The bridge to possible

The Latest in Cisco Secure Access

SSE Innovations

Neil Patel, Engineering Product Manager
@neilnpate1

BRKSEC-2285

cisco Live!

About Me

10 years in Cybersecurity

Cloud, Endpoint, & Network

Home automation enthusiast

DC Comics over Marvel

Car aficionado

Cisco Webex App

https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-2285

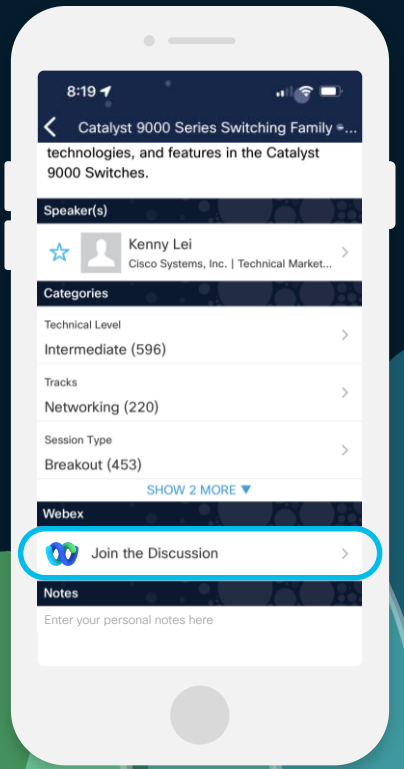
Questions?

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 7, 2024.

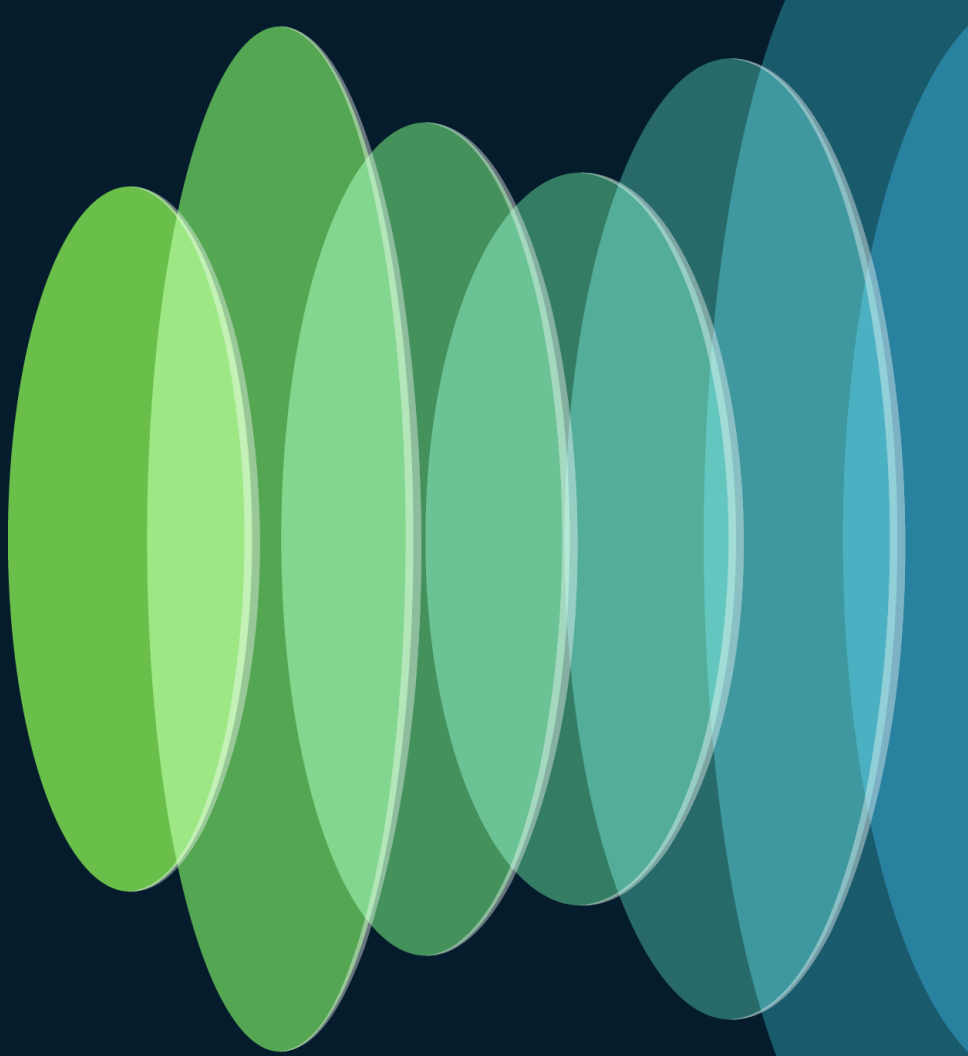


Agenda

- Today’s Challenge
- Latest SSE Architecture
- Newest Capabilities
- Leverage A.I.
- Future Look
- Conclusion

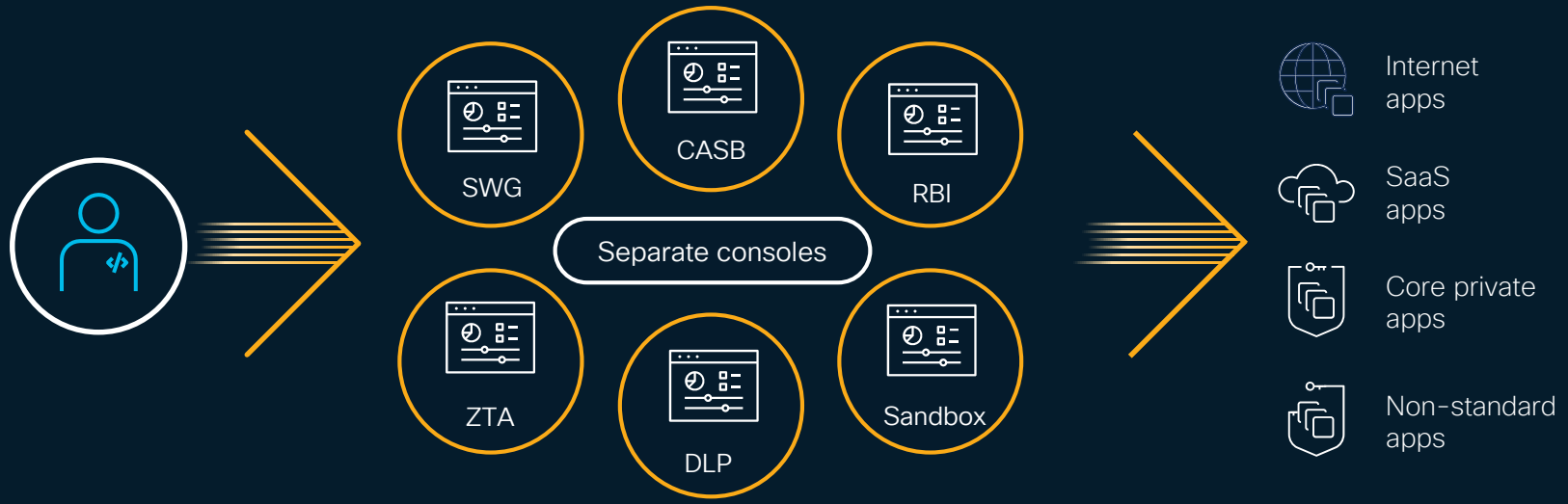
SSE Summary

Today's Challenge



cisco Live!

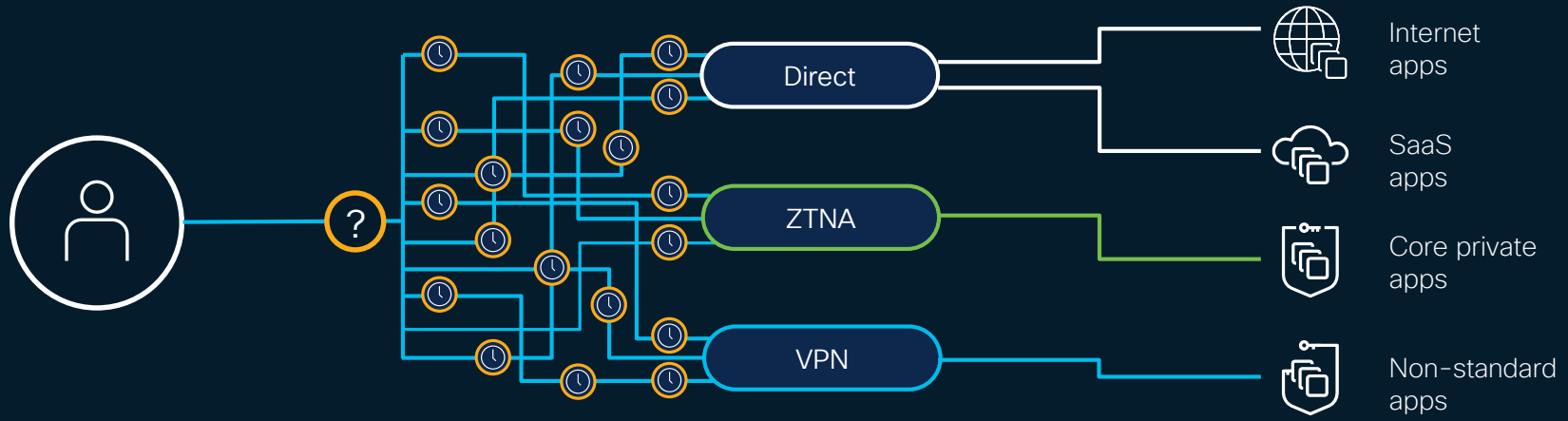
IT Challenges



Multiple products increase cost and inefficiencies

- Licenses/hardware
- Policy management
- Client management
- Reporting
- Elevated staffing levels

User Challenges

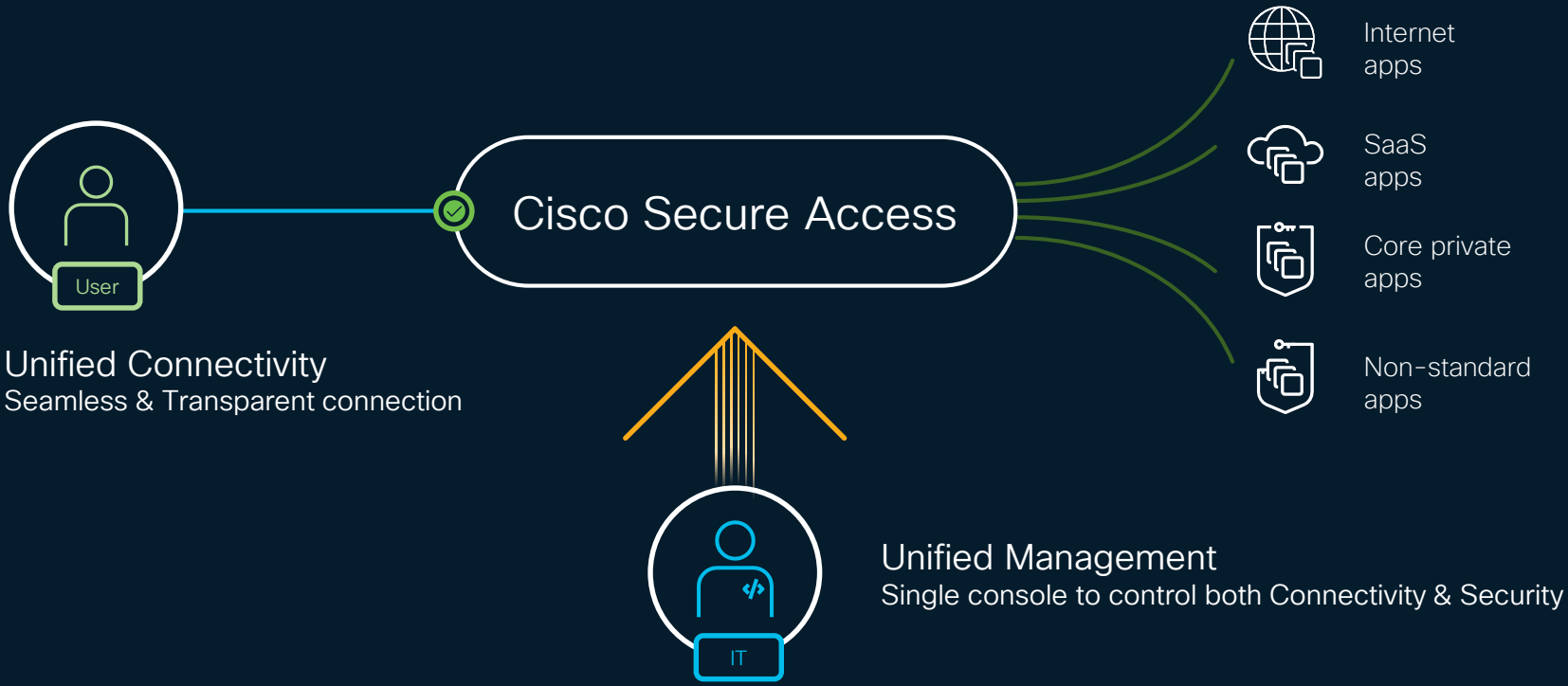


Varying connectivity methods ultimately create frustration

- Many connection decisions
- Various processes
- Multiple steps
- Repetitive authentication tasks

