
cisco Live!
Let's go
#CiscoLive

The bridge to possible

Cisco Hybrid Cloud Security: It's never been easier to protect hybrid and multicloud environments

PSOSEC-1024

Yuval Yatskan, Sr. Director, Product Marketing

June 4-9, 2023

Cisco Webex App

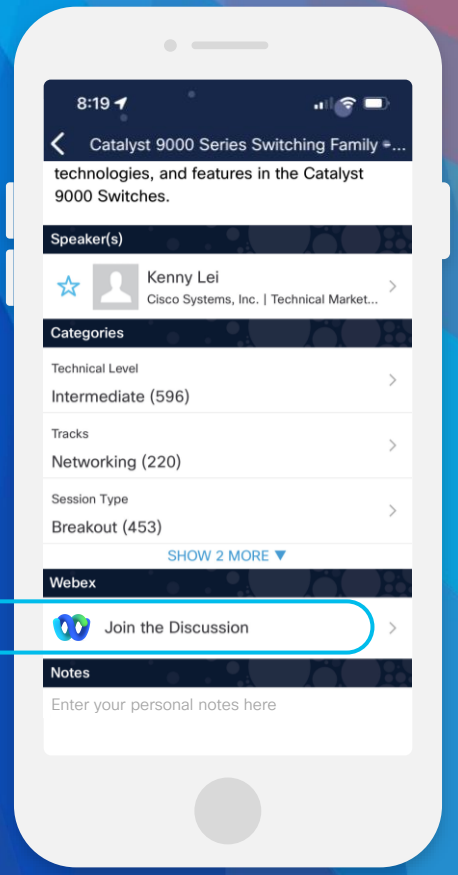
Questions?

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.

