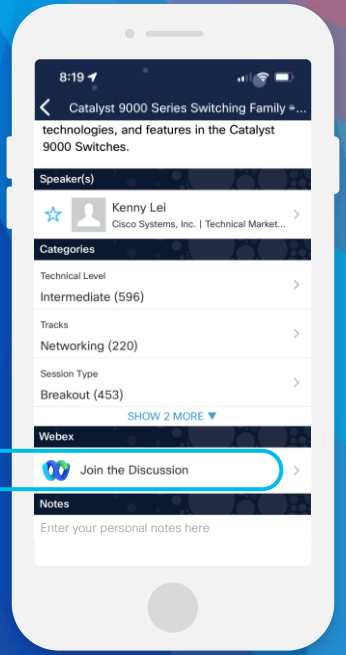
Questions?

Use Cisco Webex App to chat
with the speaker after the session

How

1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until June 9, 2023.



https://ciscolive.ciscoevents.com/ciscolivebot/#BRKXAR-3000

Who are we?

Jeremy Bowman

Sr. Delivery Architect

Cisco CX

8+ Years @ Cisco

CCIE #51241 (R/S, Security)

CCDE #2018::16

Specialized in: Full Enterprise IBN with Security and Automation

@ibnsrevenge

jdb1@cisco.com

Zaheer Aziz – Principal Architect

25 Years @Cisco
2 Books
7-Patents
CCIE #4217

2017-Current	· Cisco SASE/SDWAN – Principal Architect
2015-2017	• Viptela – SDWAN Office of CTO • Incubated Professional Services
1997 To 2015 (Cisco)	

Acquired by Cisco

- TAC – Routing
- PS (NCE) – MPLS Design
- Marketing (TME) – MPLS Solution/Competitive Analysis
- PS (Lead) – Collaboration; Telepresence Exchange
- PS (Mgr) – SP Cloud Video; Service Incubation (Private Video Cloud)
- IoT – Manufacturing Lead

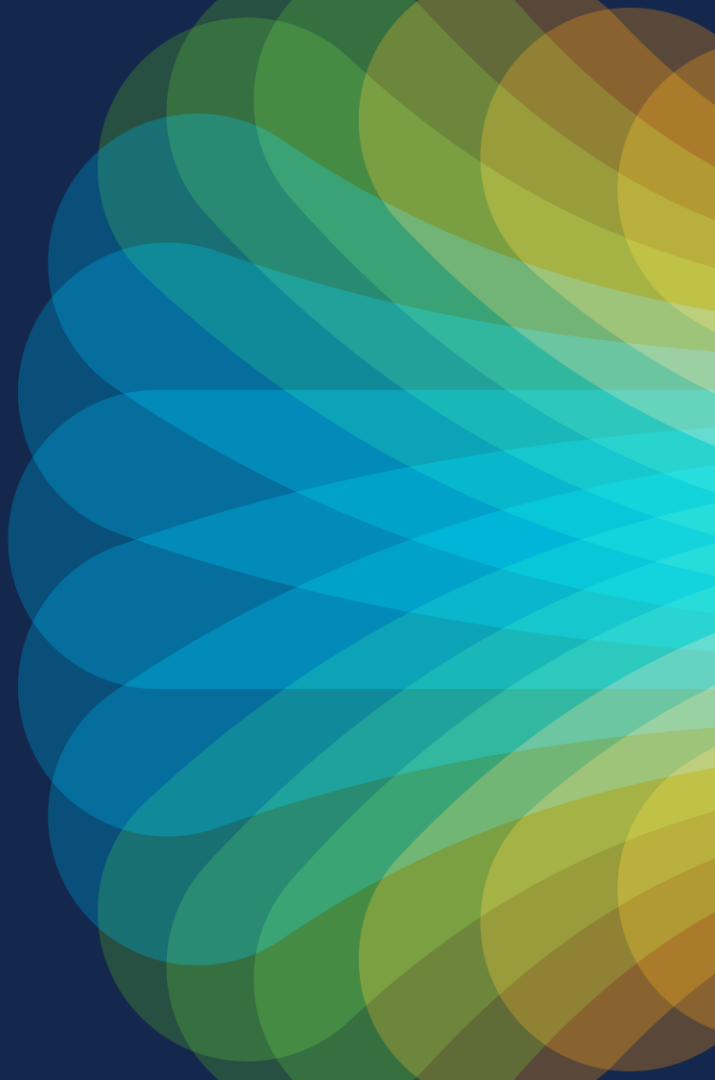
Enjoys
Ping Pong
Cricket
Reading

PS – Professional Services

Agenda

- Why are we here?
- A thing called “policy”
- Examples of policies
- Life of a packet
- Software Defined “policy” driven architectures
- What to do?
- Key takeaways

What This is NOT



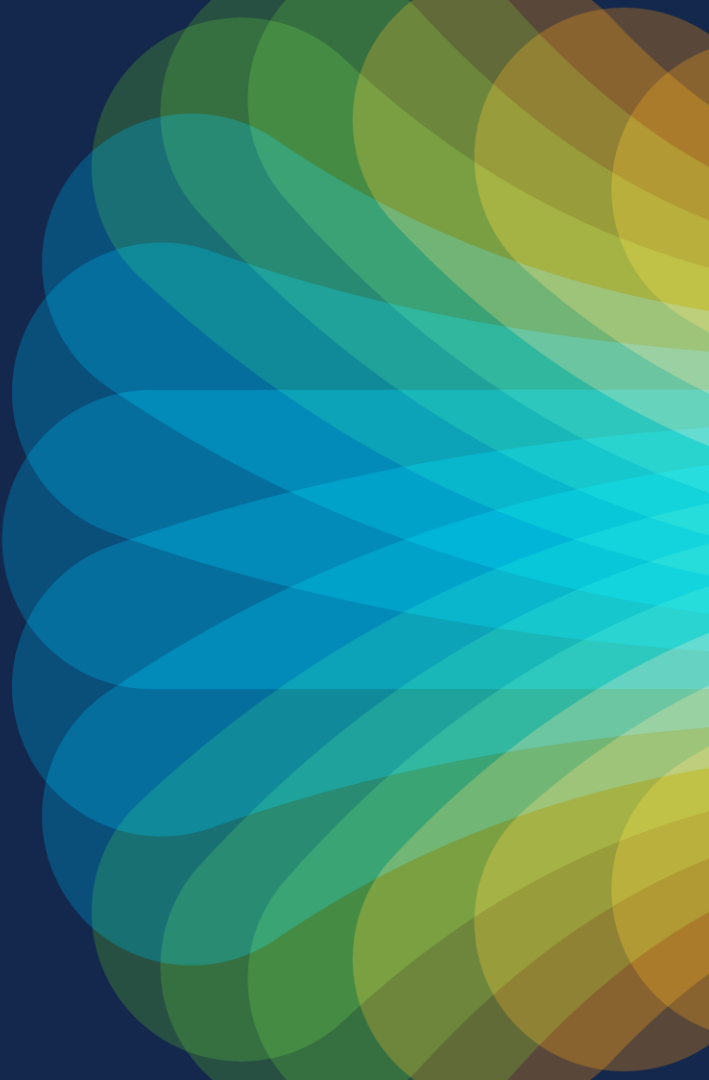
This Session is Not about

1. ACL – Access Control List
2. QoS – Queuing, Shapers, Policers
3. MTTI – Mean Time to Innocence
4. Product Recommendations

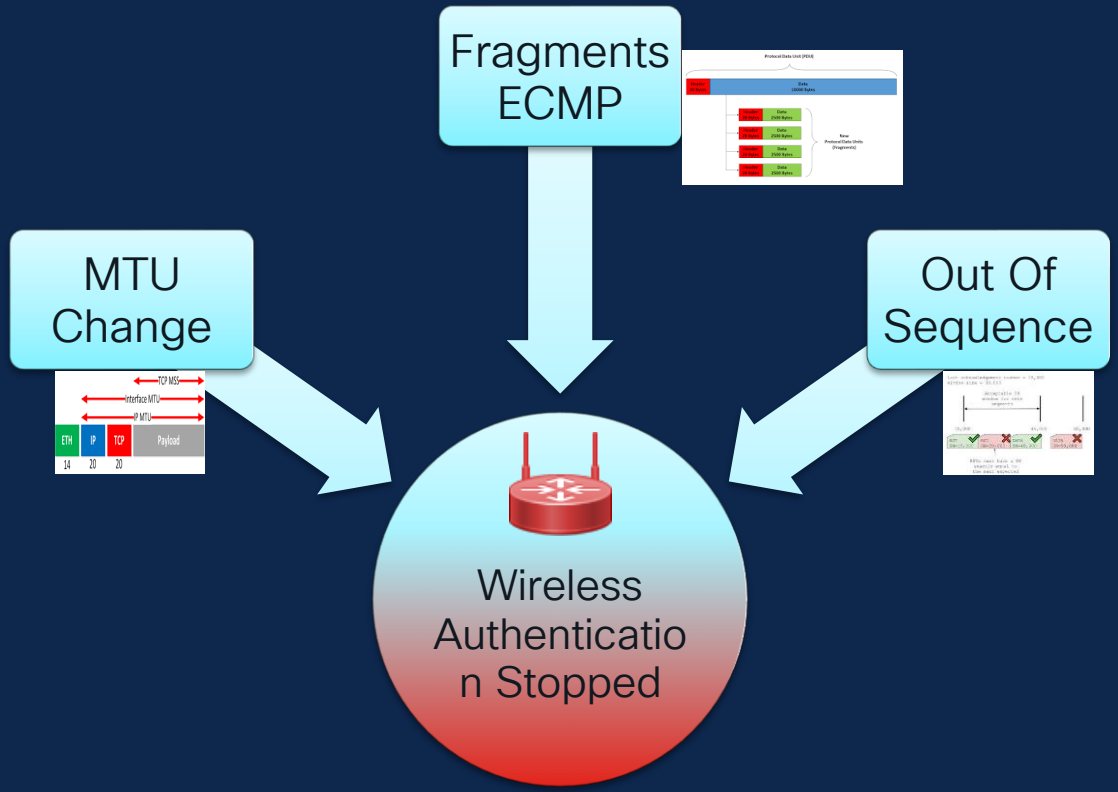
Go Ahead - Blame The Network

Why are we here?

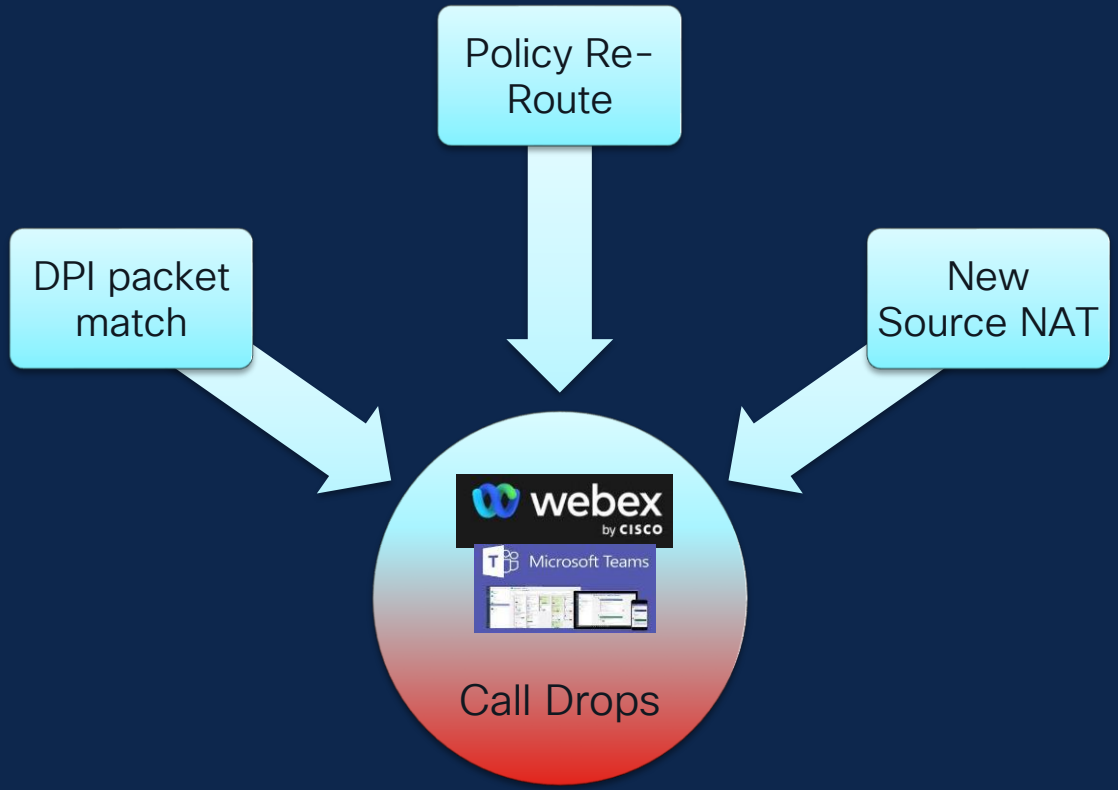
You were “in-charge” when
Monday Morning Blues happened