Cisco Secure Access

Unified Platform

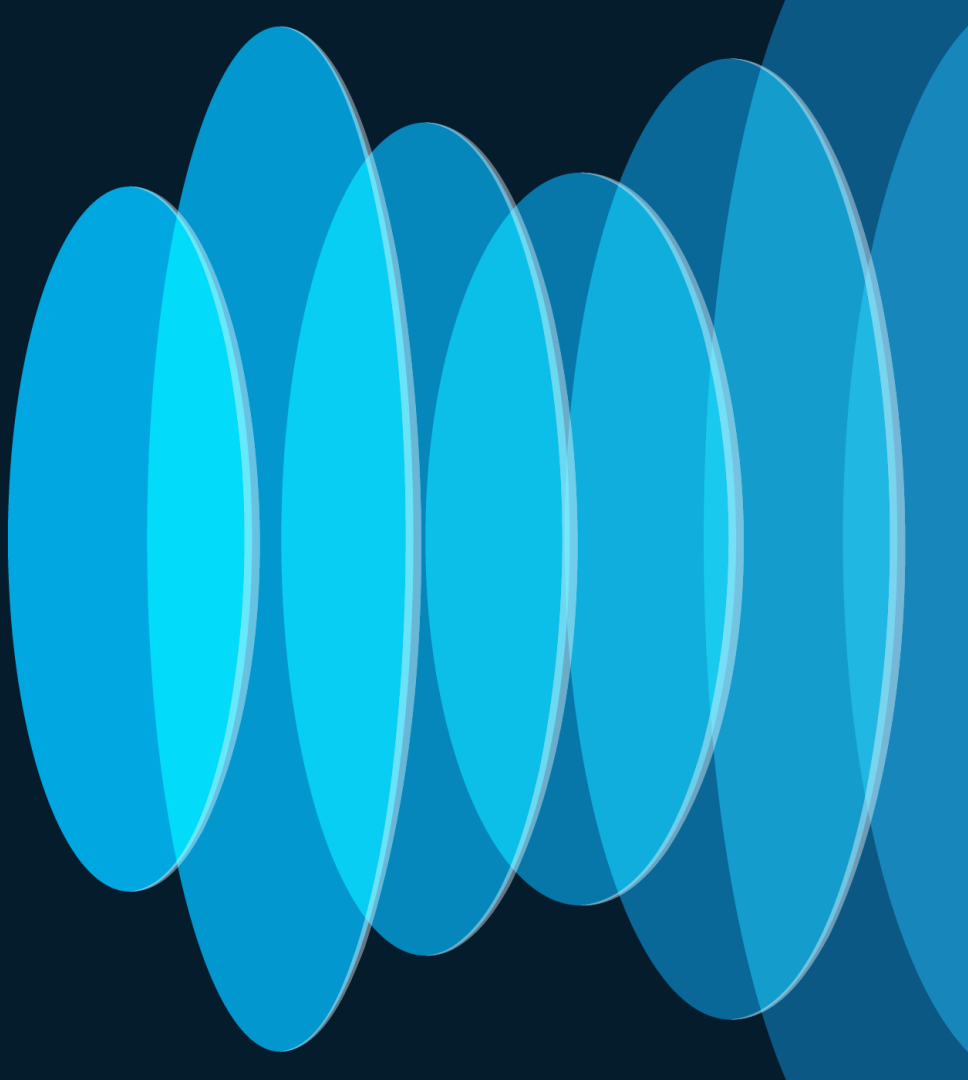


Unified Connectivity
Seamless & Transparent connection

Unified Management
Single console to control both Connectivity & Security

Innovative Design

A thoughtful architecture

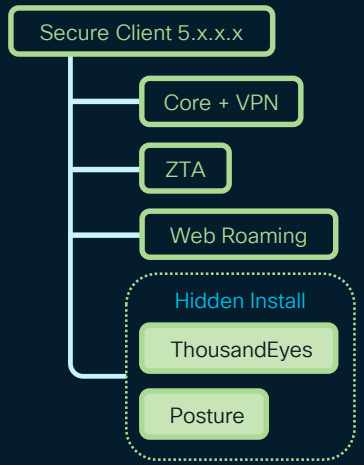


cisco Live!

End User Connectivity

Remote User – Managed Endpoint

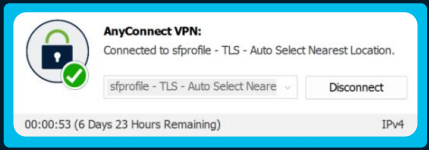
- Single Installer
- Customizable modules

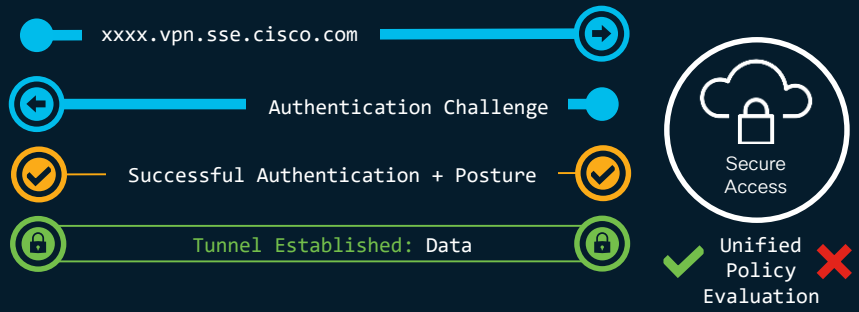


Managed Endpoint

Zero Trust VPNaaS

VPNaaS





- All ports and protocols (Private + Internet)
- Connect time Posture
- Always on + Start before logon
- IP Routable (IP Pool)

Authentication

1 SAML

- BYO IdP (Support SAML 2.0)
- SCIM User Provisioning
- +MFA
- User Interactive

2 Certificate

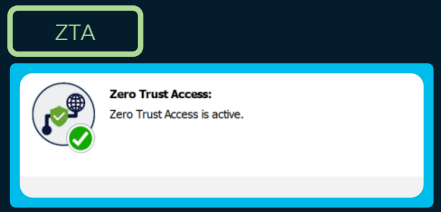
- Device Certificate
- Transparent Authentication

3 Radius

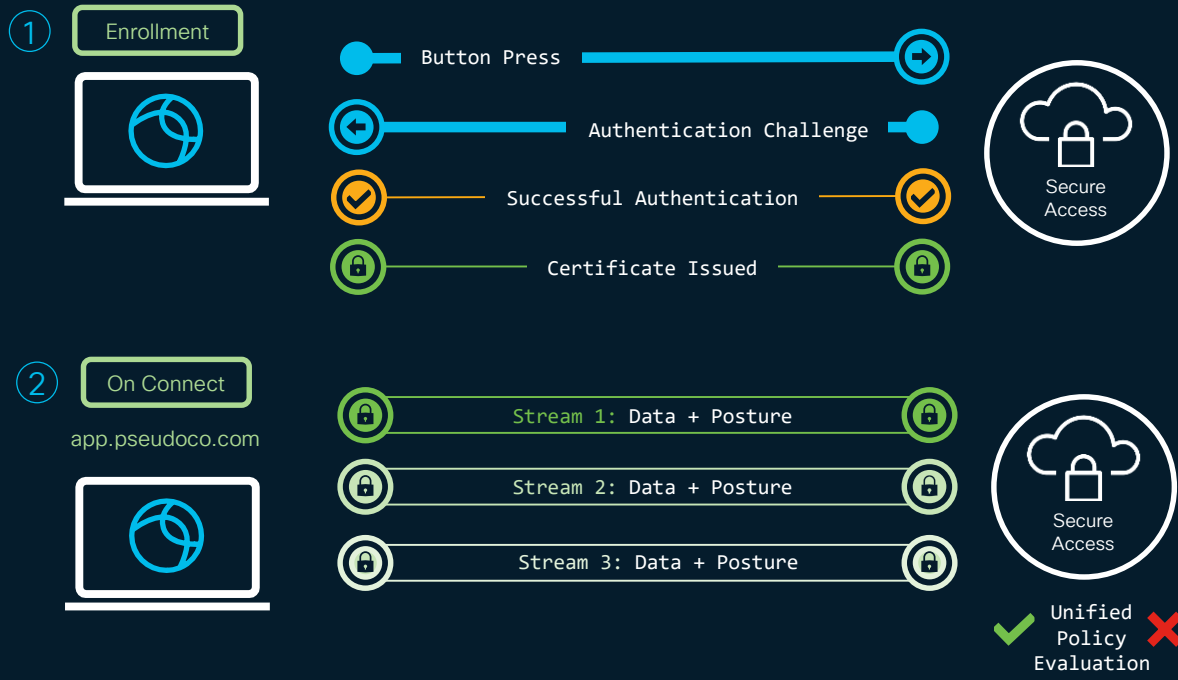
- Customize AAA servers
- User interactive

Managed Endpoint

Zero Trust Access

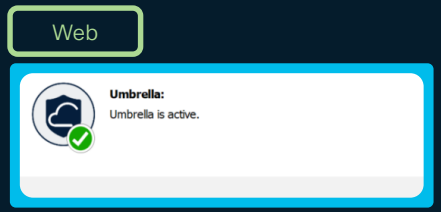


- One Time Enrollment
- SAML Based Authentication
- Per Connection Tunnel
- All ports and protocols (Private)
- QUIC + MASQUE Architecture
- Each connection carries Data + Posture
- No “at-rest” connectivity
- Anonymized connection (Ephemeral CGNAT IP)