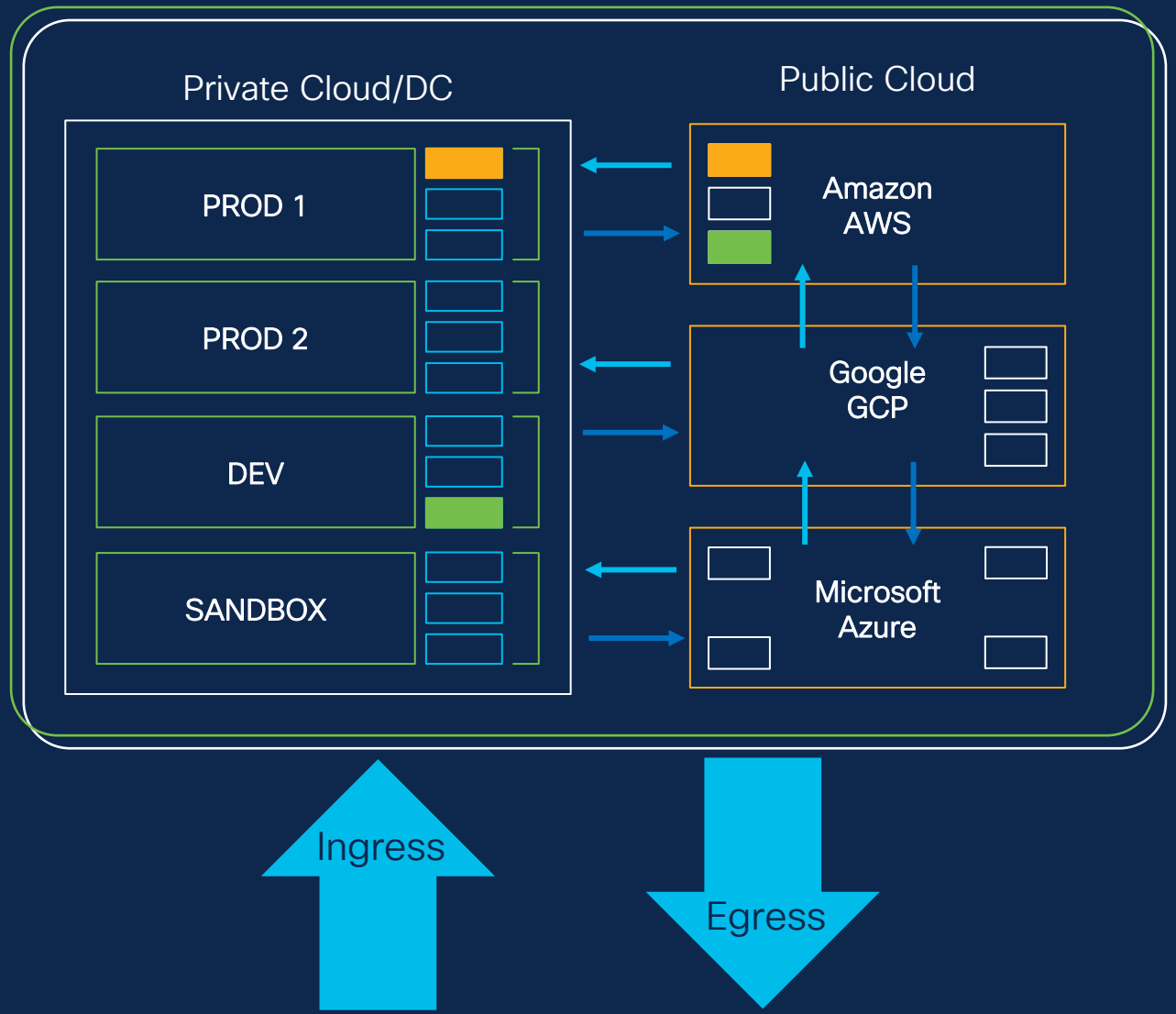


https://ciscolive.ciscoevents.com/ciscolivebot/#PSOSEC-1024

Customer needs are dynamic

82% of IT leaders have adopted hybrid cloud[1]

58% of IT leaders are deploying 2 to 3 public IaaS clouds[1]