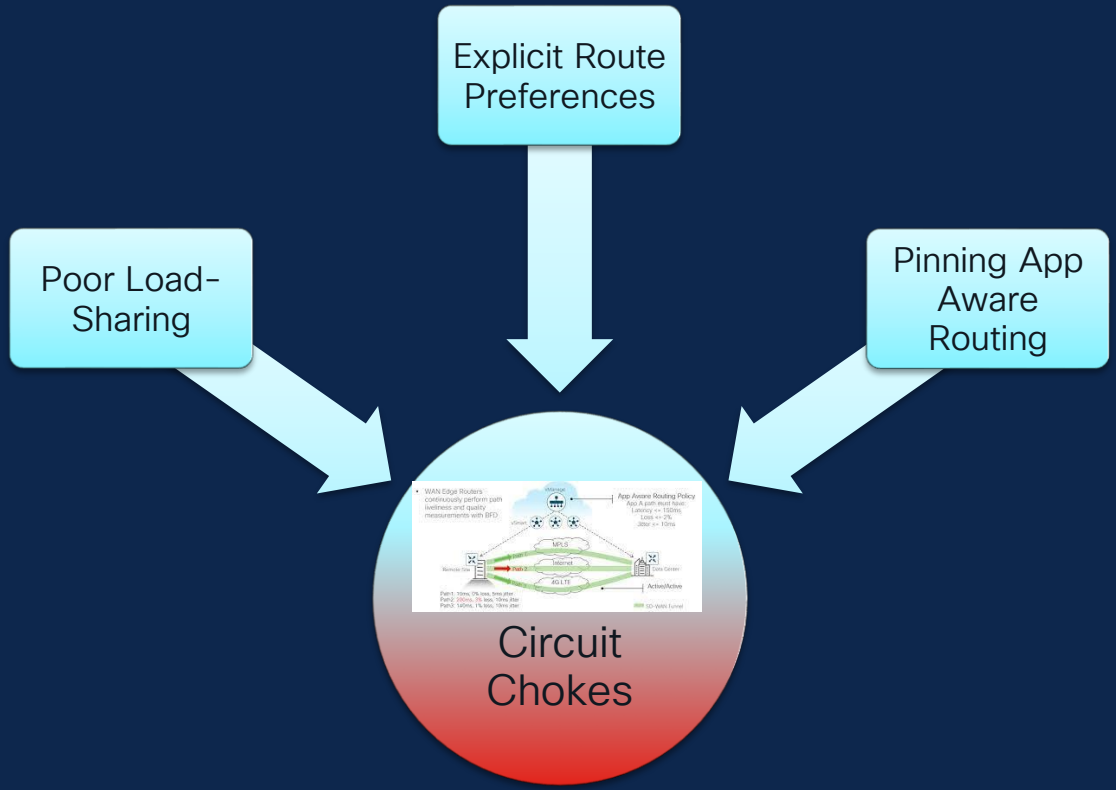
1. Wireless authentication started failing



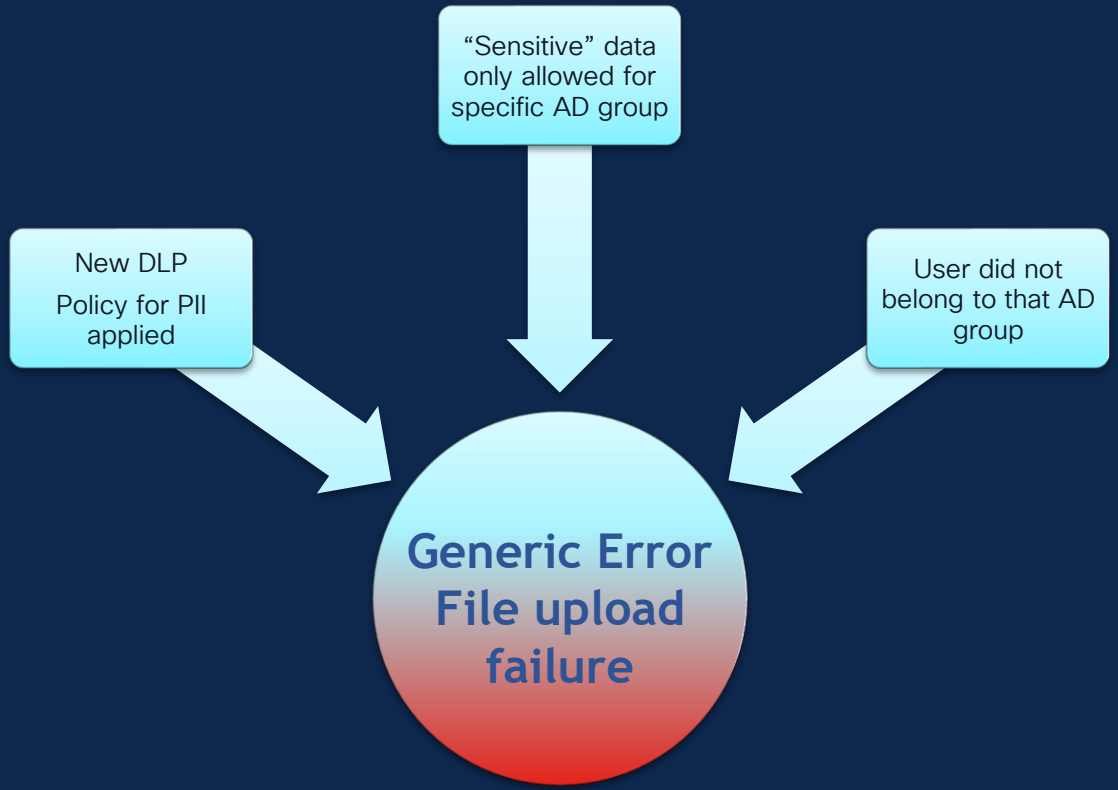
2. Cloud Hosted Apps seeing Resets



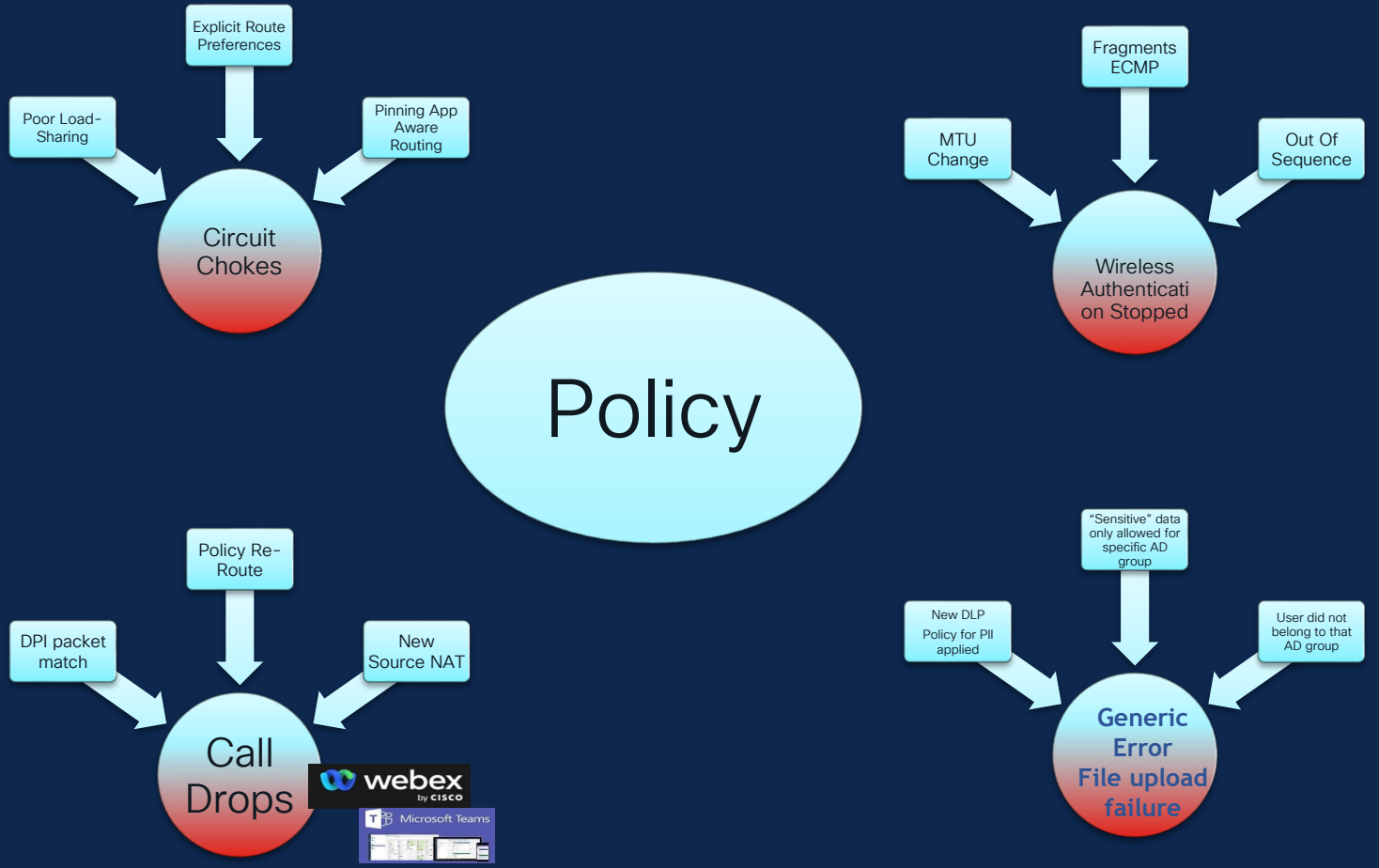
3. Choking one or more circuits while rest of the circuits sipping coffee.