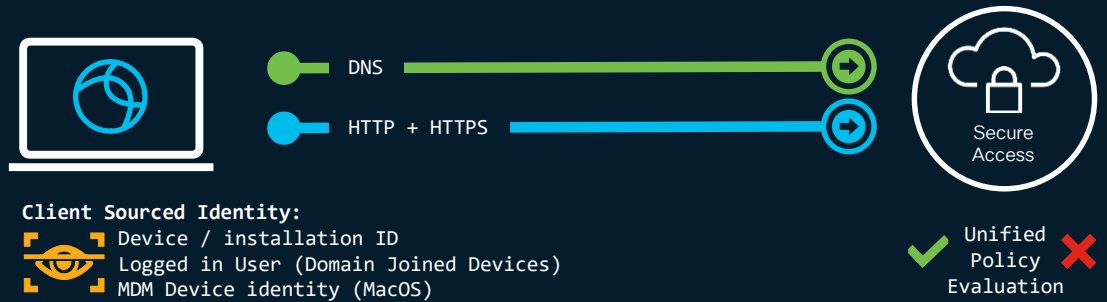


Managed Endpoint

Web Roaming

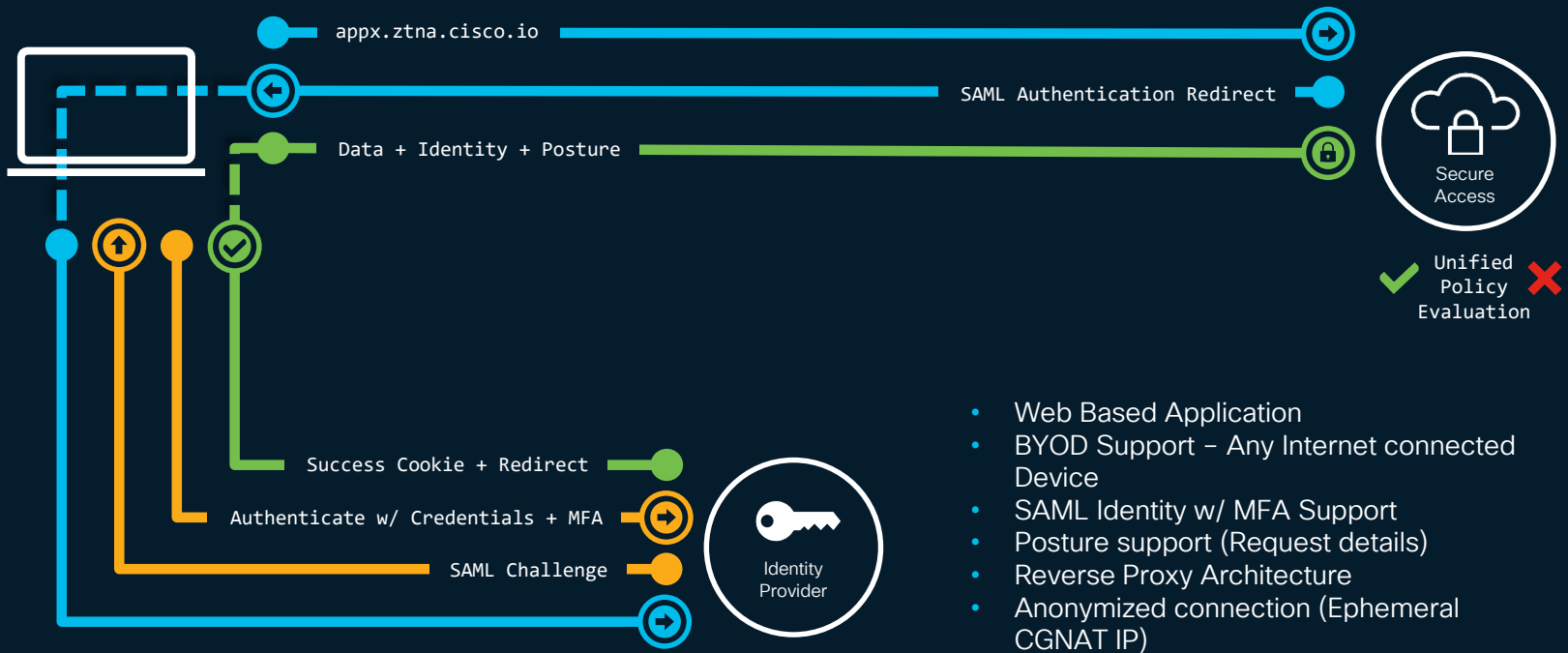


- Installation Profile enrollment
- Device Identity
- 80 + 443 HTTP/S Traffic
- Internet Only
- Network exclusion/ awareness
- DNS and/or Web Protection



Unmanaged Endpoint

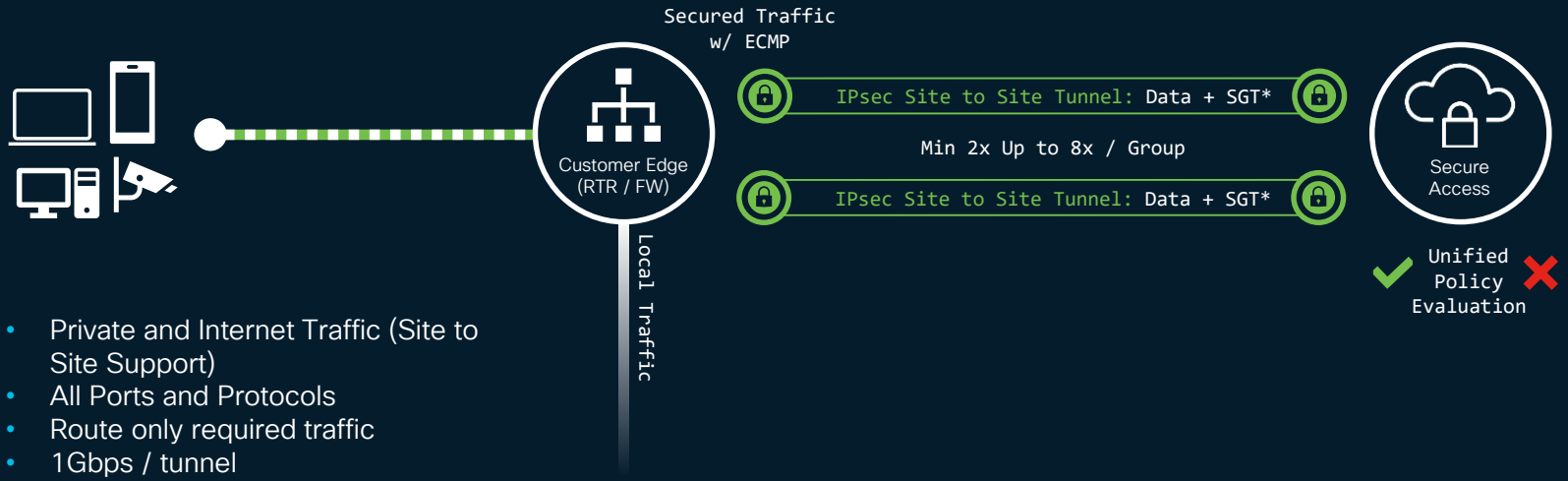
Clientless Web Access



- Web Based Application
- BYOD Support – Any Internet connected Device
- SAML Identity w/ MFA Support
- Posture support (Request details)
- Reverse Proxy Architecture
- Anonymized connection (Ephemeral CGNAT IP)

Network Device

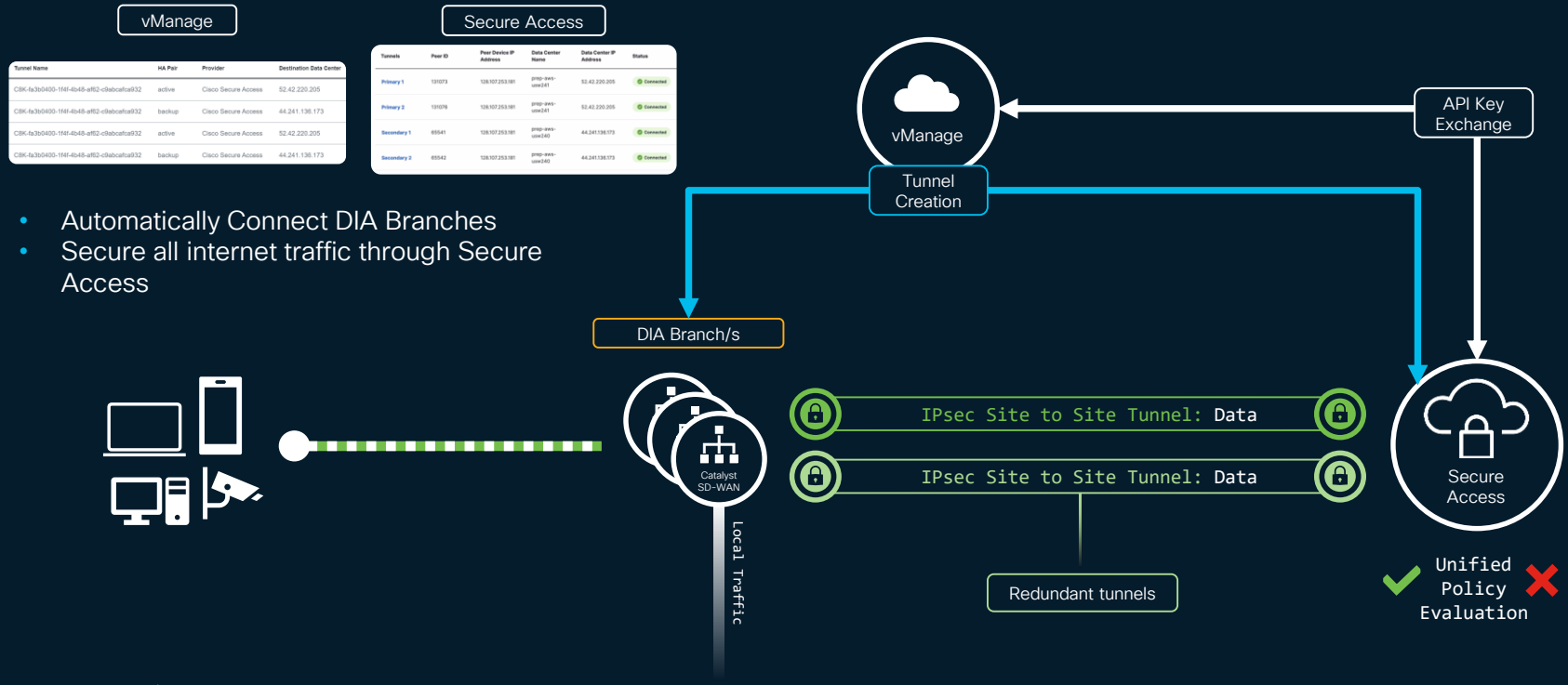
Tunnel Connectivity



- Private and Internet Traffic (Site to Site Support)
- All Ports and Protocols
- Route only required traffic
- 1Gbps / tunnel

Network Device

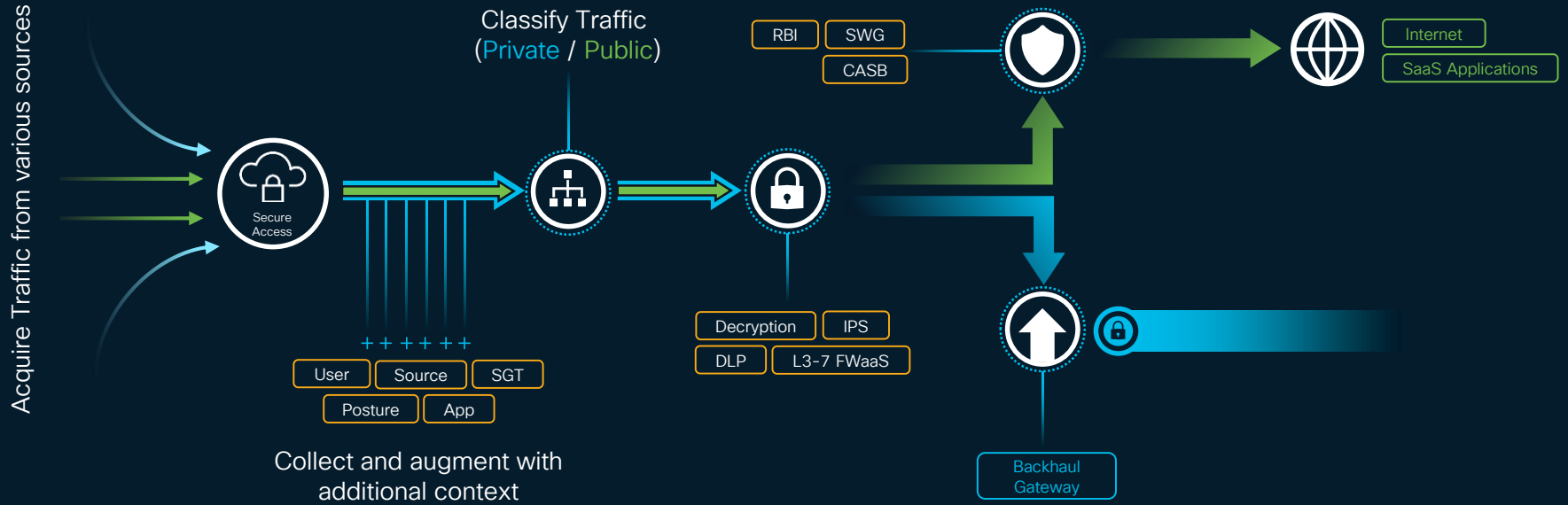
Tunnel Connectivity (DIA w/ Catalyst SD-WAN)



- Automatically Connect DIA Branches
- Secure all internet traffic through Secure Access