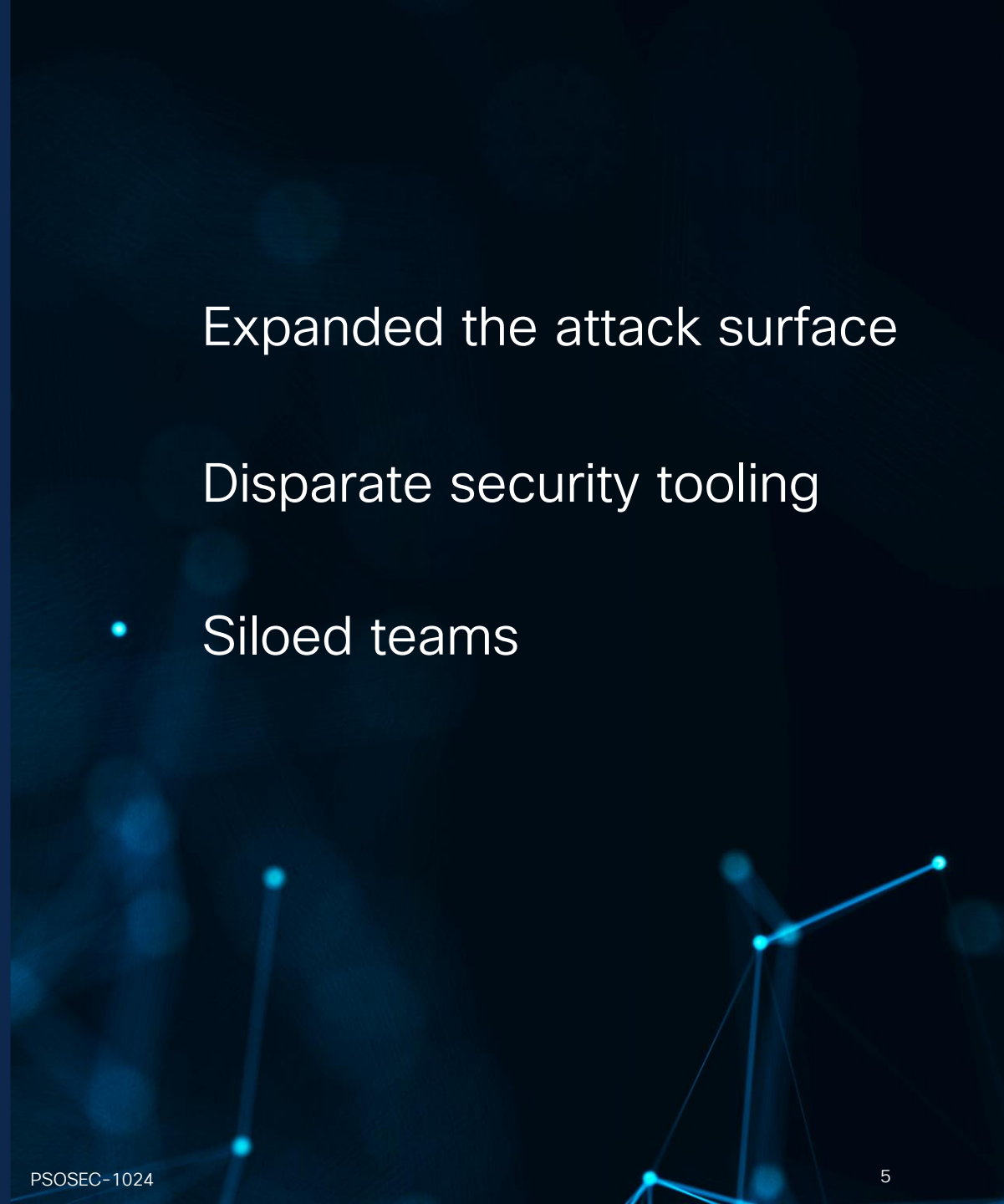


[1] 2022 Cisco Global Hybrid Cloud Trends Report

But the modern distributed application environment

has spawned complexity that is beyond human scale.

- Expanded the attack surface
- Disparate security tooling
- Siloed teams



69%

of orgs report multicloud security configurations led to data breaches or exposures.

55%

say maintaining consistent security policies across multicloud environments is one of their biggest security challenges.

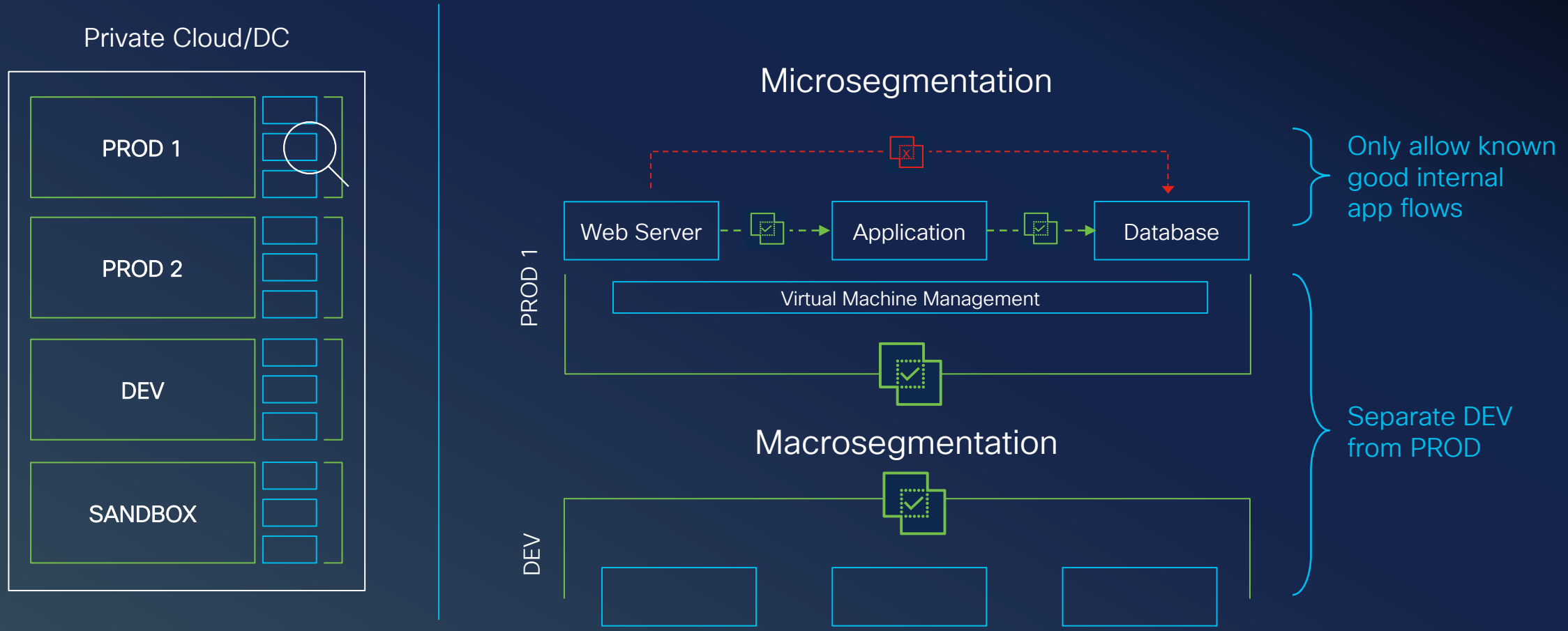
And the stakes are higher than ever...

$4.35M
Global cost of a breach[1]

287 days
To identify and contain a breach[2]

1,248
average number of attacks per week[3]

Protecting your private cloud and data center



Protecting hybrid and multicloud environments is much harder...

Protecting hybrid and multicloud environments is much harder...

Protecting hybrid and multicloud environments is much harder...