4. Cloud Security: Document upload failure impacting daily business.

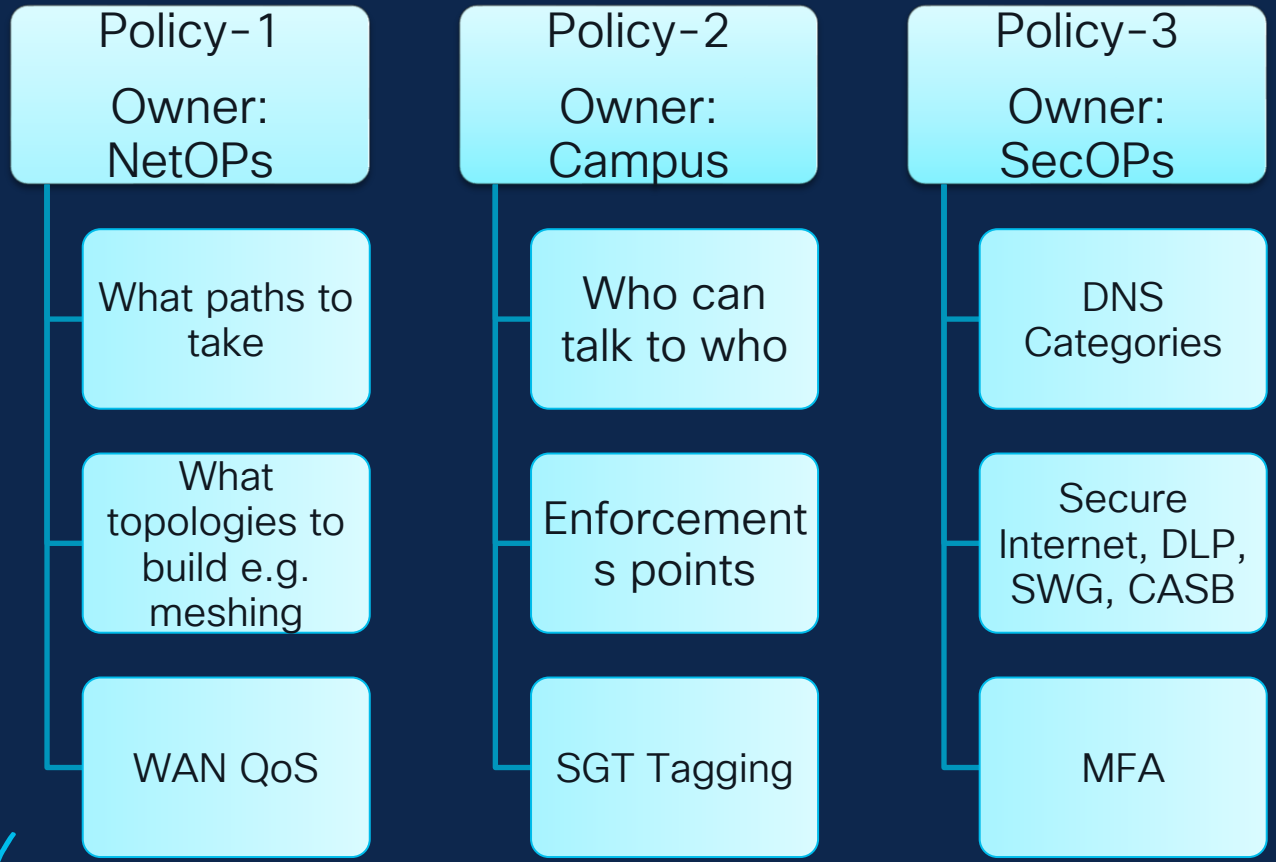


A thing called “policy”



Who Owns The Policy That Ate My Packet

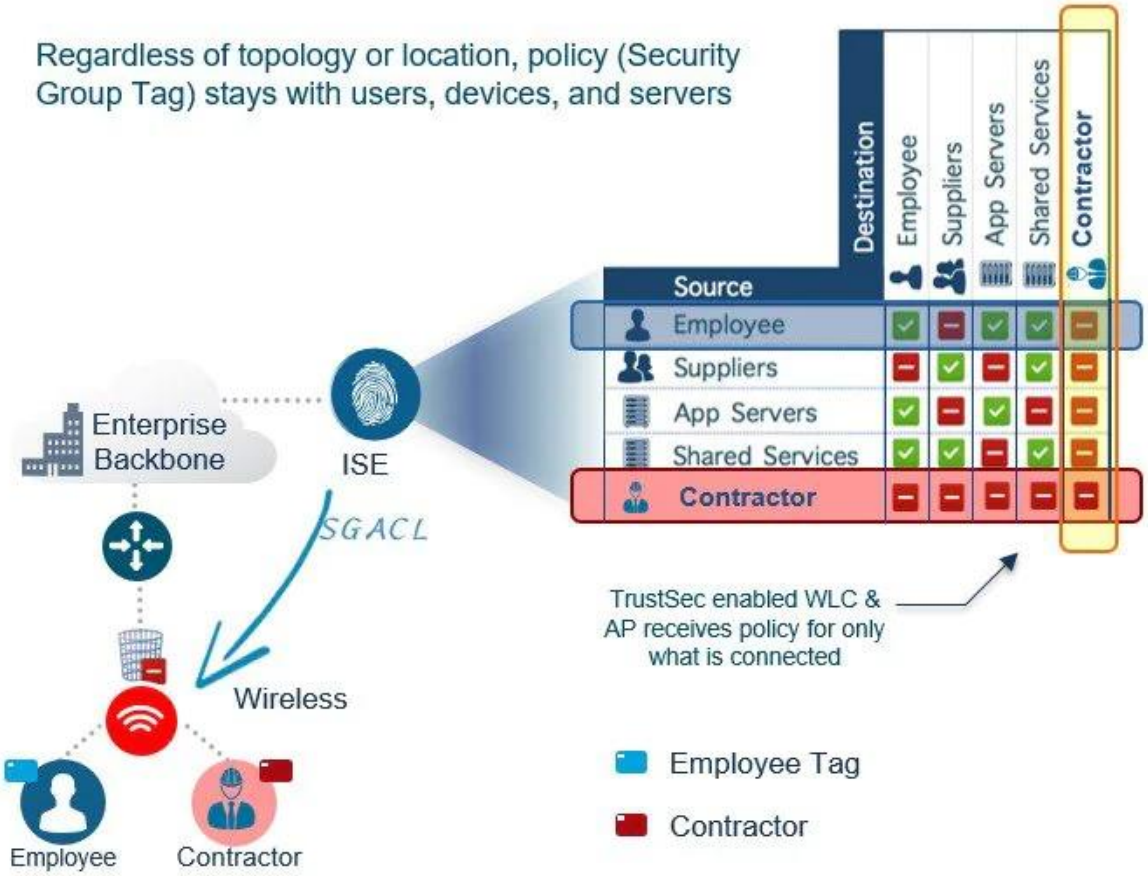
Policy Governance



“Policy” Examples

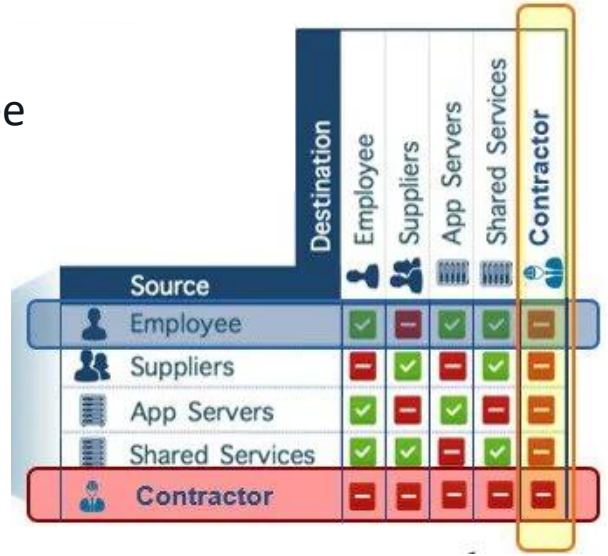
Policy Examples – TrustSec

Regardless of topology or location, policy (Security Group Tag) stays with users, devices, and servers



Policy Examples – TrustSec Visibility

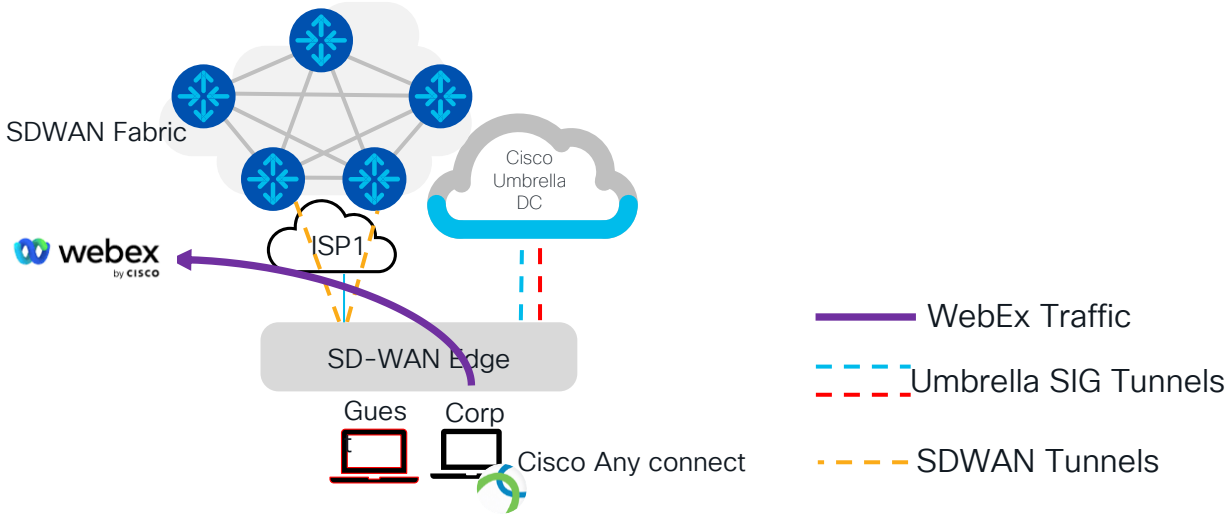
- show cts security-groups | include Contractor|Employee
- show cts role-based sgt-map <Contractor-IP>
- show cts role-based sgt-map <Employee-IP>
- show cts role-based permissions from <A> to <B>



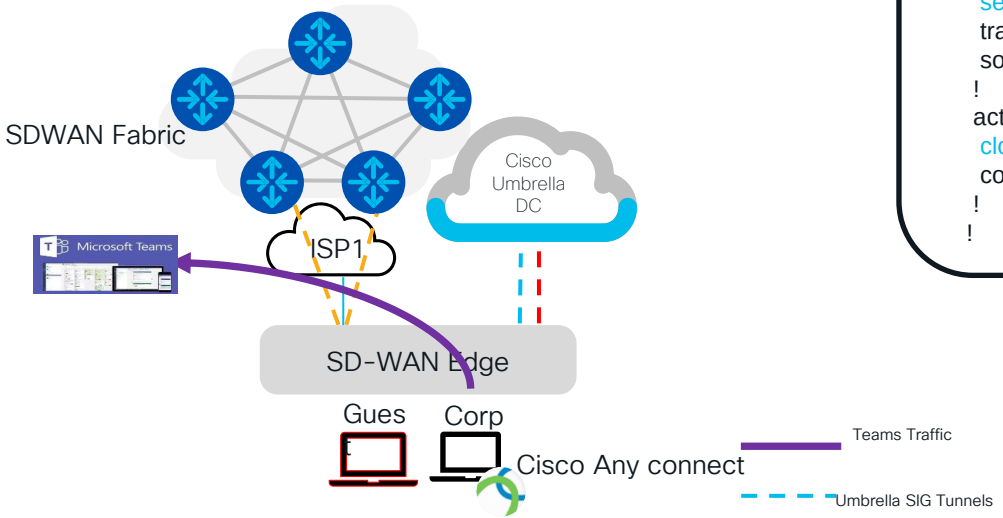
IPv4 Role-based permissions from group 4:Employees to group 5:Contractors:
DenyAll

Policy SD-WAN: Local Breakout of WebEx

Intent	Benefit	Decision	Method Used
1-Application Routing WebEx	Improve Latency. Reduce tunnel bandwidth	Local-Breakout	Data Policy – SD-AVC (App Visibility and Control)



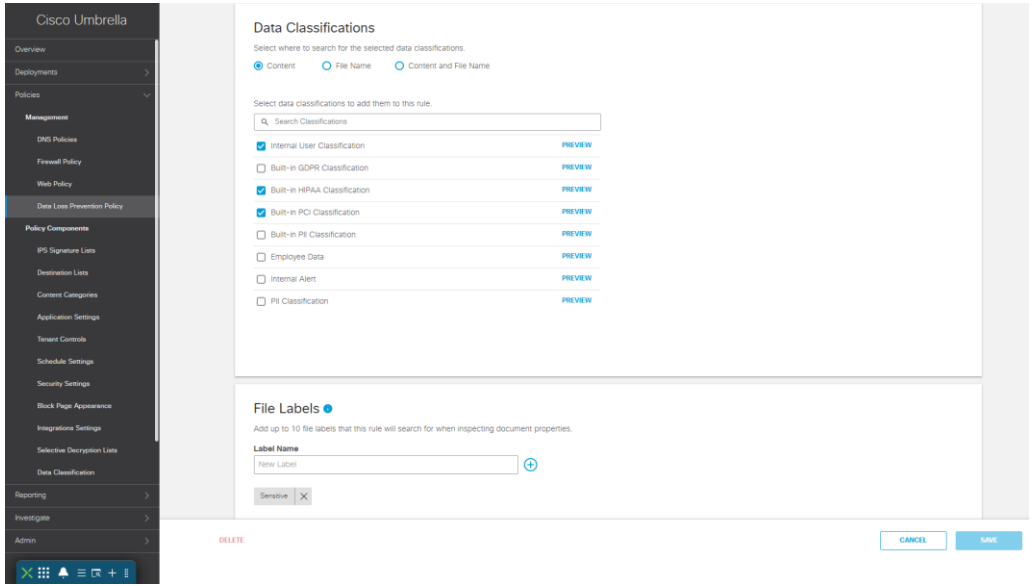
SD-WAN Local-BreakOut




```
app-route-policy _Corp-VPN_Cloud-AAR-Policy
 vpn-list Corp-VPN
  sequence 1
   match
    service-area exchange sharepoint common
    traffic-category optimize-allow
    source-ip 0.0.0.0/0
   !
   action
    cloud-saas
    count service_area_ctr_1602310673
   !
  !
```

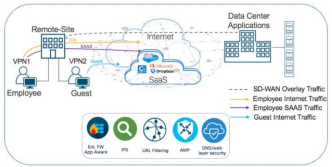
Cloud Security Policy: DLP Data Loss Prevention

Prohibits uploads of documents labeled "Sensitive“
to any SaaS destination, except for members of a certain AD Group.