Unified Cloud Architecture

Universal Traffic Acquisition & Single Data Path

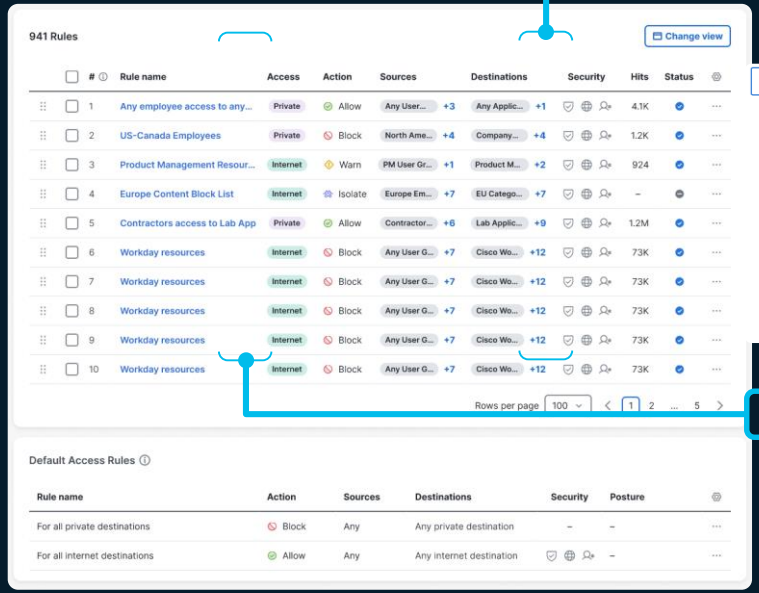


Unified Cloud Architecture

Consistent Policy & Security

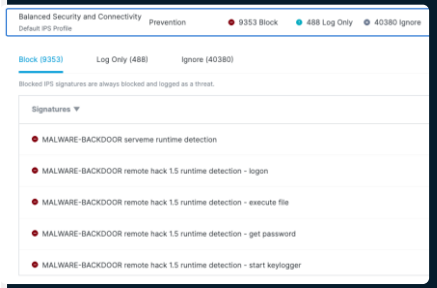
Secure Access

Unified Policy Evaluation



Consistent Security Enforcement

- Transit agnostic
- Private & Internet enforcement
- Per application / destination



Full IPS

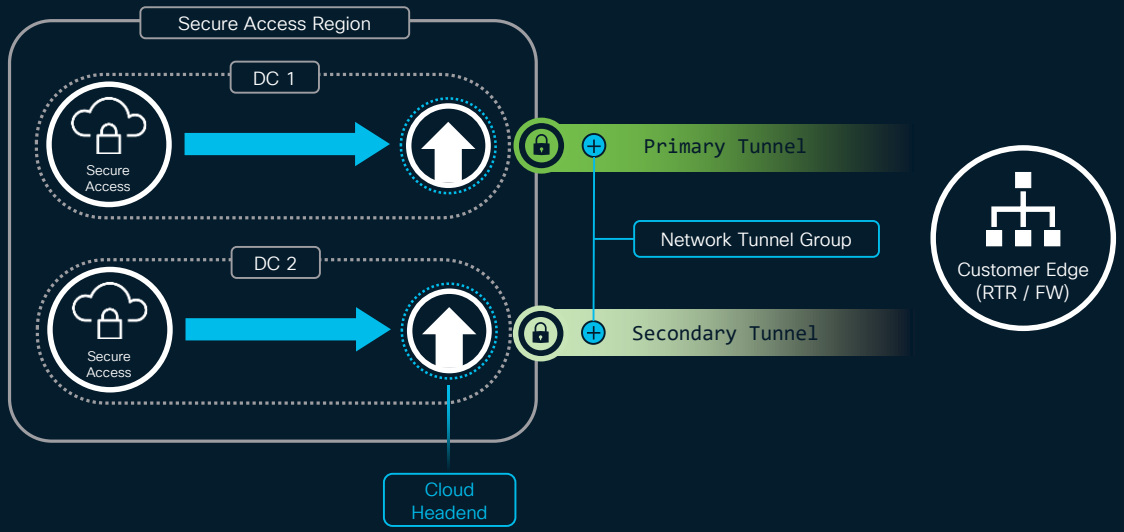
- Built on Snort 3.0
- Complete Signature Set
- TALOS updated

Unified Internet + Private Policy

- Single view of all access
- Filter and sort view
- No need to pivot

Connectivity

IPSec & SD-WAN Tunnels



Performance

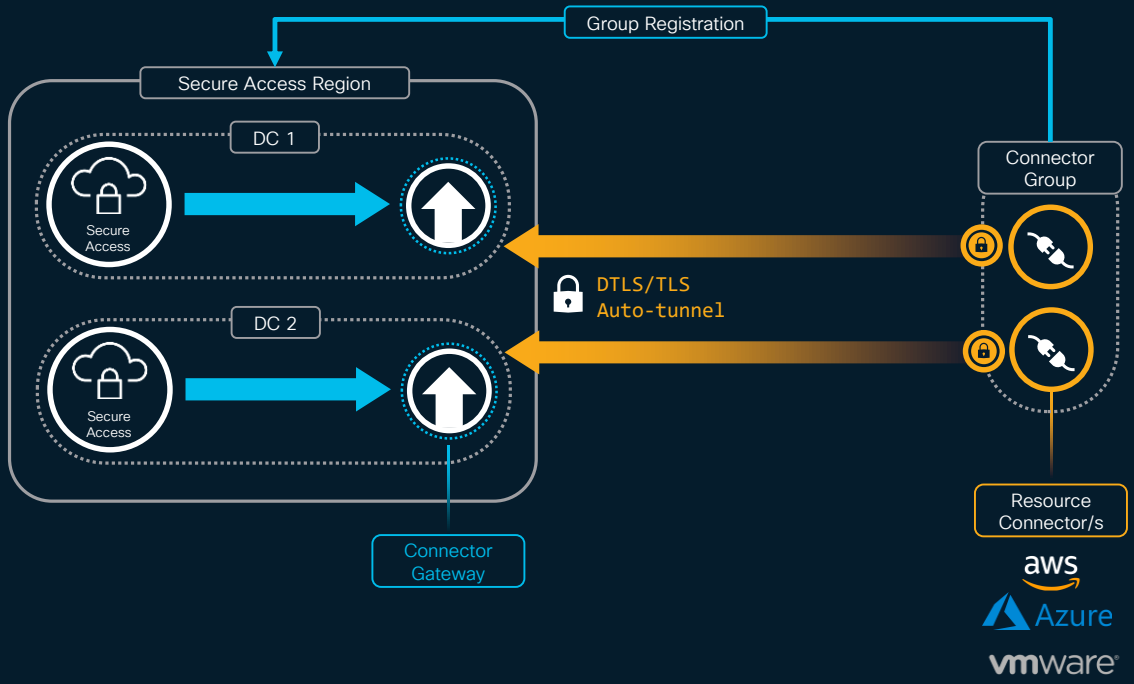
- IPsec Support for any hardware
- Intra-DC Failover
- IKE Dead Peer Detection
- BGP Keep Alive
- ECMP (Across multiple tunnels)
- Up t0 8x Tunnels per group
- 1Gbps / Tunnel

Routing

- Static Routes – manually configured
- VPN Pool & CGNAT return routes required
- BGP Peering, 1 neighbor per tunnel

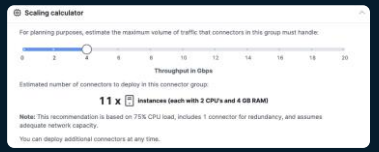
Connectivity

Resource Connectors



Performance

- Cloud side load balancing intra group + region
- 2x Connector / group recommended
- Cloud Managed (add/revoke/disable)
- Horizontal Scaling inside group
- 500Mbps / Connector

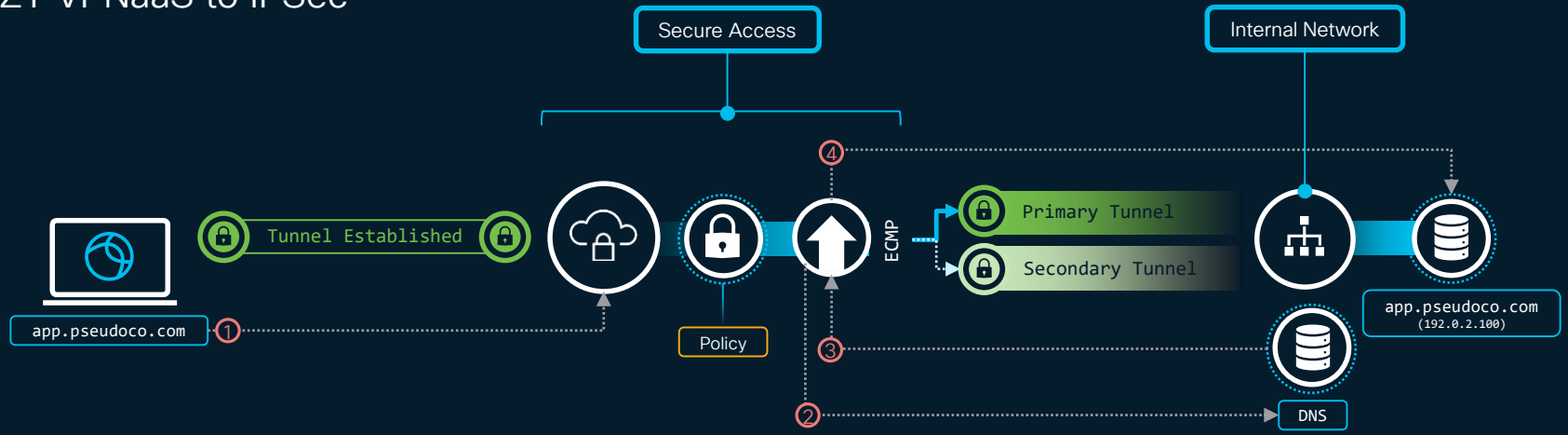


Routing

- Network Agnostic
- Support overlapping IPs

Example - End to End

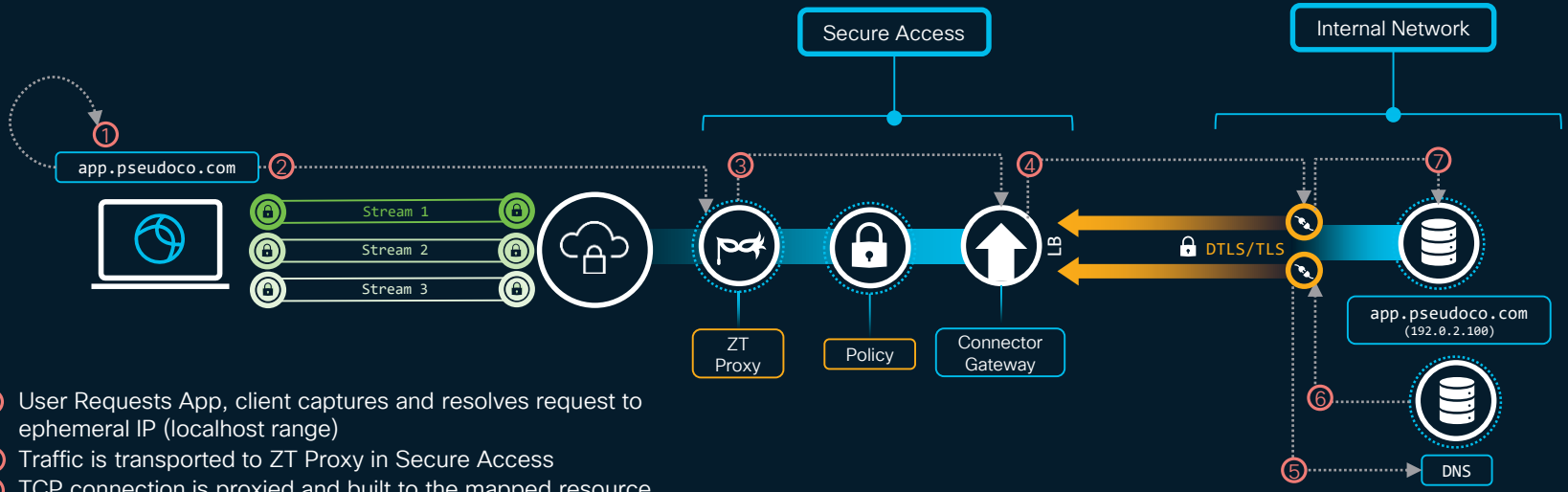
ZT VPNaaS to IPSec



① User Connected to VPNaaS requests App, traffic sent down Tunnel
② Secure Access Requests DNS resolution from internal DNS
③ Secure Access receives IP Address and Evaluates Policy
④ Secure Access routes traffic via Tunnel to App