Current IT patchwork creates problems

More products leads to more complexity within your business and IT environment

- Exfiltration
- Ransomware
- Lateral movement
- Web threats
- Stolen credentials
- Spam

76

Average number of security tools used per enterprise today

New threats spawn new vendors, putting the burden on customers

Leaving organizations with brittle, rigid and complex security stacks that fail to protect them

```
access-list CSM_FW_ACL_; 6306214 elements; name hash: 0x4a69e3f3
access-list CSM_FW_ACL_ line 1 remark rule-id 9998: PREFILTER POLICY: Default Tunnel and Priority Policy
access-list CSM_FW_ACL_ line 2 remark rule-id 9998: RULE: DEFAULT TUNNEL ACTIONRULE
access-list CSM_FW_ACL_ line 3 advanced permit ipinip any any rule-id 9998 (hitcnt=0) 0xf5b597d6
access-list CSM_FW_ACL_ line 4 advanced permit 41 any any rule-id 9998 (hitcnt=0) 0x06095aba
access-list CSM_FW_ACL_ line 5 advanced permit gre any any rule-id 9998 (hitcnt=0) 0x52c7a066
access-list CSM_FW_ACL_ line 6 advanced permit udp any eq 3544 any range 1025 65535 rule-id 9998 (hitcnt=0) 0x46d7839e
access-list CSM_FW_ACL_ line 7 advanced permit udp any range 1025 65535 any eq 3544 rule-id 9998 (hitcnt=77) 0xaf1d5aa5
access-list CSM_FW_ACL_ line 8 remark rule-id 268447747: ACCESS POLICY: MyTinyAccessPolicy - Mandatory
access-list CSM_FW_ACL_ line 9 remark rule-id 268447747: L7 RULE: DROP all bad stuff
access-list CSM_FW_ACL_ line 10 advanced permit ip ifc INET any any rule-id 268447747 (hitcnt=83363) 0x29d63446
access-list CSM_FW_ACL_ line 11 remark rule-id 268447749: ACCESS POLICY: MyTinyAccessPolicy - Mandatory
access-list CSM_FW_ACL_ line 12 remark rule-id 268447749: L7 RULE: Clients -> Internet
access-list CSM_FW_ACL_ line 13 advanced permit ip ifc LAN object-group FMC_INLINE_src_rule_268447749 ifc INET any rule-id 268447749
(hitcnt=1731679) 0x925c6e8c
access-list CSM_FW_ACL_ line 13 advanced permit ip ifc LAN 192.168.1.0 255.255.255.0 ifc INET any rule-id 268447749 (hitcnt=0) 0xec999bf6
access-list CSM_FW_ACL_ line 13 advanced permit ip ifc LAN 192.168.2.0 255.255.255.0 ifc INET any rule-id 268447749 (hitcnt=1731679) 0x724e89ef
access-list CSM_FW_ACL_ line 13 advanced permit ip ifc LAN 192.168.3.0 255.255.255.0 ifc INET any rule-id 268447749 (hitcnt=0) 0x68d32543
access-list CSM_FW_ACL_ line 14 advanced permit ip ifc WLAN object-group FMC_INLINE_src_rule_268447749 ifc INET any rule-id 268447749 (hitcnt=0)
0x6884bd05
access-list CSM_FW_ACL_ line 14 advanced permit ip ifc WLAN 192.168.7.0 255.255.255.0 ifc INET any rule-id 268447749 (hitcnt=0) 0xd043dbe0
access-list CSM_FW_ACL_ line 14 advanced permit ip ifc WLAN 192.168.8.0 255.255.255.0 ifc INET any rule-id 268447749 (hitcnt=0) 0xd1261b65
access-list CSM_FW_ACL_ line 14 advanced permit ip ifc WLAN 192.168.11.0 255.255.255.0 ifc INET any rule-id 268447749 (hitcnt=0) 0xf126518c
access-list CSM_FW_ACL_ line 15 advanced permit ip ifc test object-group FMC_INLINE_src_rule_268447749 ifc INET any rule-id 268447749 (hitcnt=0)
0x64e17fa7
```