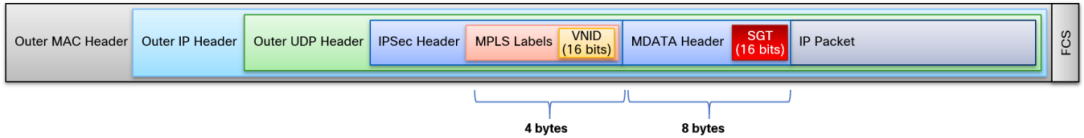


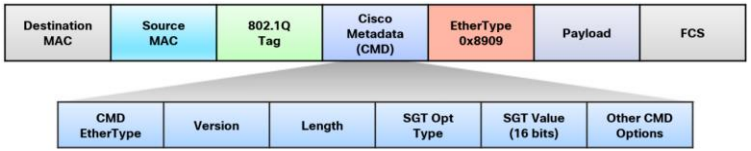
Life of a packet

Life of a Packet

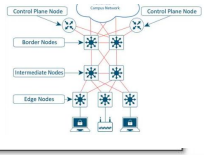


SDWAN

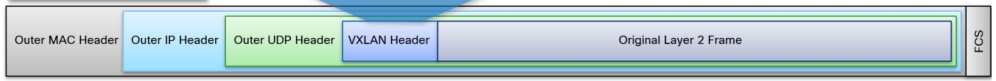




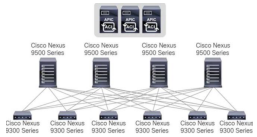
Ethernet
802.1q



SDA

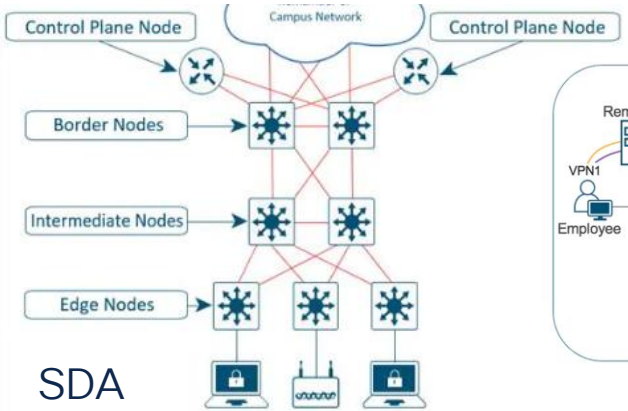


ACI

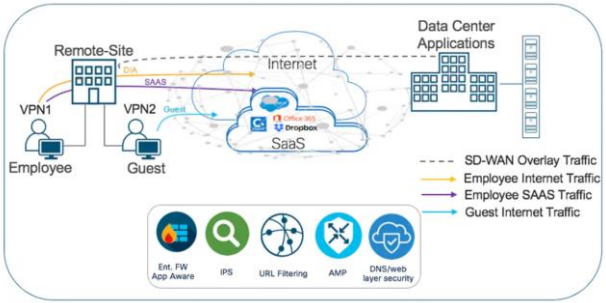


Software Defined “Policy” Architectures

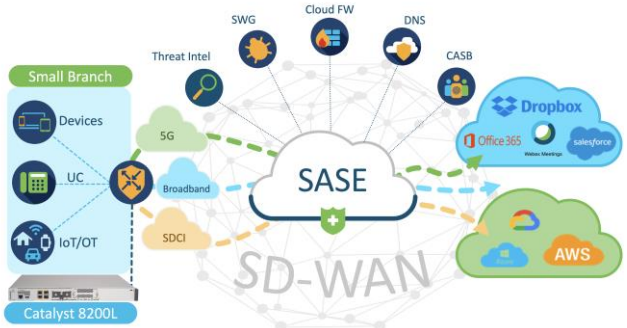
Policy Defined Architectures



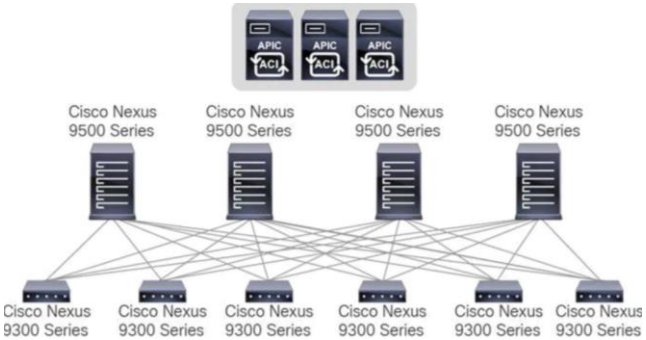
SDA



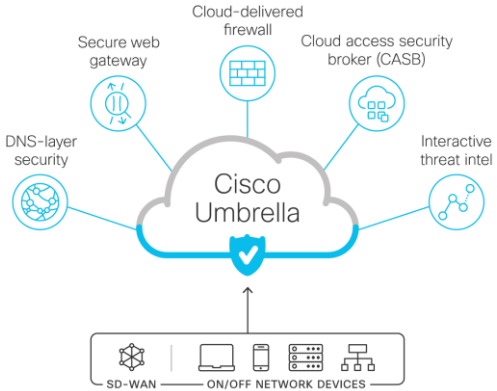
SDWAN



Cloud



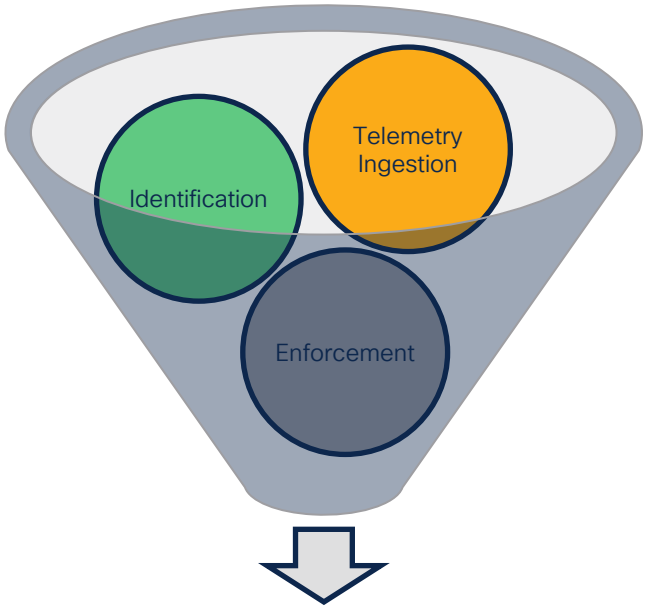
ACI



Umbrella

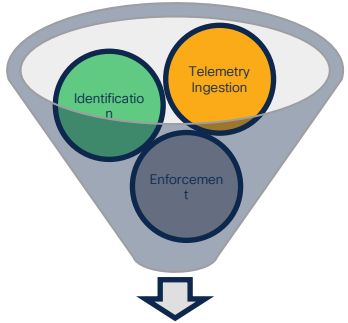
What to Do?

What To Do?