Example - End to End

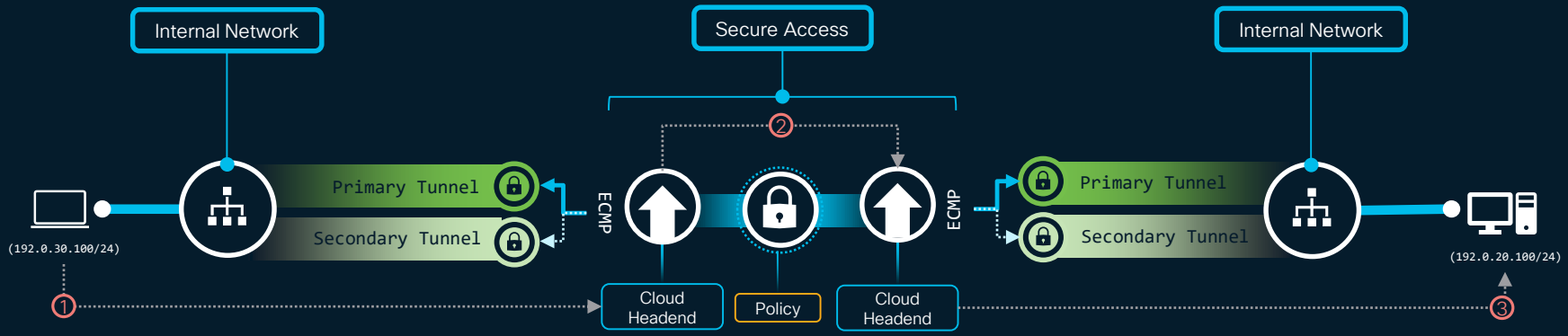
Zero Trust Access to Resource Connectors



1. User Requests App, client captures and resolves request to ephemeral IP (localhost range)
2. Traffic is transported to ZT Proxy in Secure Access
3. TCP connection is proxied and built to the mapped resource connector, Policy is enforced on traffic
4. Gateway establishes connection to resource connector
5. Resource connector resolves APP IP
6. Local DNS responds with App IP
7. Resource connector establishes connection to App

Example - End to End

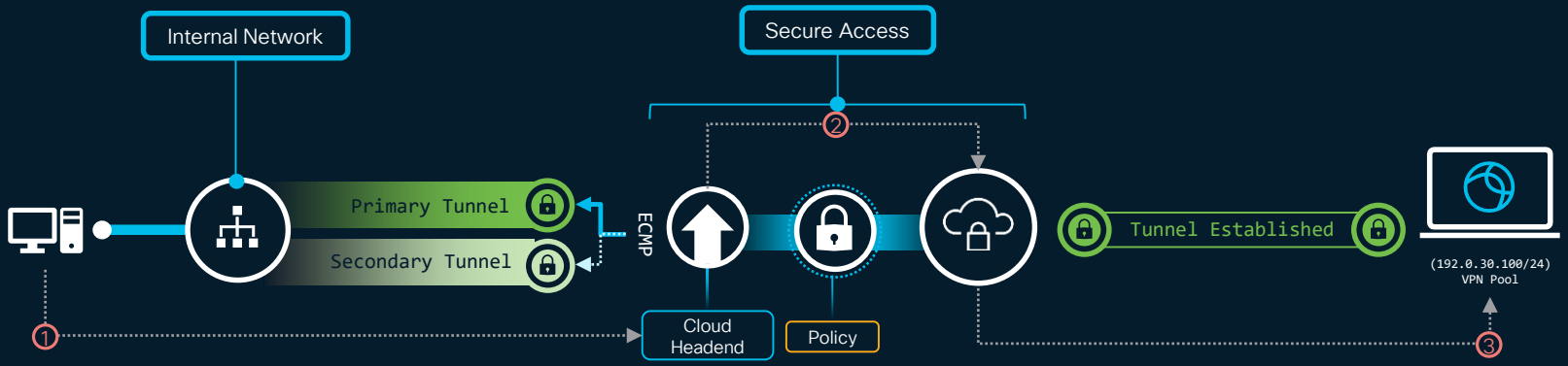
Branch / DC to Branch / DC



1. User on site requests IP in a different site, traffic is routed to Secure Access
2. Secure Access enforces policy
3. Secure Access directs traffic down to second site to destination IP

Example - End to End

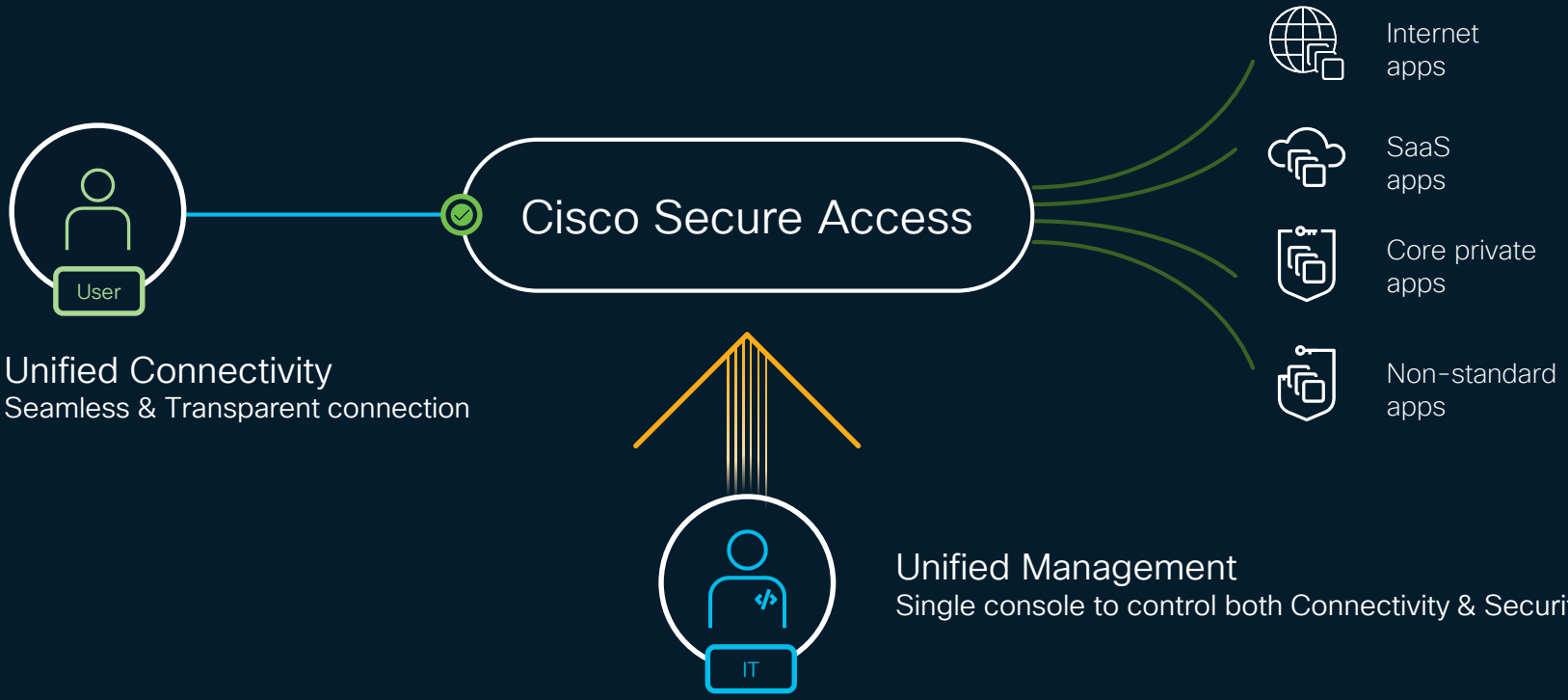
Branch / DC to VPNaaS User



① User on site requests IP of a roaming User, traffic is routed to Secure Access
② Secure Access enforces policy
③ Secure Access directs traffic through VPN Tunnel to destination endpoint (VPN Pool IP)

Cisco Secure Access

Unified Platform

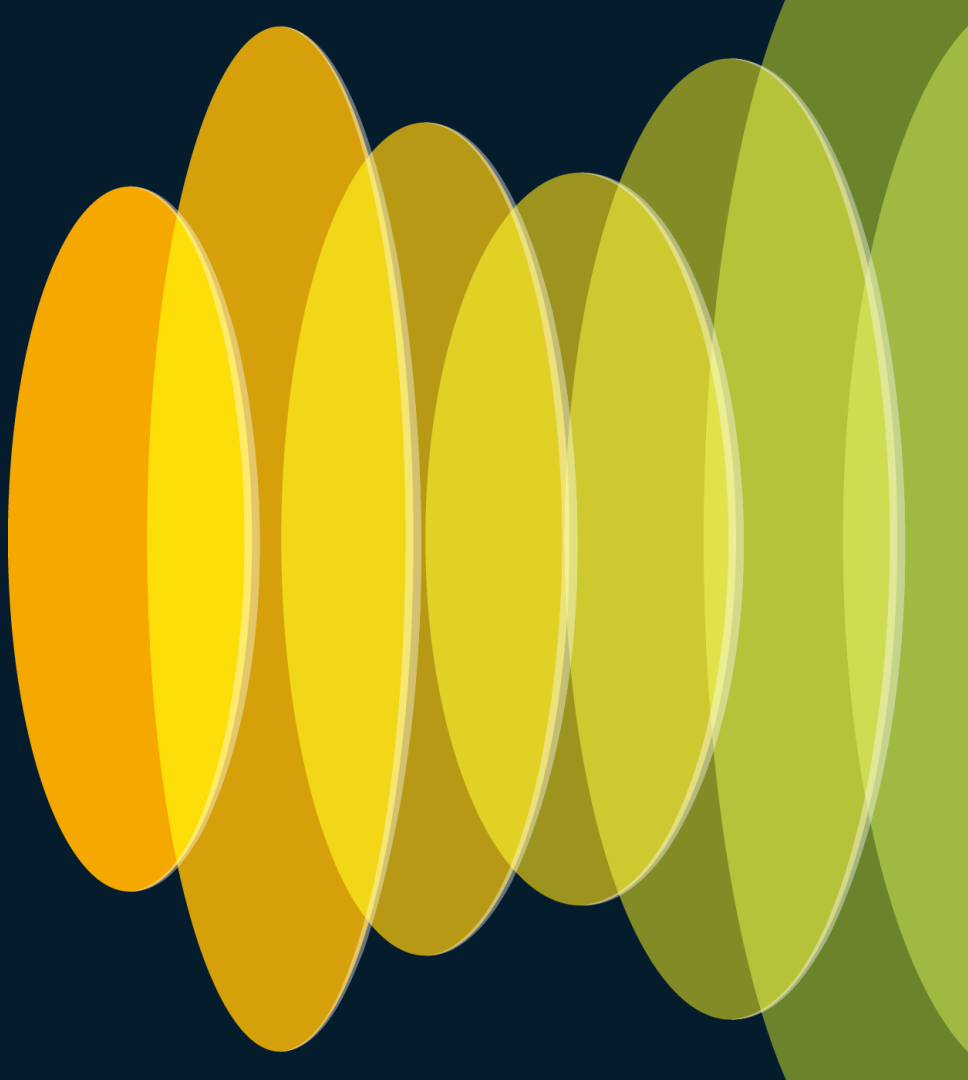


Unified Connectivity
Seamless & Transparent connection

Unified Management
Single console to control both Connectivity & Security

Latest Innovations

All new!