Leaving organizations with brittle, rigid and complex security stacks that fail to protect them

```
access-list CSM_FW_ACL_; 6306214 elements; name hash: 0x4a69e3f3
access-list CSM_FW_ACL_ line 1 remark rule-id 9998: PREFILTER POLICY: Default Tunnel and Priority Policy
access-list CSM_FW_ACL_ line 2 remark rule-id 9998: RULE: DEFAULT TUNNEL ACTIONRULE
access-list CSM_FW_ACL_ line 3 advanced permit ipinip any any rule-id 9998 (hitcnt=0) 0xf5b597d6
access-list CSM_FW_ACL_ line 4 advanced permit 41 any any rule-id 9998 (hitcnt=0) 0x06095aba
access-list CSM_FW_ACL_ line 5 advanced permit gre any any rule-id 9998 (hitcnt=0) 0x52c7a066
access-list CSM_FW_ACL_ line 6 advanced permit udp any eq 3544 any range 1025 65535 rule-id 9998 (hitcnt=0) 0x46d7839e
access-list CSM_FW_ACL_ line 7 advanced permit udp any range 1025 65535 any eq 3544 rule-id 9998 (hitcnt=77) 0xaf1d5aa5
access-list CSM_FW_ACL_ line 8 remark rule-id 268447747: ACCESS POLICY: MyTinyAccessPolicy - Mandatory
access-list CSM_FW_ACL_ line 9 remark rule-id 268447747: L7 RULE: DROP all bad stuff
access-list CSM_FW_ACL_ line 10 advanced permit ip ifc INET any any rule-id 268447747 (hitcnt=0) 0xa1fbca72
access-list CSM_FW_ACL_ line 11 remark rule-id 268447749: ACCESS POLICY: MyTinyAccessPolicy - Mandatory
access-list CSM_FW_ACL_ line 12 remark rule-id 268447749: L7 RULE: Clients - Internet
access-list CSM_FW_ACL_ line 13 advanced permit ip ifc LAN object-group FMC_INLINE_src_rule_268447749 ifc INET any rule-id 268447749
(hitcnt=1731679) 0x925c6e8c
access-list CSM_FW_ACL_ line 13 advanced permit ip ifc LAN 192.168.1.0 255.255.255.0 ifc INET any rule-id 268447749 (hitcnt=0) 0xec999bf6
access-list CSM_FW_ACL_ line 13 advanced permit ip ifc LAN 192.168.2.0 255.255.255.0 ifc INET any rule-id 268447749 (hitcnt=1731679) 0x724e89ef
access-list CSM_FW_ACL_ line 13 advanced permit ip ifc LAN 192.168.3.0 255.255.255.0 ifc INET any rule-id 268447749 (hitcnt=0) 0x68432543
access-list CSM_FW_ACL_ line 14 advanced permit ip ifc WLAN object-group FMC_INLINE_src_rule_268447749 ifc INET any rule-id 268447749 (hitcnt=0)
0x6884bd05
access-list CSM_FW_ACL_ line 14 advanced permit ip ifc WLAN 192.168.7.0 255.255.255.0 ifc INET any rule-id 268447749 (hitcnt=0) 0xd043dbe0
access-list CSM_FW_ACL_ line 14 advanced permit ip ifc WLAN 192.168.8.0 255.255.255.0 ifc INET any rule-id 268447749 (hitcnt=0) 0xd1261b65
access-list CSM_FW_ACL_ line 14 advanced permit ip ifc WLAN 192.168.11.0 255.255.255.0 ifc INET any rule-id 268447749 (hitcnt=0) 0xf126518c
access-list CSM_FW_ACL_ line 15 advanced permit ip ifc test object-group FMC_INLINE_src_rule_268447749 ifc INET any rule-id 268447749 (hitcnt=0)
0x64e17fa7
```

- Hundreds of thousands firewall rules
- Multiple security tools that disagree on your security posture and actions to prioritize
- Appliances struggle to scale with high volumes of encrypted traffic
- Difficulty to apply least privileged access to applications and resources

Protecting hybrid and multicloud environments requires a new and different approach

1

Consolidate security and connectivity vendors

2

Simple to manage yet comprehensive security stack.