Multi-Domain Policy

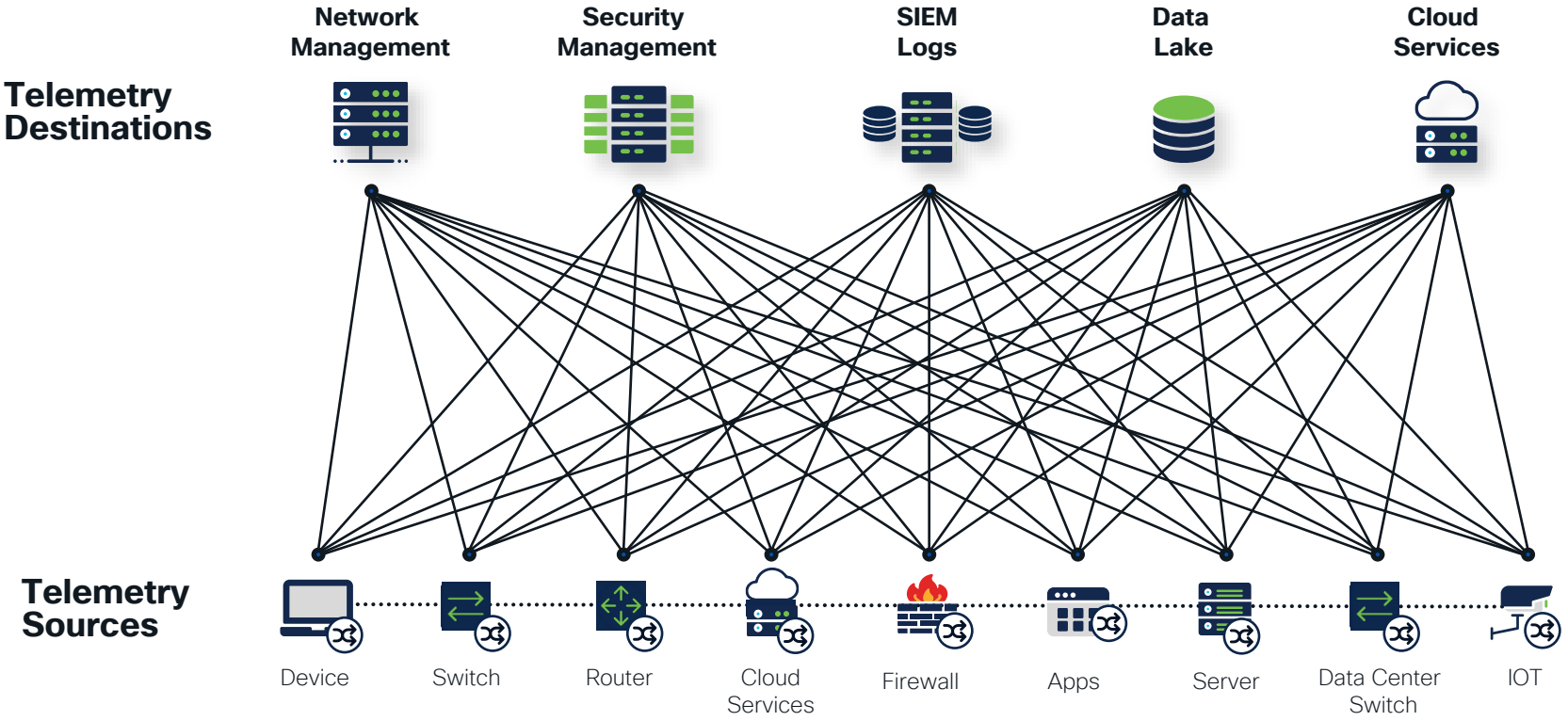
1- Telemetry Ingestion



1- “Periodic” for Trending and Reporting

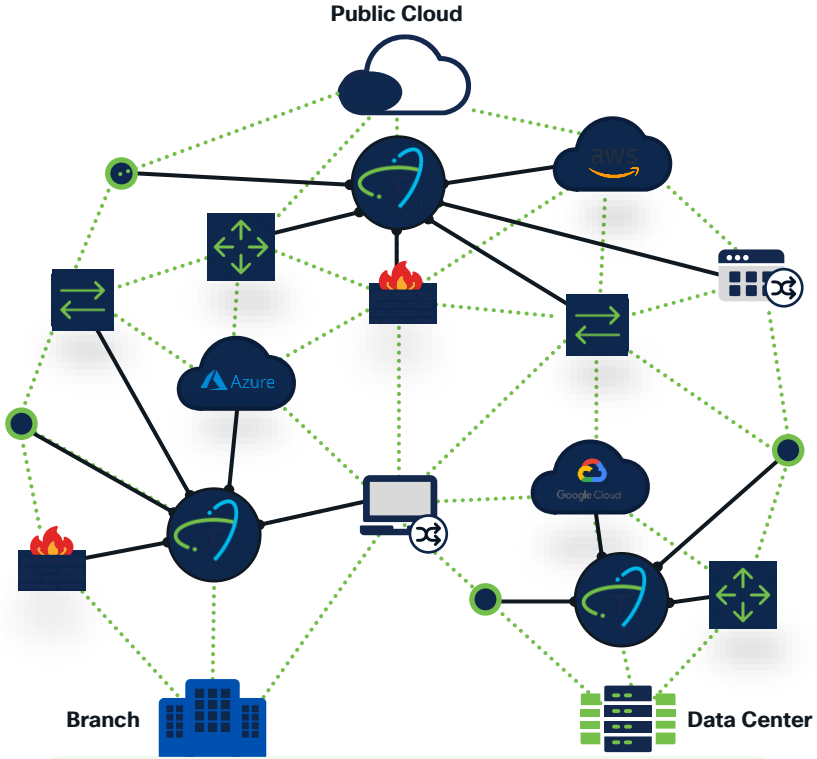
2- “Near Real Time” for troubleshooting

Telemetry Streams



Telemetry Broker

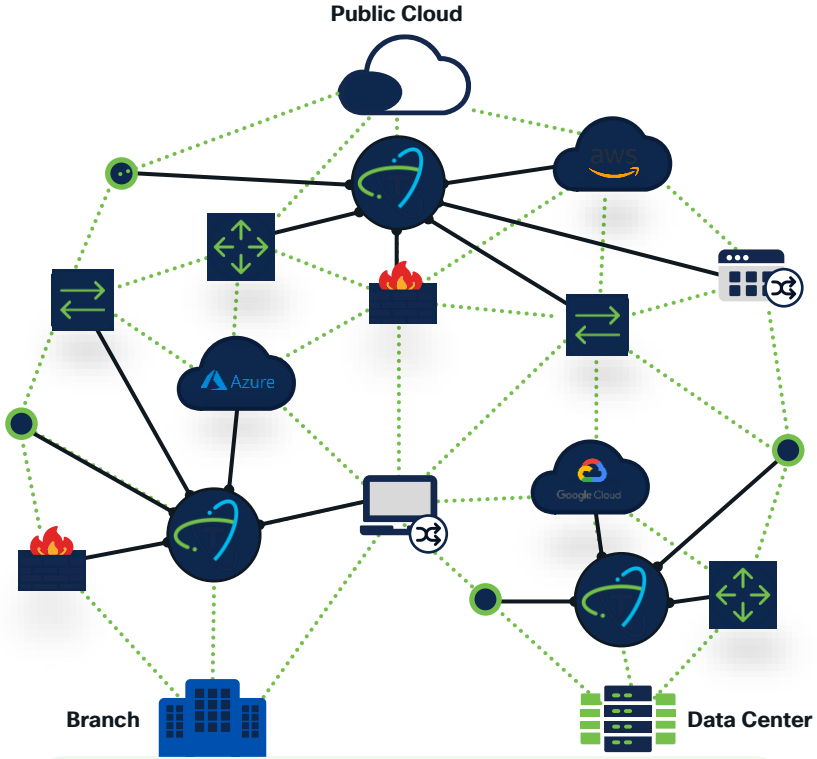
Provides Full Visibility to On-Prem and Cloud Telemetry



Omni Cloud Enterprise

Telemetry Broker

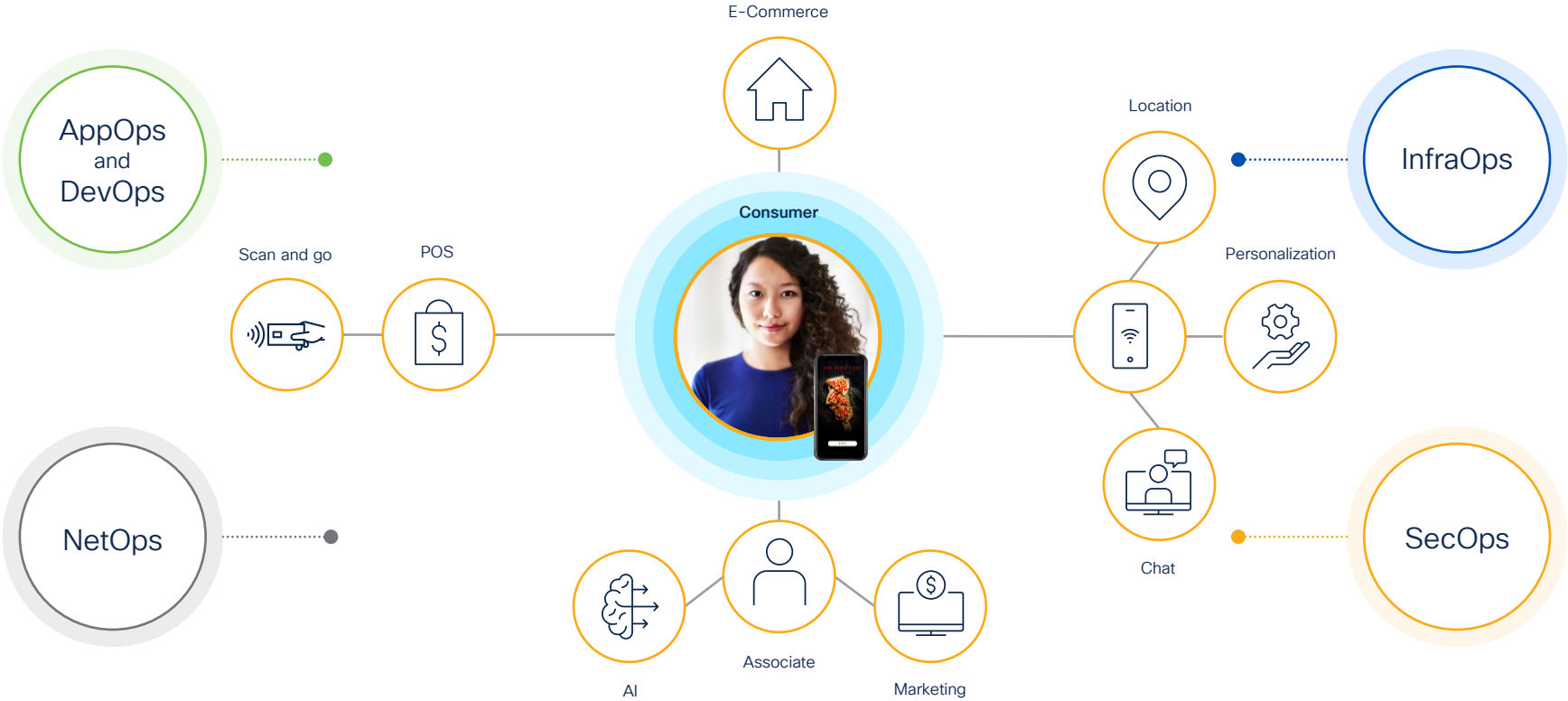
Provides Full Visibility to On-Prem and Cloud Telemetry



Omni Cloud Enterprise

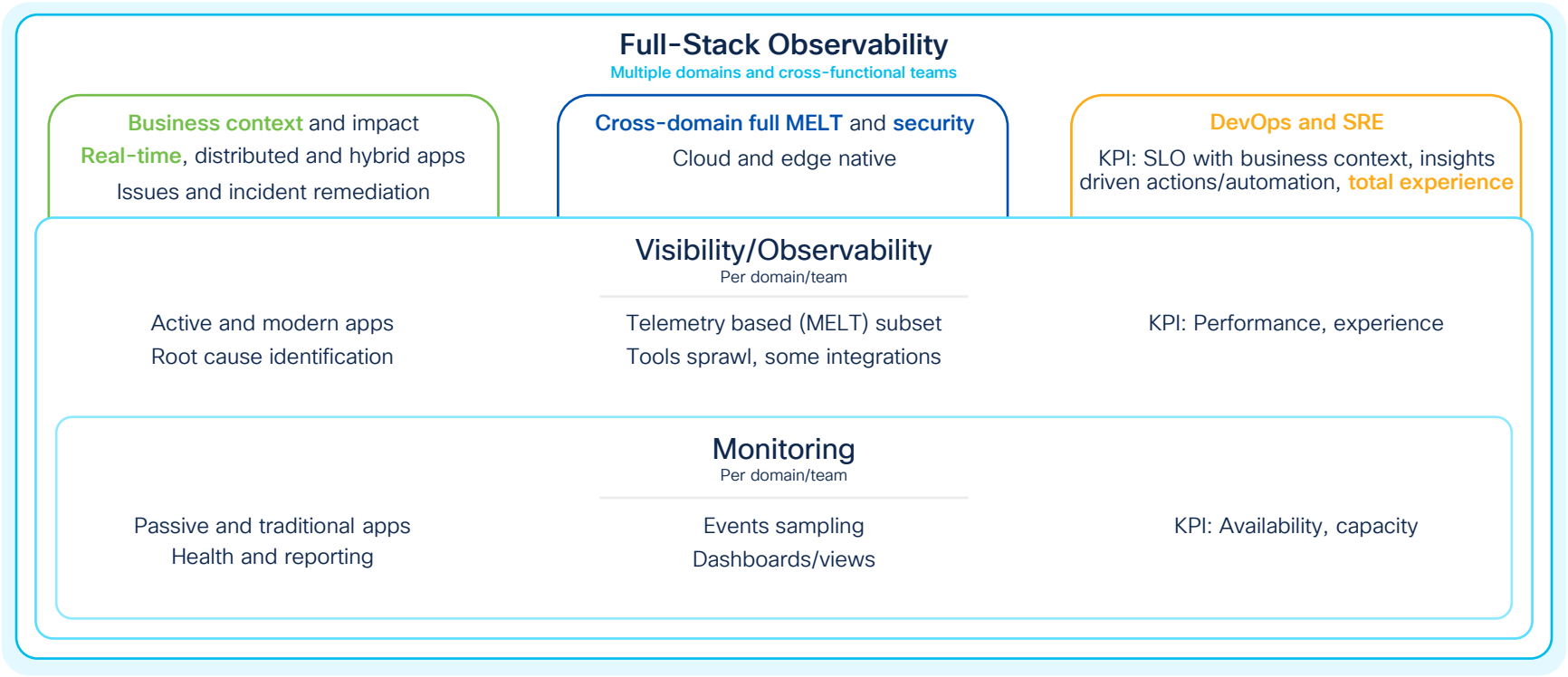
Your teams need to see the full stack of available data