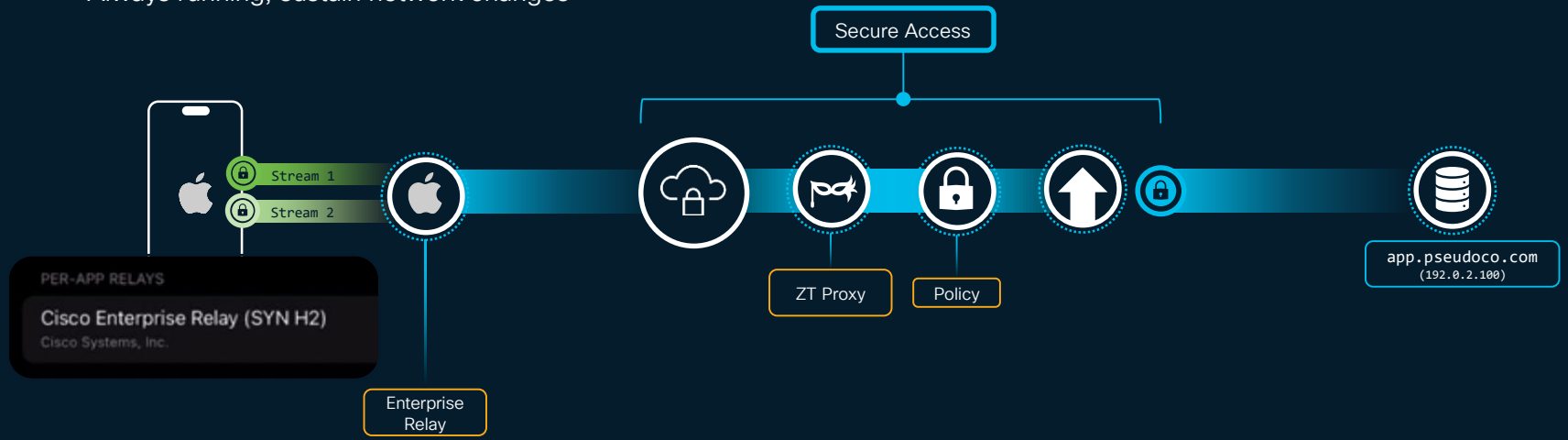
cisco Live!

iOS Native Zero Trust

Apple + Cisco Enterprise Relay (iOS 17 +)

Native Experience

- Co-Developed with Apple
- Native Connectivity without VPN
- Per App visibility & connectivity
- Consistent experience PC/ MAC/ iOS
- Always running, sustain network changes

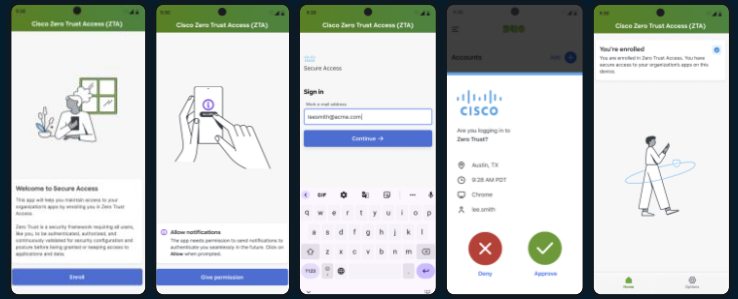


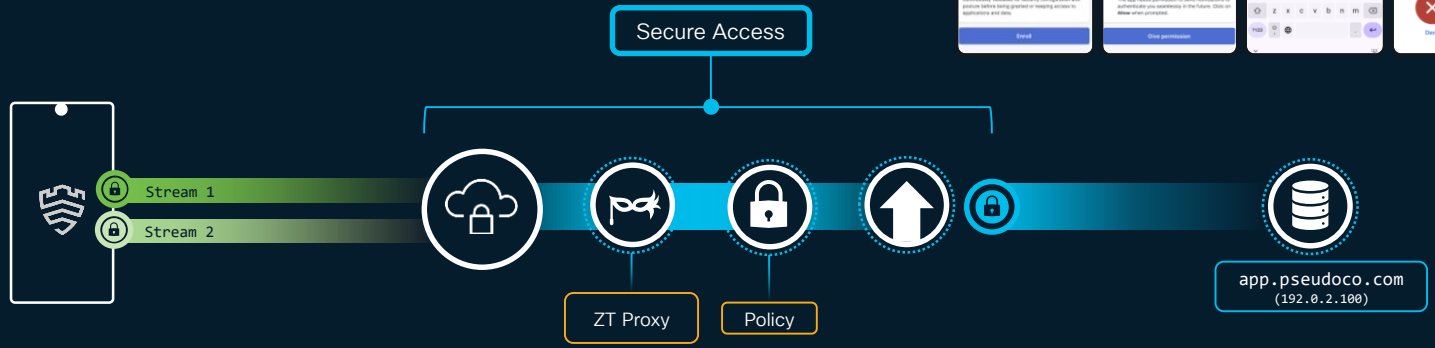
Android Native Zero Trust

Samsung Knox framework + Cisco (Knox 3.10 +)

Consistent Policy

- Native connectivity to secure access
- No VPN required
- Deeper device integration resulting in better performance
- More efficient use of resources
- Per application control all ports and protocols
- Sustain network changes, seamlessly



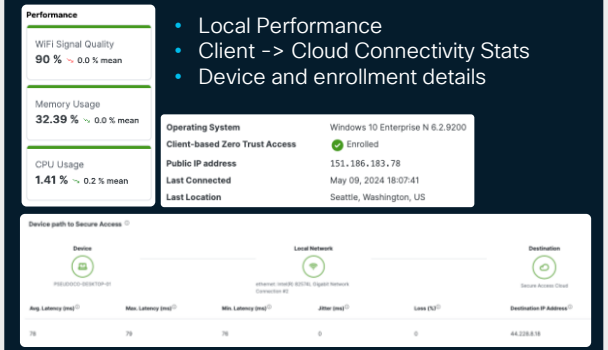


Digital Experience Insights

End to end visibility

Client Connectivity

- Local Performance
- Client -> Cloud Connectivity Stats
- Device and enrollment details

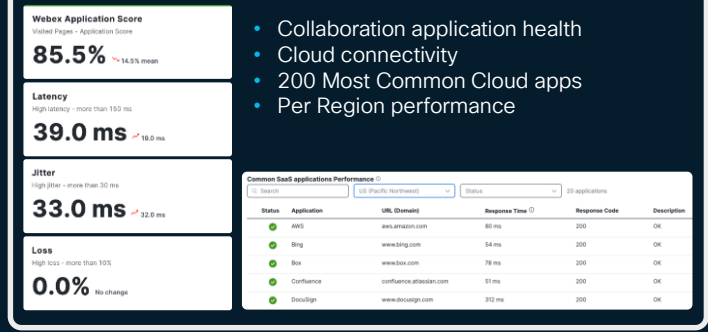


User Actions

- User based activity trends
- Active policy enforcement

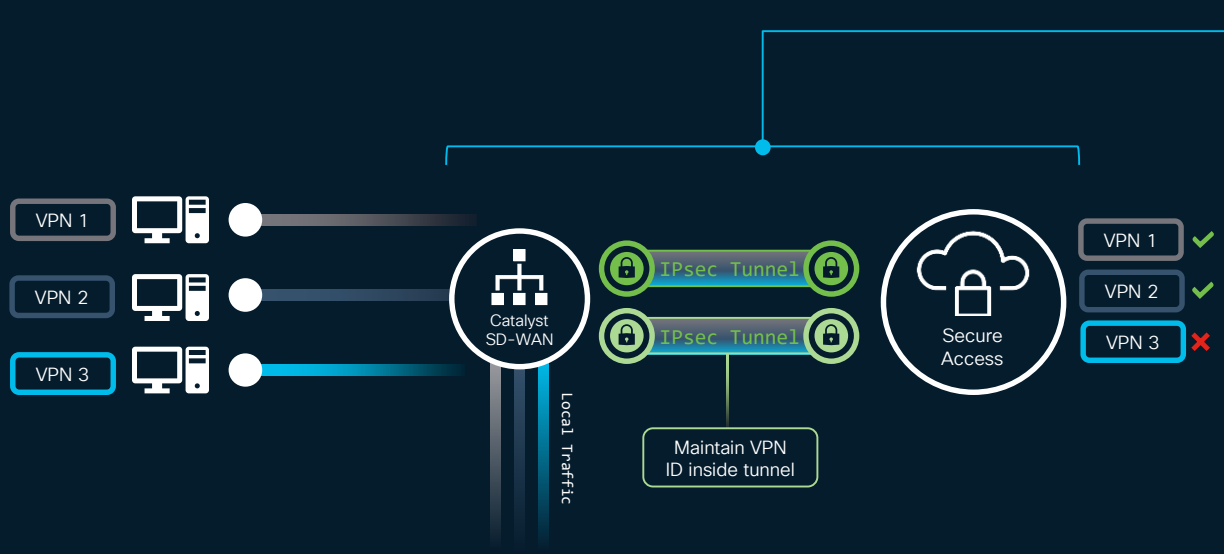
Cloud Connectivity

- Collaboration application health
- Cloud connectivity
- 200 Most Common Cloud apps
- Per Region performance



Catalyst SD-WAN

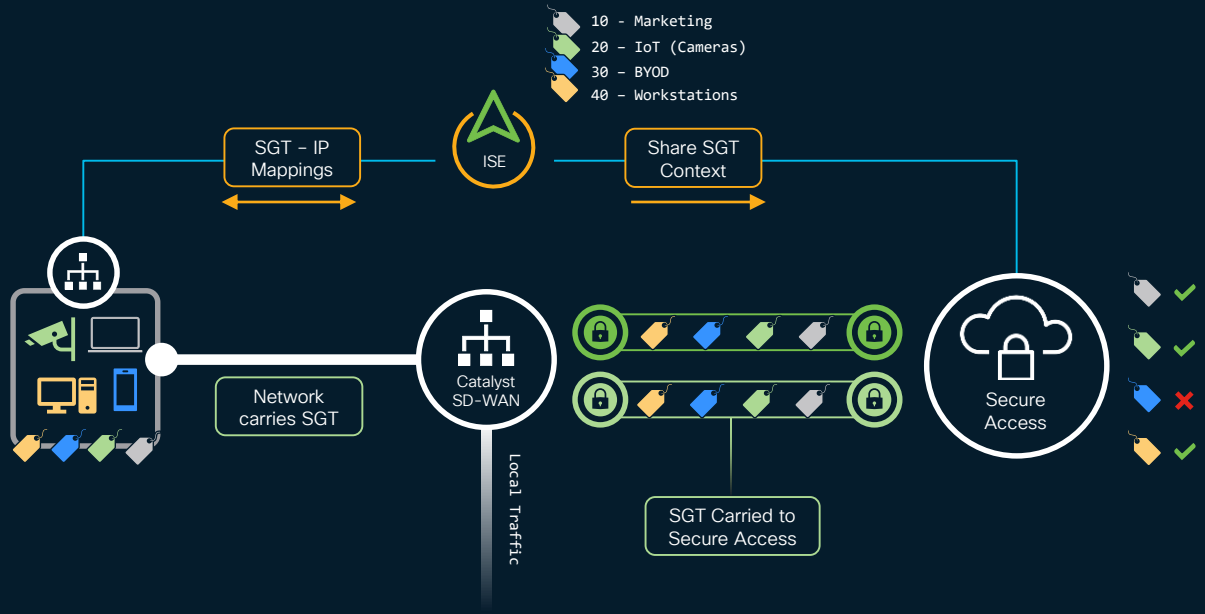
VPNID support for consistent segmentation



- VPNID Based policy across both SDWAN & Secure Access
- Maintain Segmentation in branch & in the cloud
- Universal support across Catalyst & Viptela SD-WAN