3

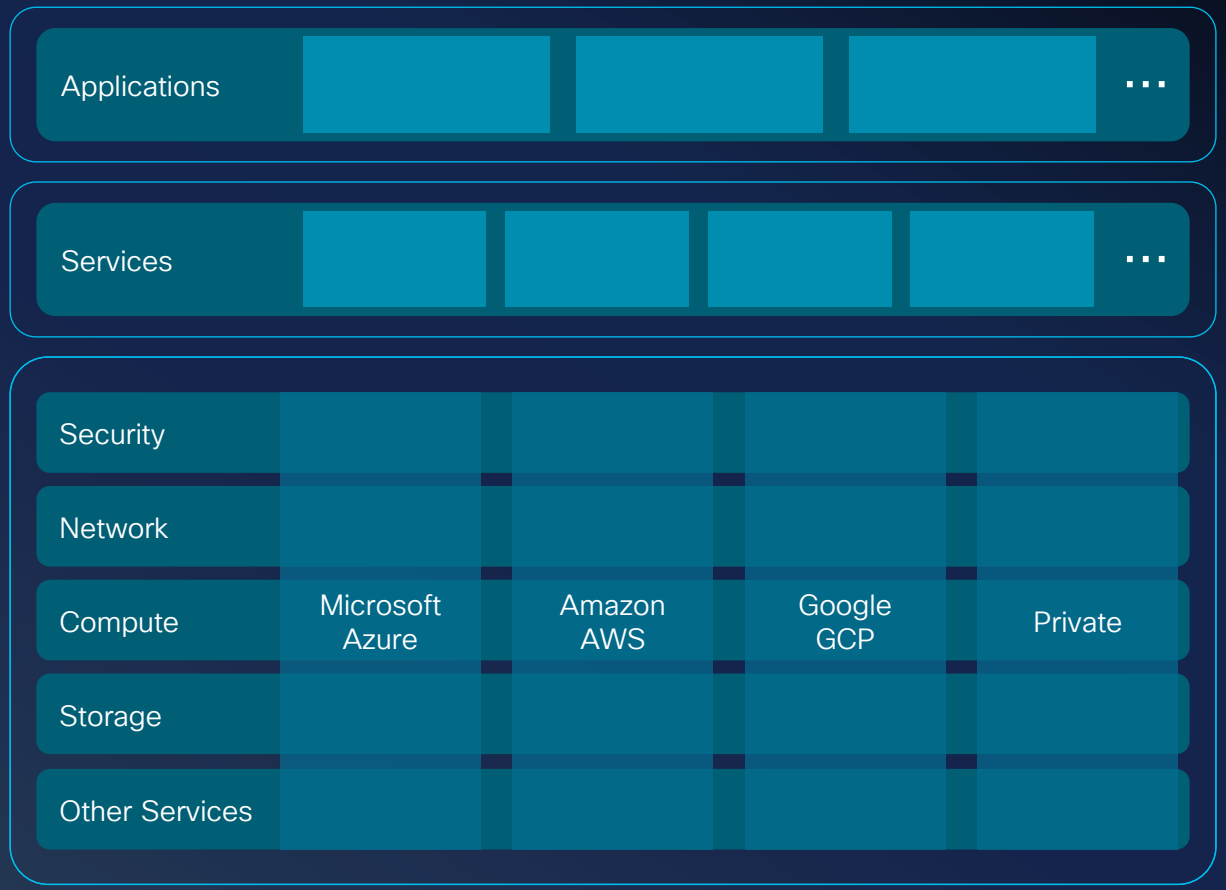
See more threats and detect them faster

Hybrid Multicloud Future

Software as a Service

Platform as a Service

Infrastructure as a Service



Expect a different patchwork of security tech in a multicloud world

Cisco Security Cloud

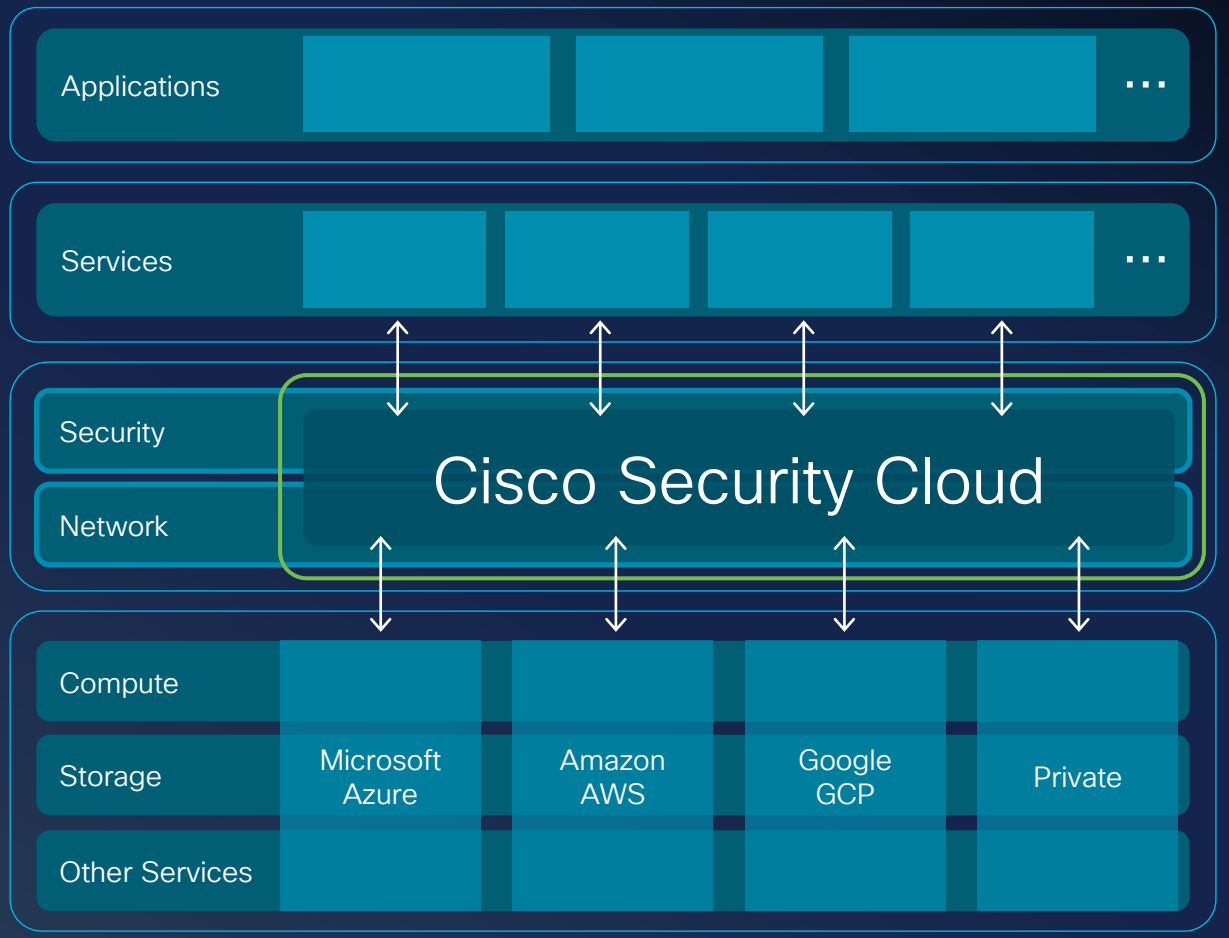
Software as a Service

Platform as a Service

Security & Networking as a Service

Optimizes performance & security of every connection

Infrastructure as a Service



Talos powers the Cisco portfolio with intelligence

400B
security events observed daily

500
threat researchers

Cisco XDR has the broadest native telemetry

One central data warehouse, analytics, and management in the Security Cloud

We see every email, even forwarded emails, to spot phishing

We see more web requests than anyone (600B per day) to spot fast-changing malicious sites

We uniquely track every process that makes a connection

We see more network traffic, in more detail, than anyone

Cisco Security Cloud benefits

Users

Seamless and fast connections and continuous granting of trust

IT

Centralized policy and advanced security enforcement

Developers + DevSecOps

Are free to focus on business logic not security functions

Security Operations Center

A unique end-to-end view that stops advanced threats like ransomware

Fill out your session surveys!