Shared context across the digital experience



Full-Stack Observability

Builds on monitoring and visibility, and adds business context



Cisco Full-Stack Observability

Full-Stack Visibility

Observable and optimizable technology stack

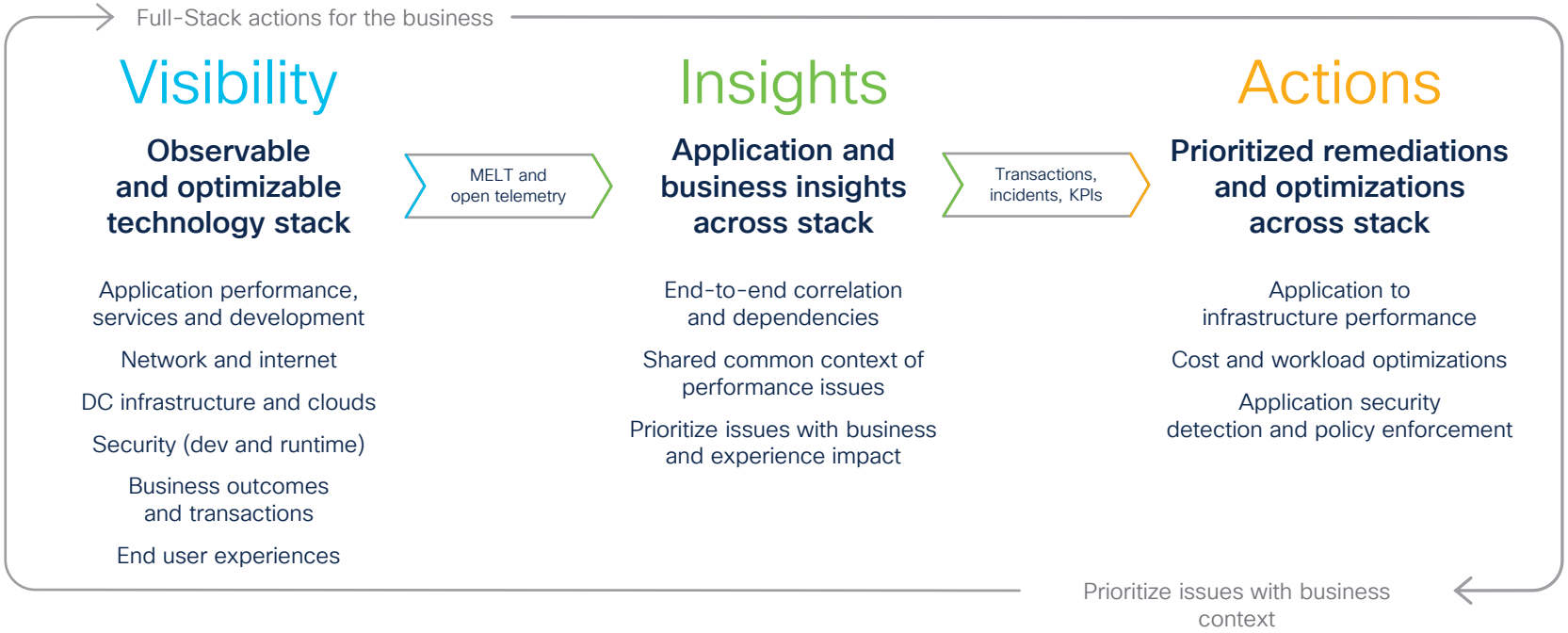
Full-Stack Insights

Application and business insights across stack

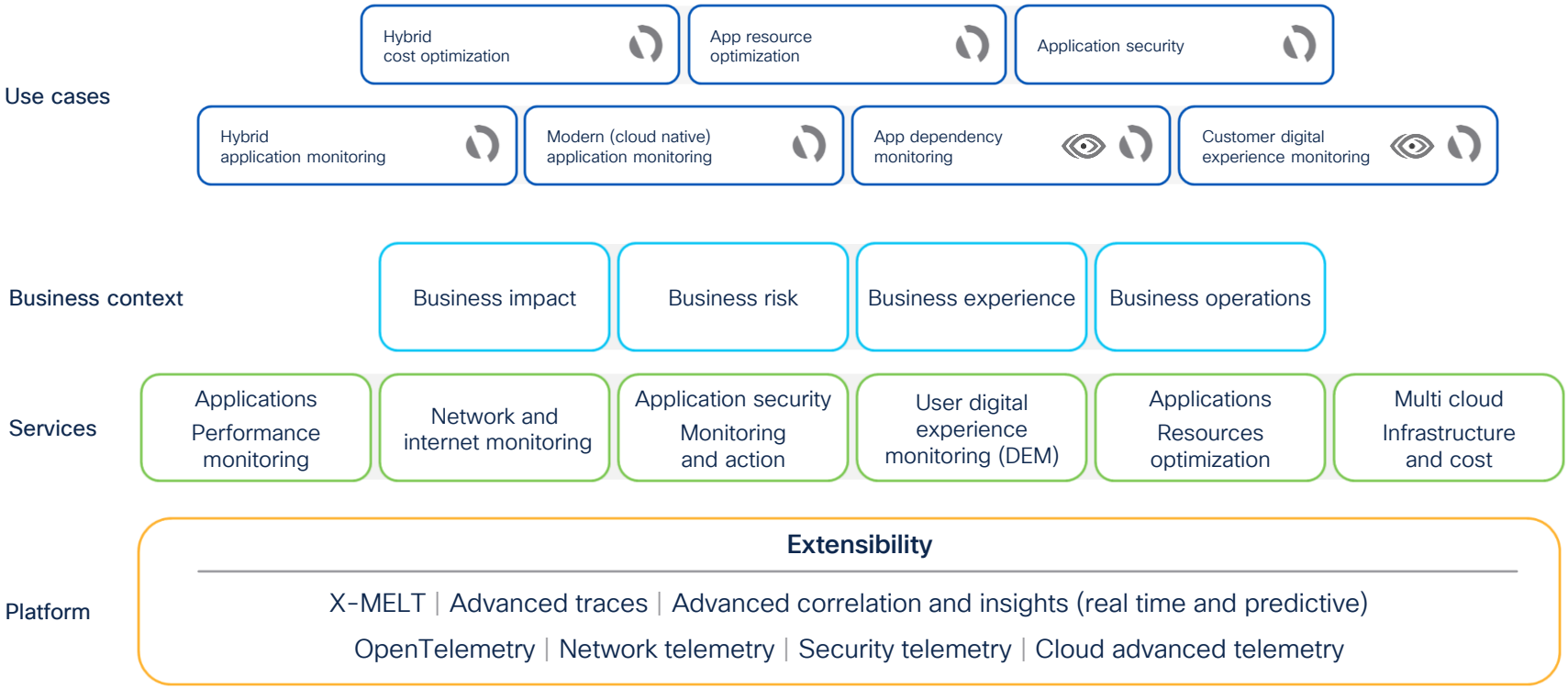
Full-Stack Actions

Prioritized remediations and optimizations across stack

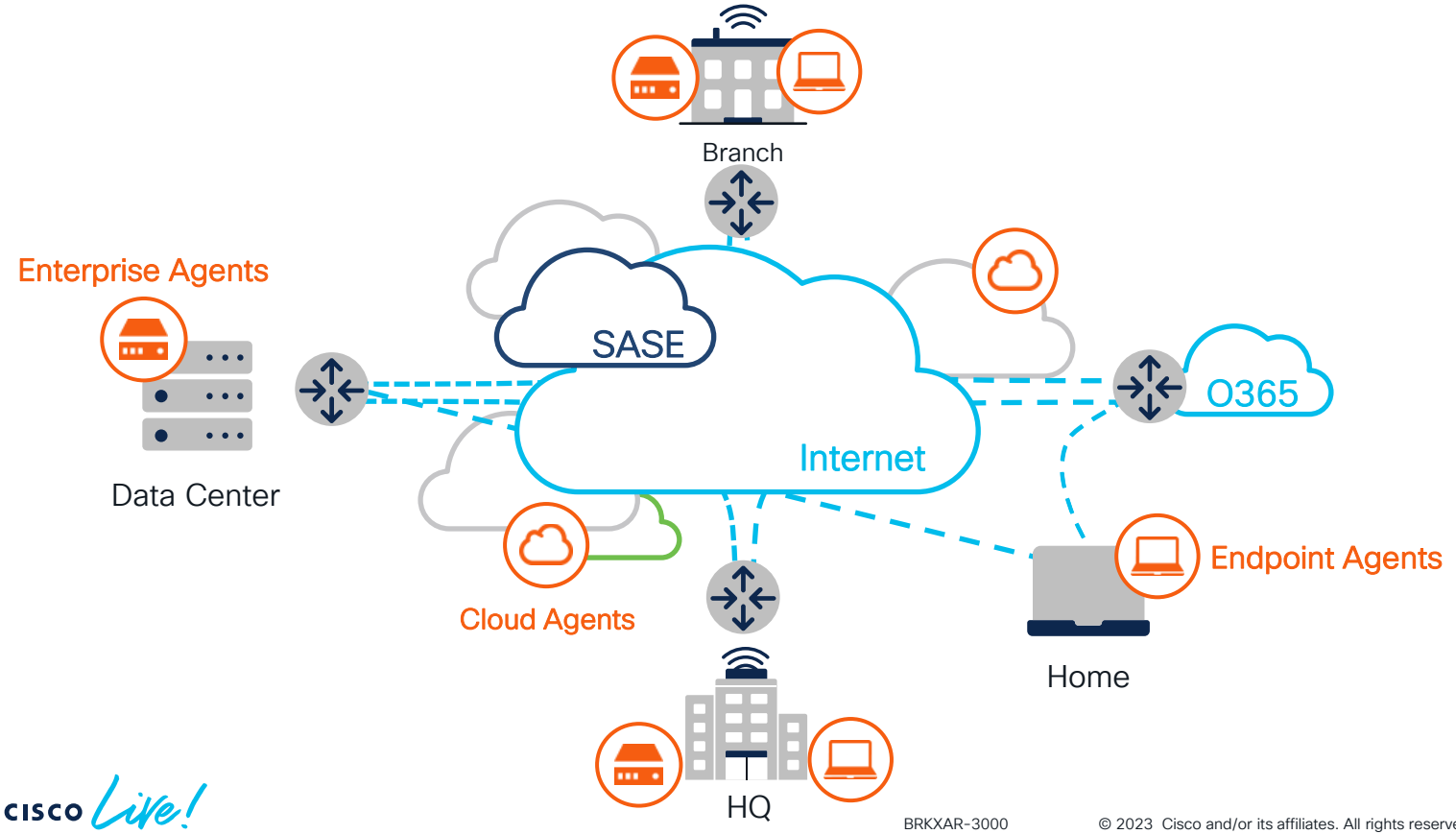
Differentiated solution with business context