Identity Services Engine

SGT Support for consistent policy and enforcement

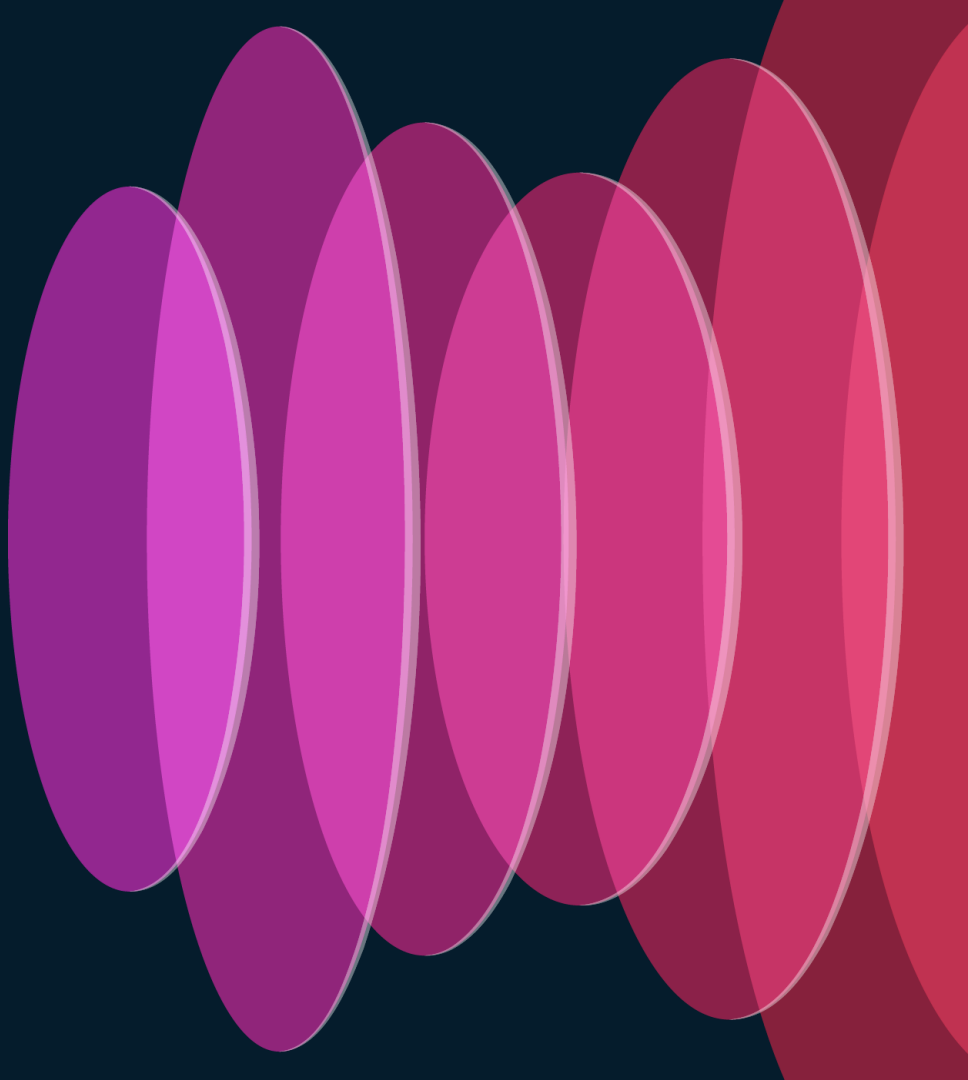


Consistent Policy

- 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

A.I.

Streamlined Experiences

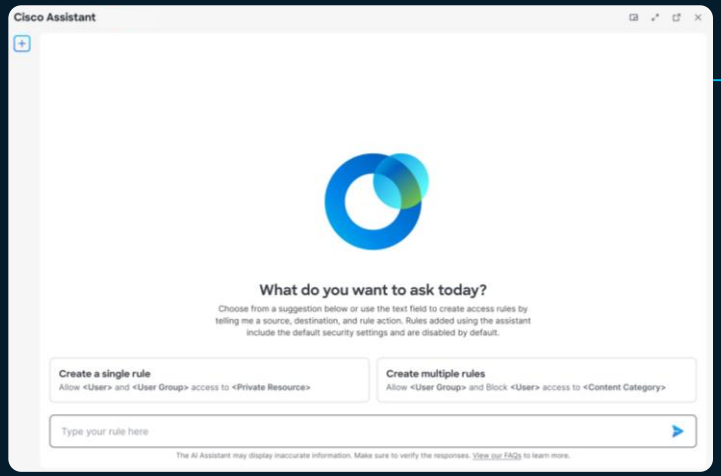


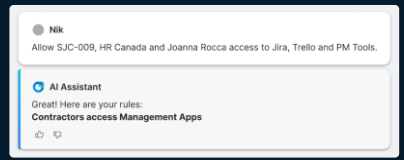
Policy Assistant

Let AI do the heavy lifting

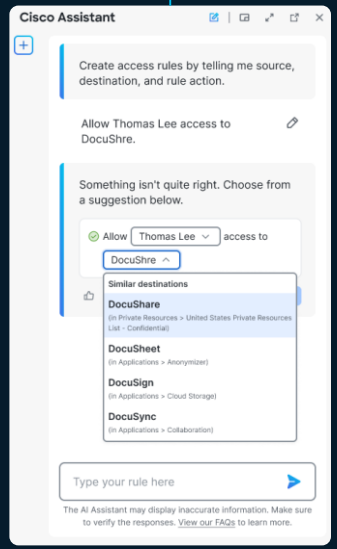
Simplified Experience

- Infer Required access based on language input at prompt
- Reduce rule creation time by up to 70%
- Default disable to ensure administrator has ability to review generated content





Intelligent Interaction

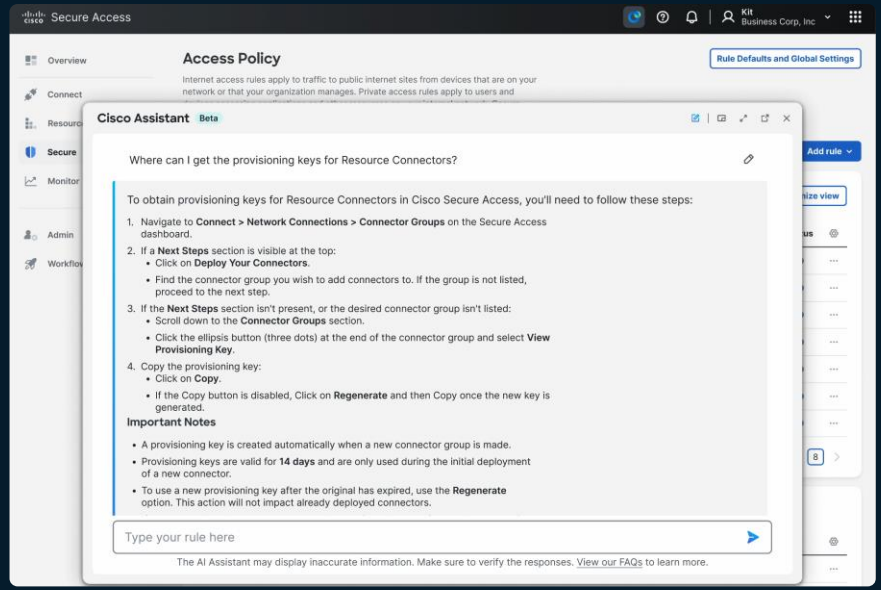


Documentation Assistant

All the answers (about secure access) at your fingertips

Ease of Use

- Personalized answers based on conversation
- Complete knowledge of Secure Access and its features
- Guide you with process or explain features
- Provide caveats and disclaimers when necessary
- We are used to keyword matches – it's a skill, but now we don't need to worry about that

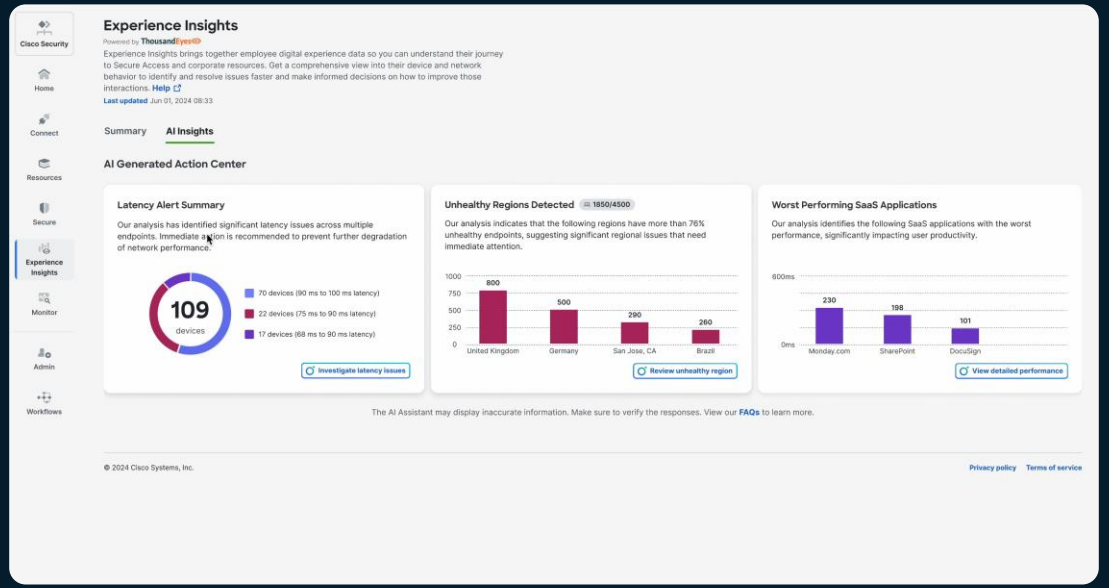


Digital Experience AI Assistant

All the answers (about secure access) at your fingertips

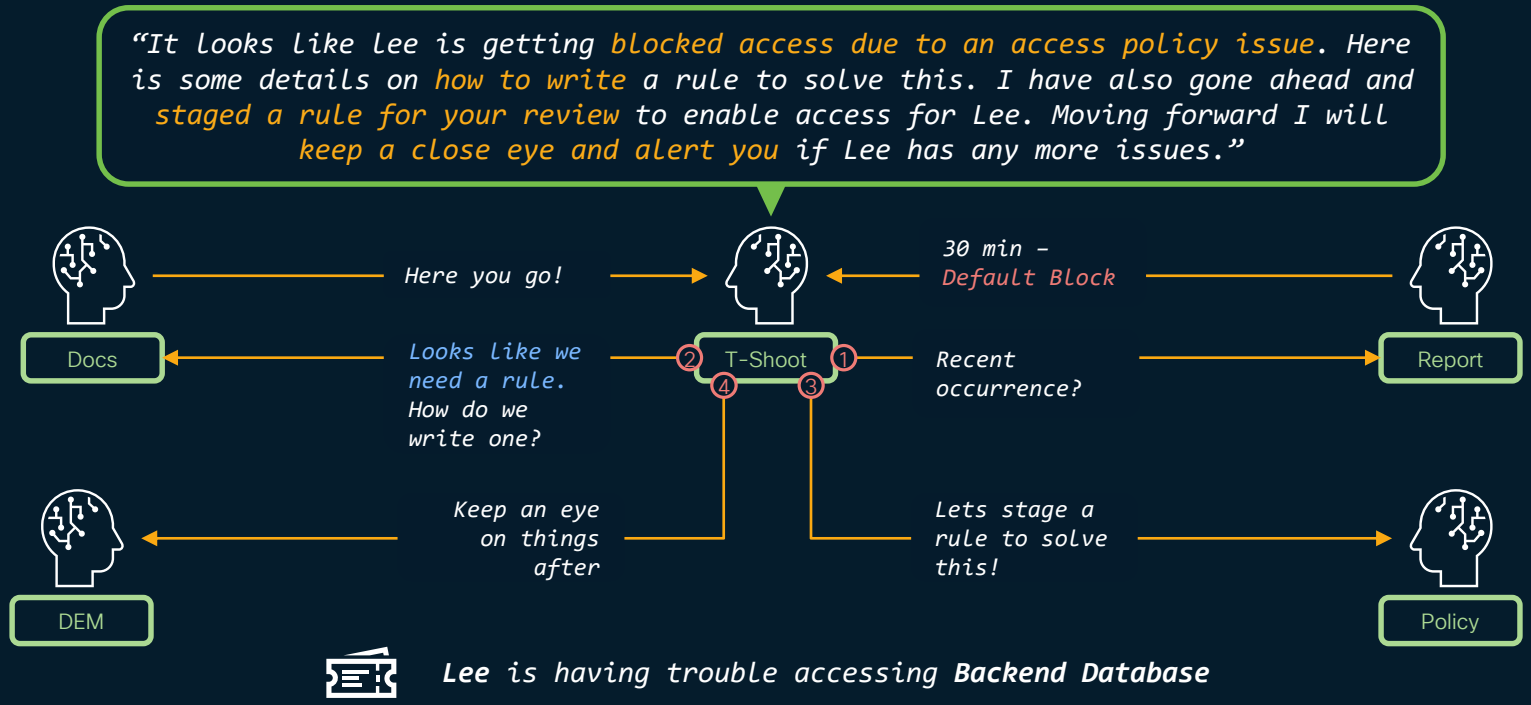
Understand and React

- Grouped Alerting
- recommended actions and additional templated details when relevant
- Interact with assistant to dive deeper without needing to pivot