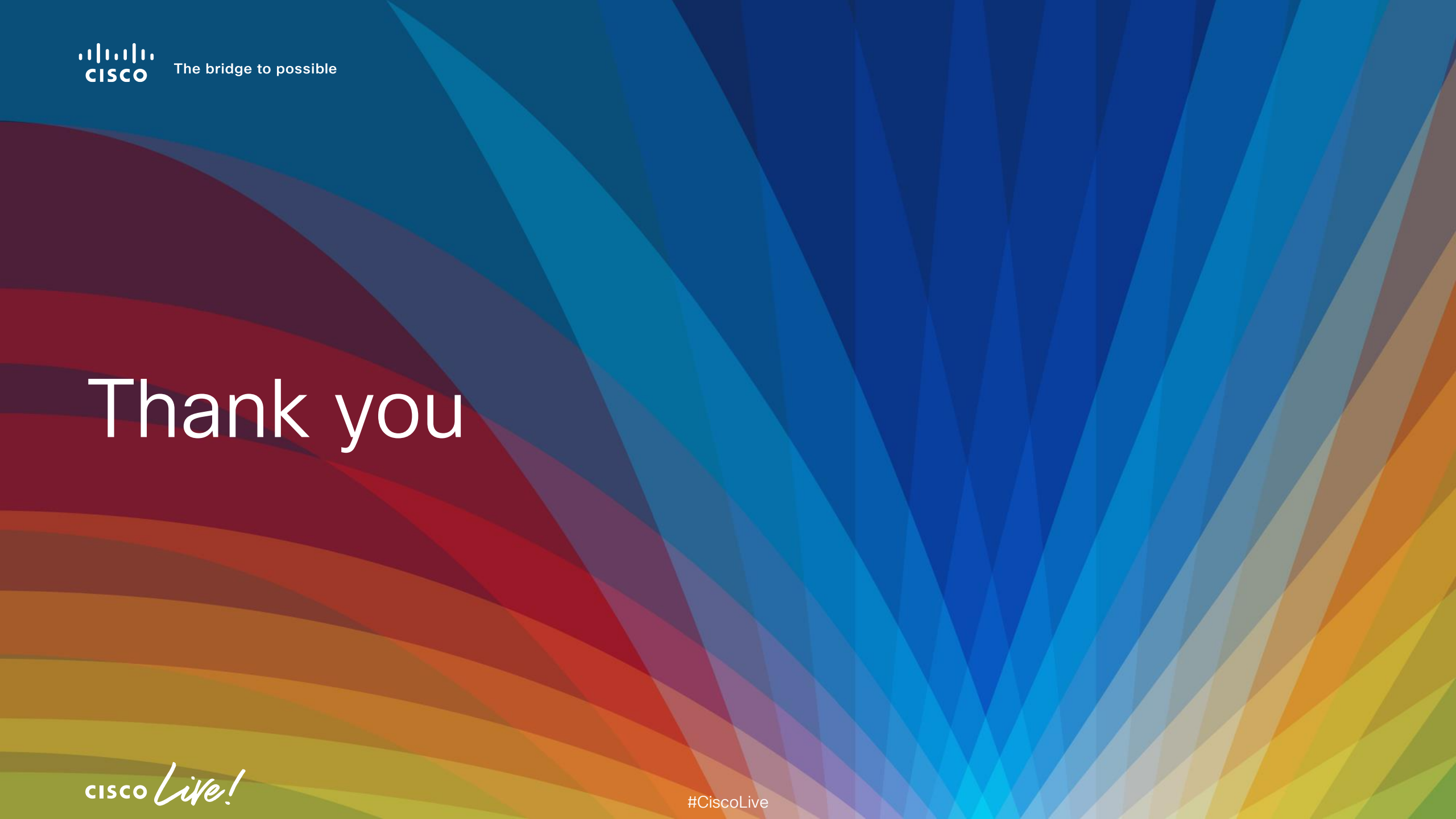
Attendees who fill out a minimum of four session surveys and the overall event survey will get **Cisco Live-branded socks** (while supplies last)!

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


cisco
The bridge to possible
Thank you
cisco Live!
#CiscoLive

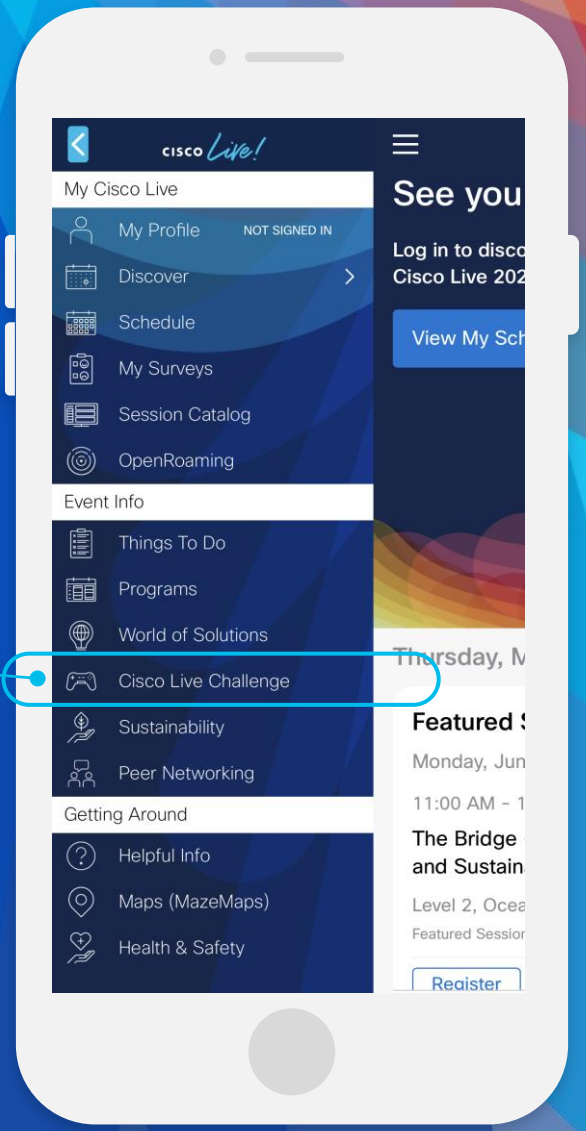
Cisco Live
Challenge

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!

cisco Live!

Let's go