Cisco Full-Stack Observability Architecture Foundation

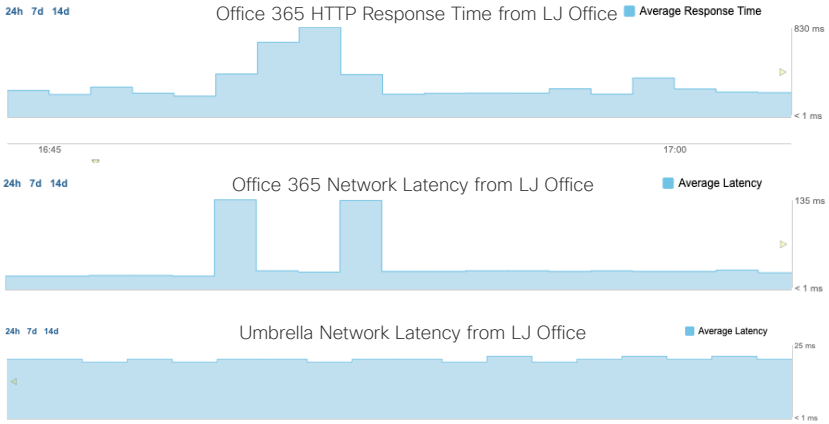


Collect performance data from every perspective



Multi-layer Correlation

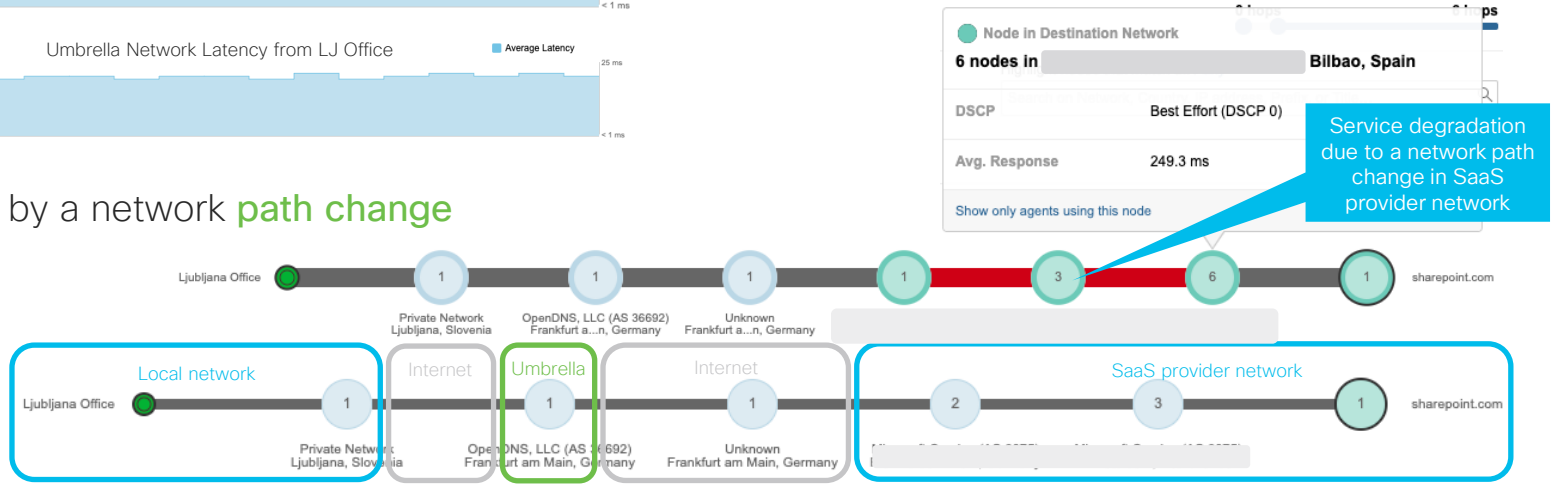
When service degradation occurs, quickly identify where the problem is.



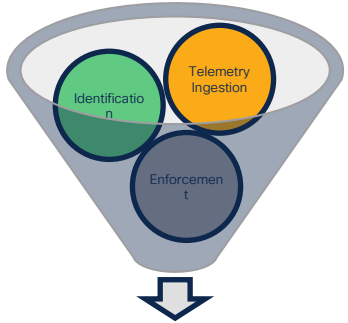
1 Increase in the service response time

2 Due to an increase in network latency

3 Caused by a network path change



2- Identification

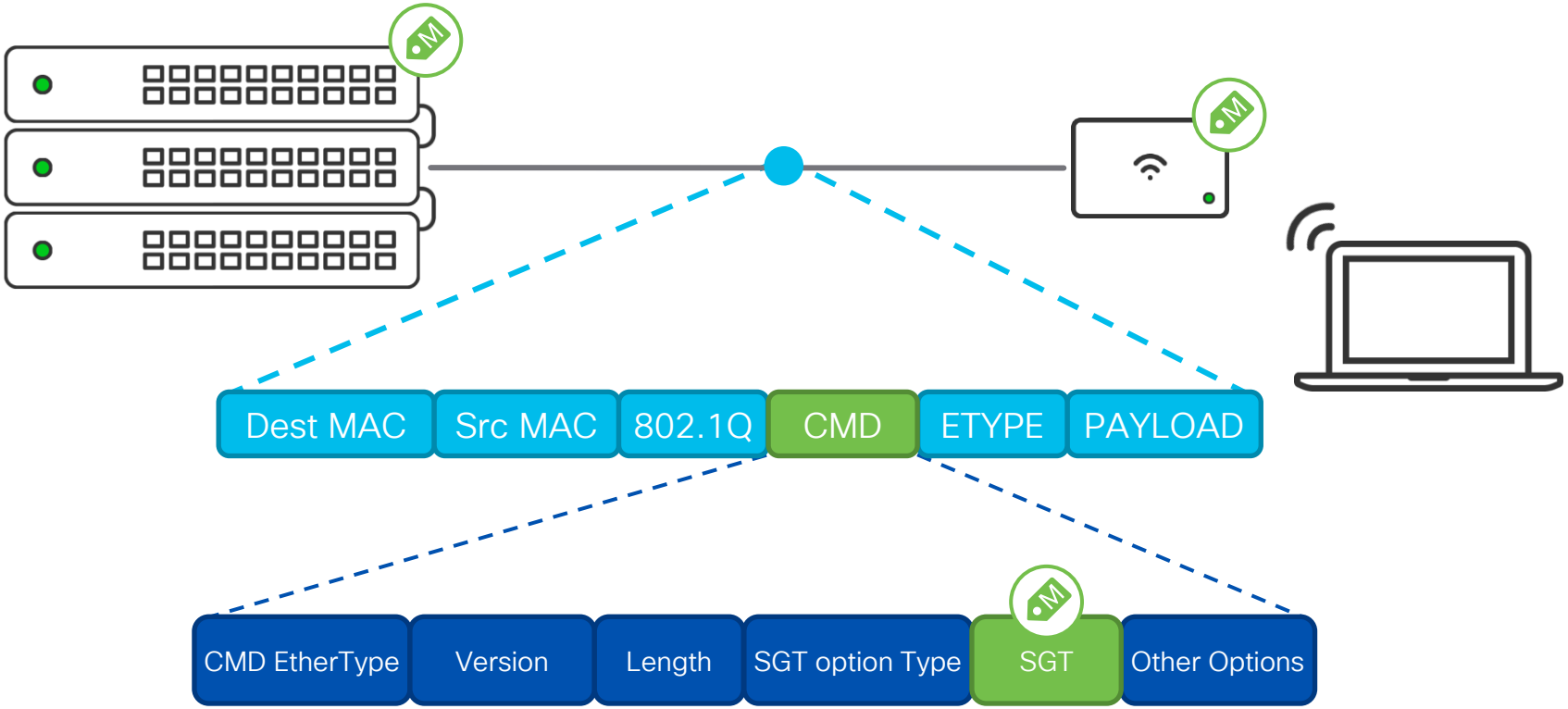


1- IP Subnets – Default

2- DSCP – Used in QoS, lacks granularity

3- MetaData, CMD, SGT – Our focus

What are SGTs?



Flexible Tag Assignment

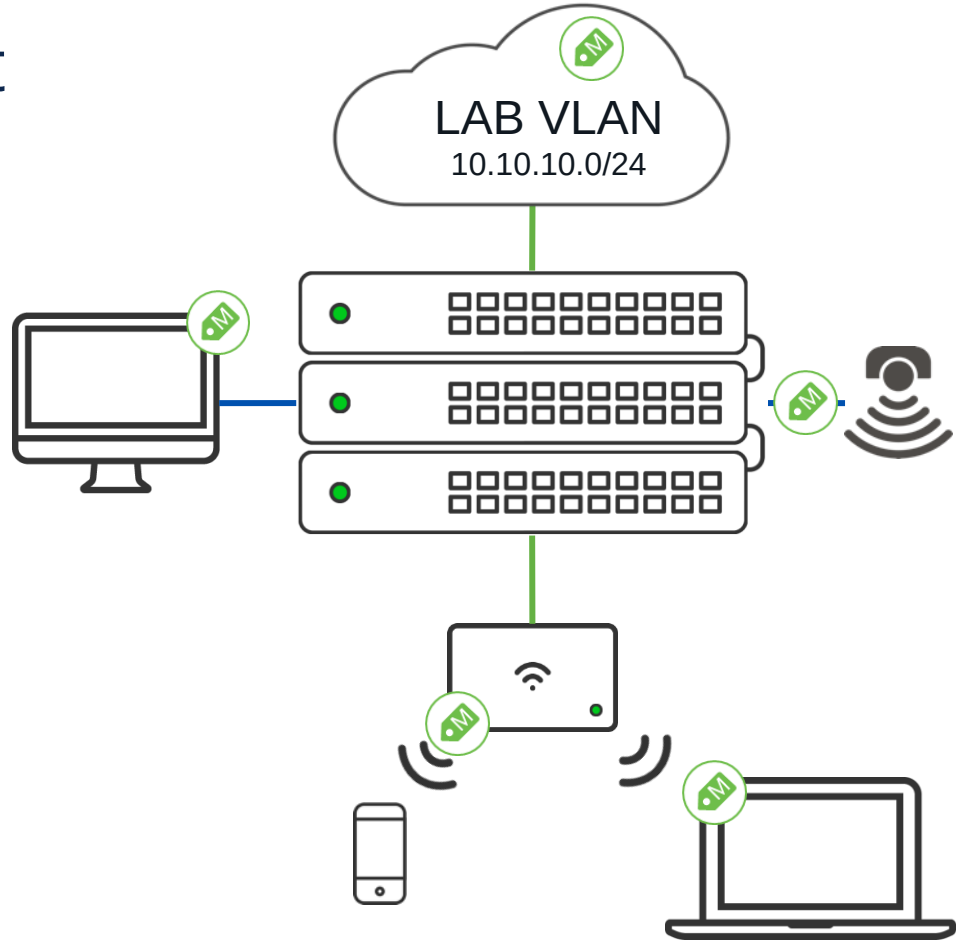
Tags can be applied in many different ways:

Statically assigned to a switch port
- Wired IOT Sensors

Static assignment per SSID
- Guest Users

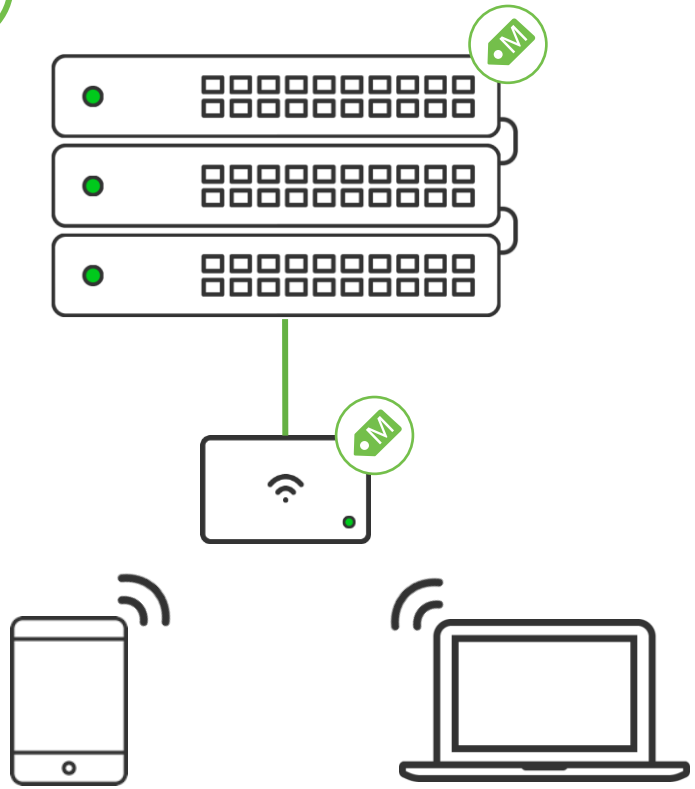
Dynamic assignment via RADIUS
- Wired & Wireless 802.1x

Static IP to SGT Mapping
- Last resort to map traffic to an SGT
- Uses network objects as source for mapping



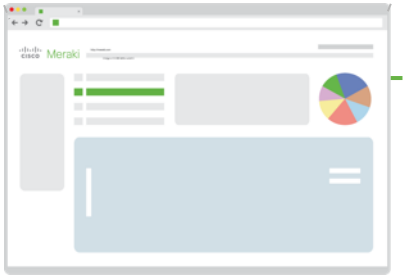
Introducing Adaptive Policy

- Way to identify and segment users, devices, and networks by using a tag
- Built on the Cisco TrustSec (CTS) model using SGT
- Org-wide policy based on intent, not IP
- Works within or between VLANs (i.e. Layer 2 or Layer 3 isolation)
  - Reduces the need for complex configurations like Private VLAN
- Enable zero-trust on the network by leveraging SGT