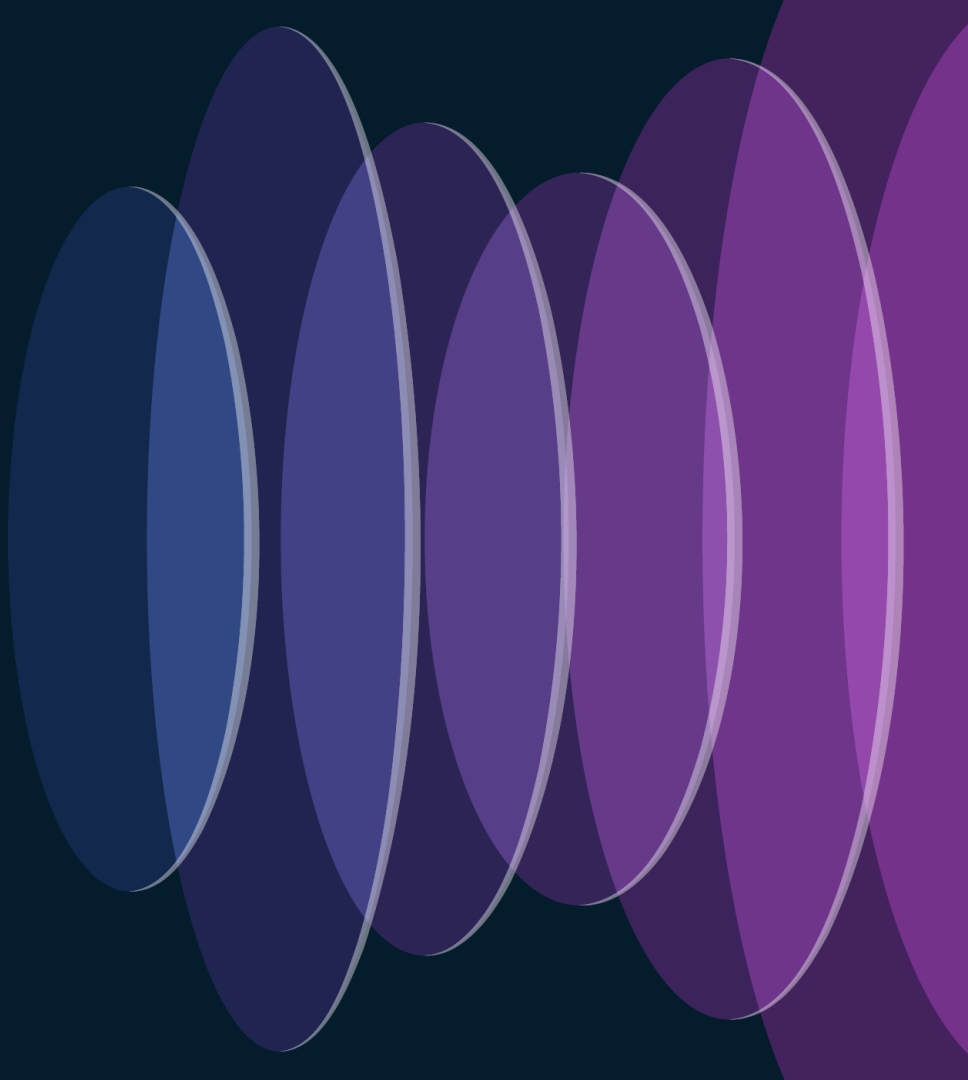
Complete AI Assistant

Coming together to create exponential value



Vision

Building atop a strong Foundation

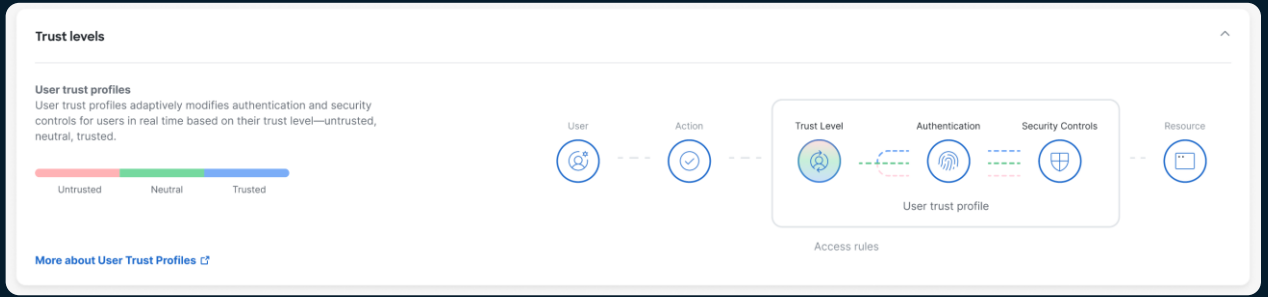


Cisco Identity Intelligence

Additional User Context augmented Zero Trust

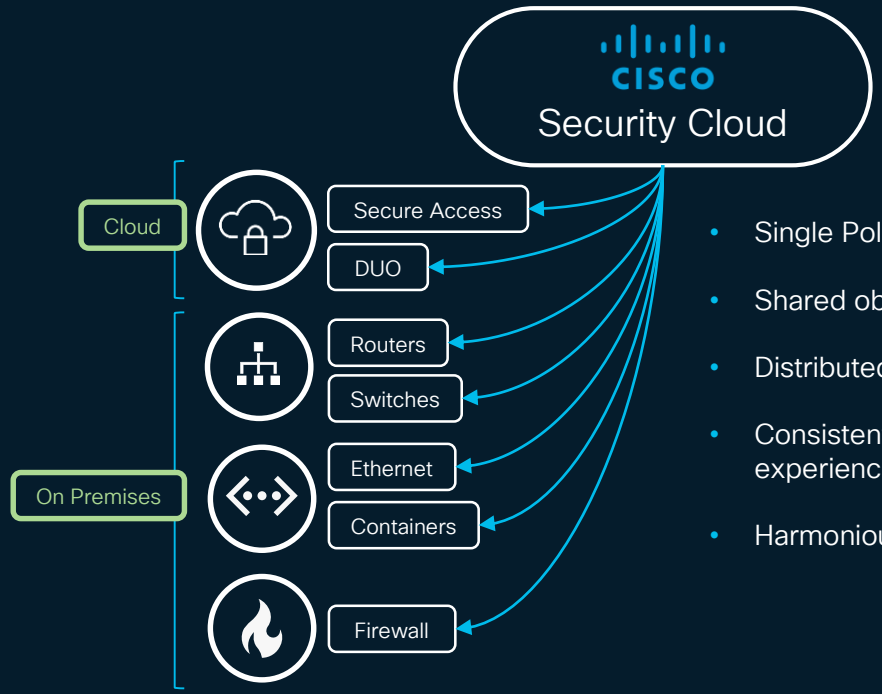
Trust Levels

- Derived from behavior and client signals
- Correlate across multiple identity providers
- Dynamically change access when trust level changes
- Create a “gradient” of control based on trust and desired inspection



Cisco Security Cloud

A Single Policy, Consistent Experience w/ Distributed Enforcement



- Single Policy in the Security Cloud
- Shared objects and context
- Distributed enforcement across data plane
- Consistent and optimized end user experience
- Harmonious AI Assistants

Fill out your session surveys!

Complete a minimum of 4 session surveys and the Overall Event Survey to be entered in a drawing to **win 1 of 5 full conference passes** to Cisco Live 2025.

Earn 100 points per survey completed and compete on the Cisco Live Challenge leaderboard.

Level up and earn **exclusive prizes!**

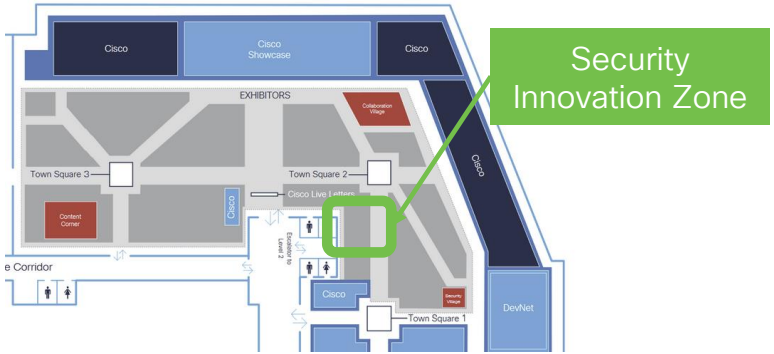
Complete your surveys in the **Cisco Live mobile app.**

Continue your education

- Hear Tom Gillis at the Security Deep Dive Keynote KDDSEC-1000!

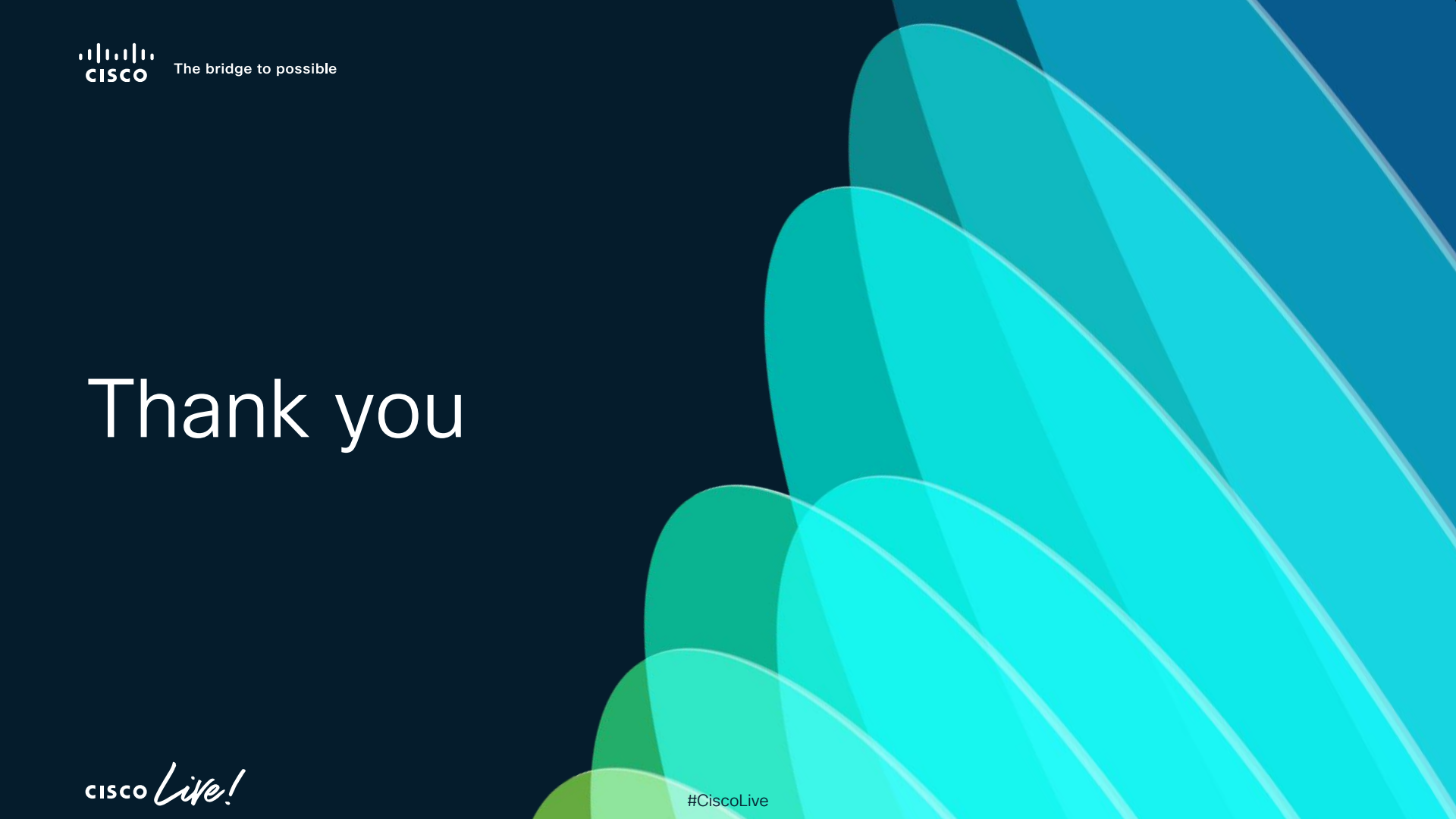
  Securing User to Application and Everything in Between
  Wednesday, June 5 | 1 – 2pm

- Visit us at the Security Innovation Zone (#4435) for demos and workshops



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!
#CiscoLive