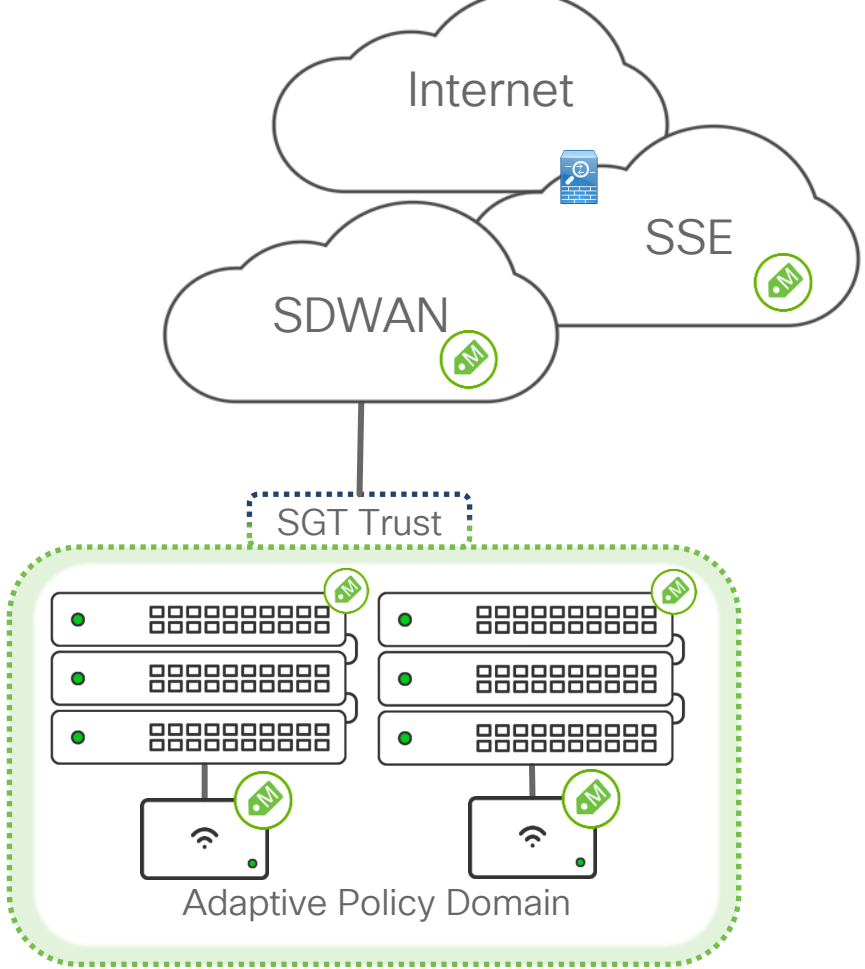
One Consistent Policy Across All Sites

SRC | DST	Employee	IoT	IoT Server
Employee	✔	✖	✔
IoT	✖	✖	✔
IoT Server	✔	✔	✔



Policy & Groups are configured in dashboard and pushed to Adaptive Policy nodes like any other Meraki configuration change

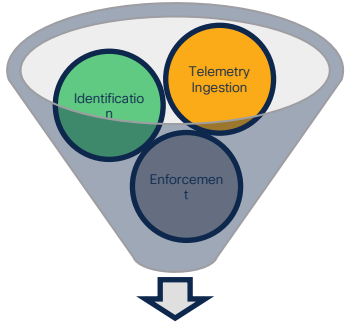
End-to-End Policy Orchestration



Multidomain Integration – Things to remember

- SGT's are gaining recognition across domains SDA, SD-WAN etc
  - As long as the values map similarly, it will work
- ISE would be required to keep the SGT mapping
  - Leverage the Policy Sync container to synchronize with Dashboard
- SGT's are also compatible with Cisco Catalyst, ISR, CSR, ASA, ACI, Nexus, and FTD devices that support SGTs

3- Enforcement

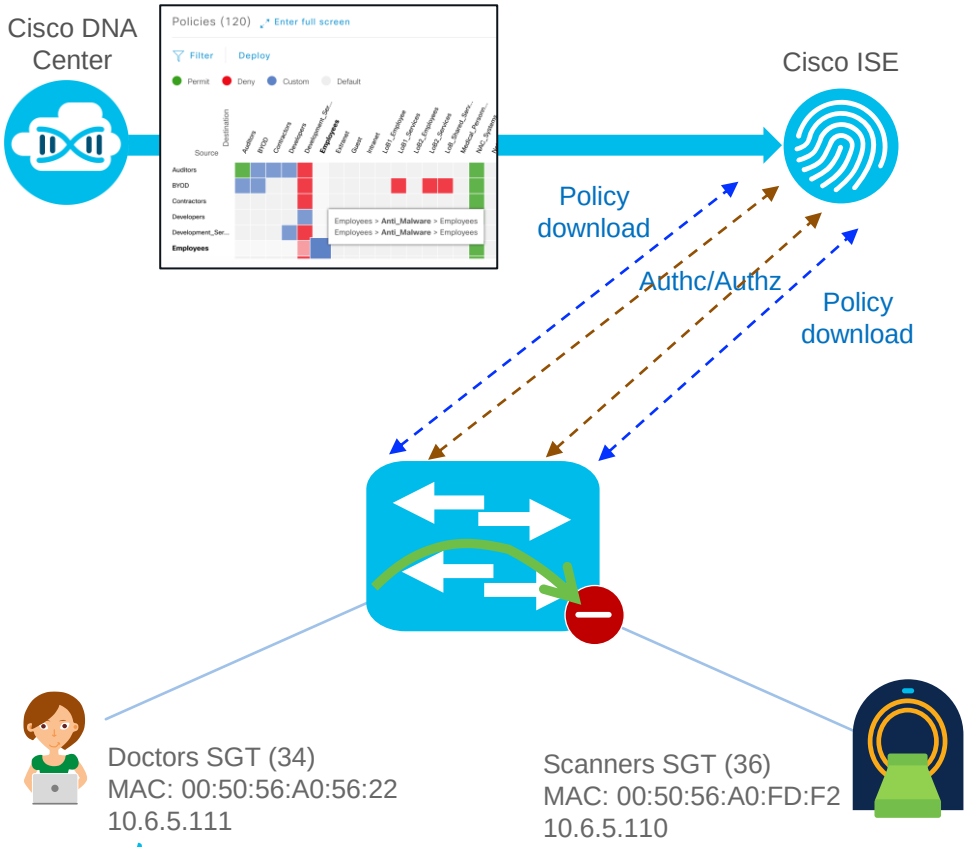


1- Consistent application

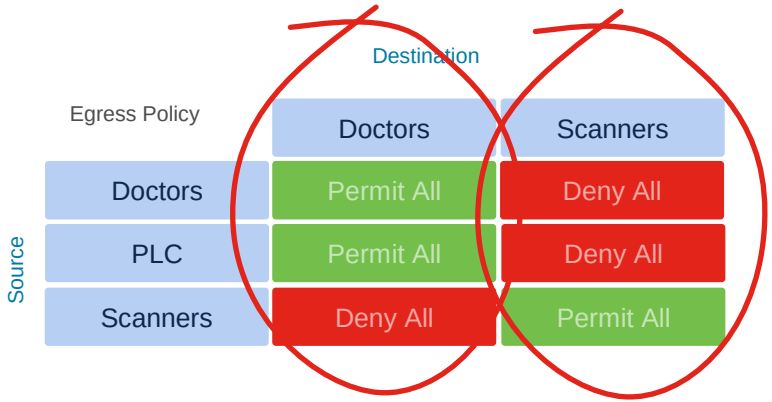
2- Improve security risk management

3- Compliance

Classification, SGT Lookup and Enforcement



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



Key Takeaways

- Multi-Domain Networks governs by their independent policies.
- Policies in different domains generally don't talk to each other.
- Troubleshooting in multi-domain is tough
- Need a robust Multi-Domain policy architecture, which can identify, ingest telemetry, enforce policy, and report

Fill out your session surveys!

Attendees who fill out a minimum of four session surveys and the overall event survey will get **Cisco Live-branded socks** (while supplies last)!

Attendees will also earn 100 points in the **Cisco Live Challenge** for every survey completed.

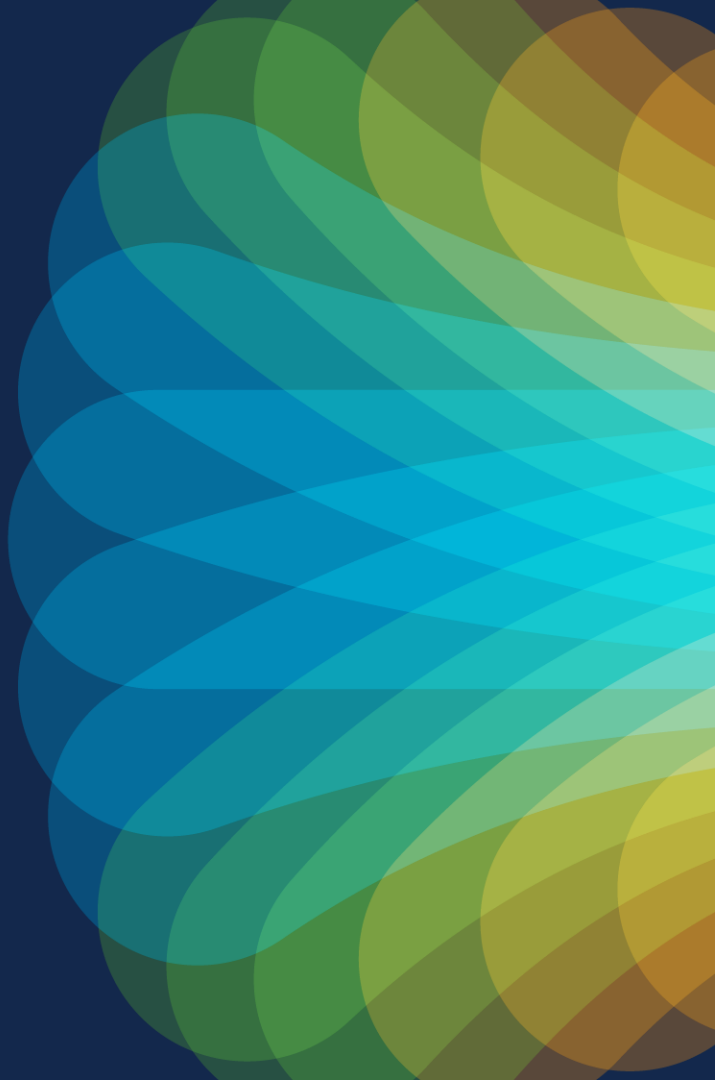
These points help you get on the leaderboard and increase your chances of winning daily and grand prizes

Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

The bridge to possible

Thank you



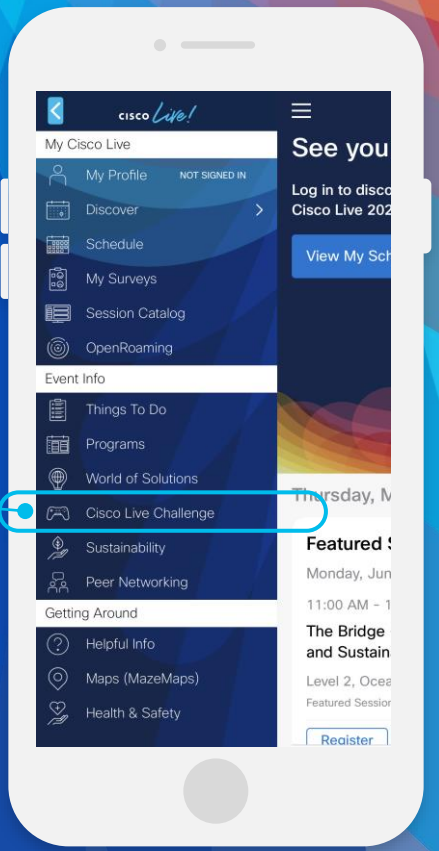
Cisco Live
Challenge

Gamify your Cisco Live experience!

Get points for attending this session!

How:

1. Open the Cisco Events App.
2. Click on 'Cisco Live Challenge' in the side menu.
3. Click on View Your Badges at the top.
4. Click the + at the bottom of the screen and scan the QR code:




cisco Live!
Let's go
#CiscoLive