Let's go

The bridge to possible

Cisco Secure Access

Overview and End-to-end flow review

Jonny Noble – Director, Technical Marketing
@JonnyNoble3

BRKSEC-1708

“Reconciliation” - Dustin Koa Art

cisco

Cisco Webex App

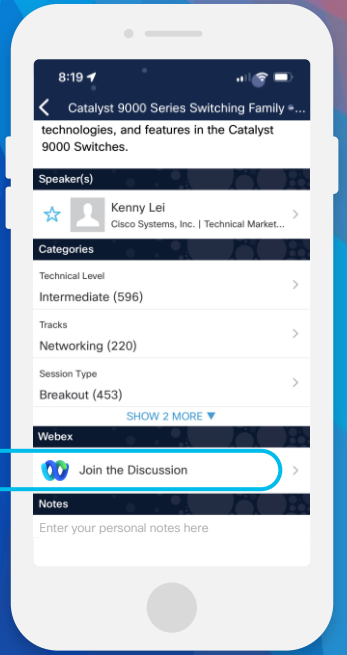
Questions?

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 December 22, 2023.



https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-1708

Abstract

- This session provides an end-to-end introduction and overview for Cisco's latest Security Service Edge solution, Cisco Secure Access
- We will take a closer look at the latest innovations in Cisco's Secure Service Edge (SSE), including new ZTNA client-based and clientless capabilities, simplified policy management, and a unified client that will remove the frustration of securely connecting for your hybrid workforce, all coming together to protect your users and applications
- The session will start by defining the current challenges enterprises are facing and the use cases that Cisco Secure Access solves, followed by an overview of the architecture, a deep dive on the flow of data for the supported use-cases for secure internet and private access, what differentiates this solution from others in the market, concluding with a look at the dashboard and end-user experience
- Ample time will be kept for QA and an open discussion with the audience

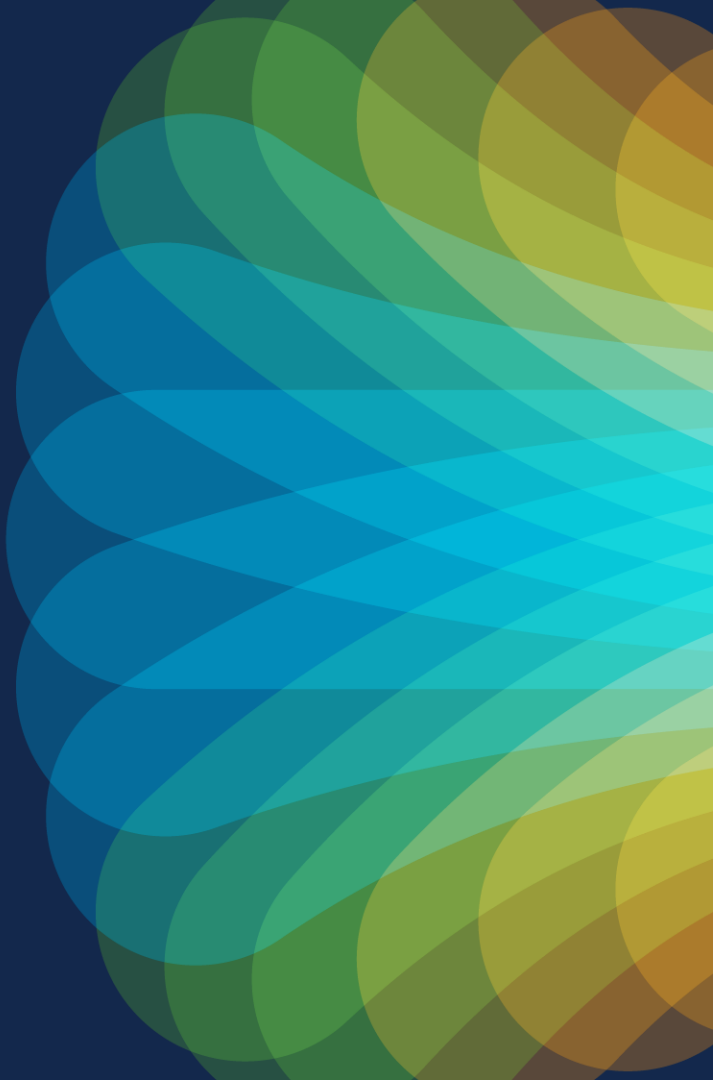
Jonny Noble - About me...

- I am Director of Technical Marketing for Cloud Security at Cisco, with expertise in Secure Service Edge and surrounding SASE-related technologies
- I am focused on cyber-security and have over 25 years of vast experience in customer-facing disciplines in leading global hi-tech organizations
- I am a seasoned speaker at Cisco Live events and regularly represent Cisco at numerous other customer and partner events, trade shows, and exhibitions
- I hold degrees in Electronics, Sociology, a Business MBA, and am CISSP certified

Agenda

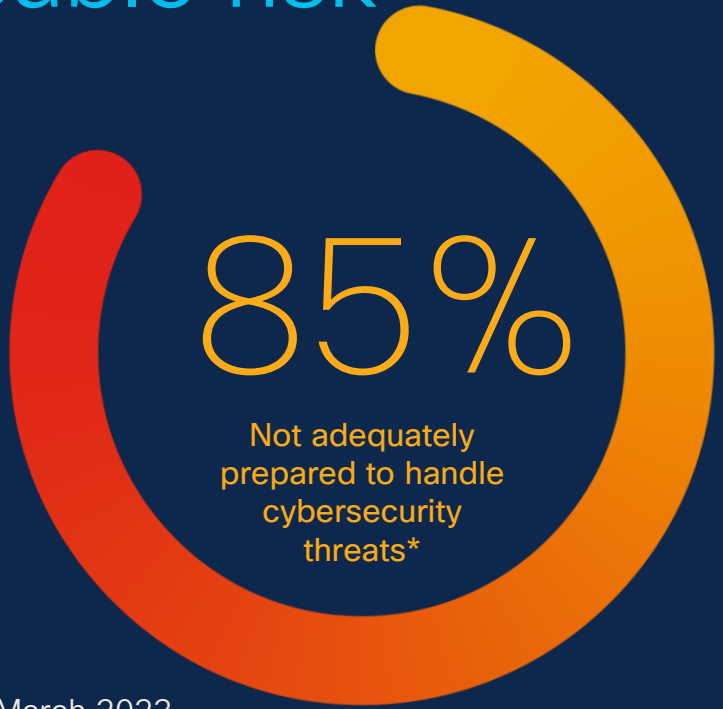
- Session Introduction
- Setting the scene for Cisco Secure Access
- What have we built?
- Architecture and flow
- Demos
- Q&A and summary

Let’s set the scene, and session expectations



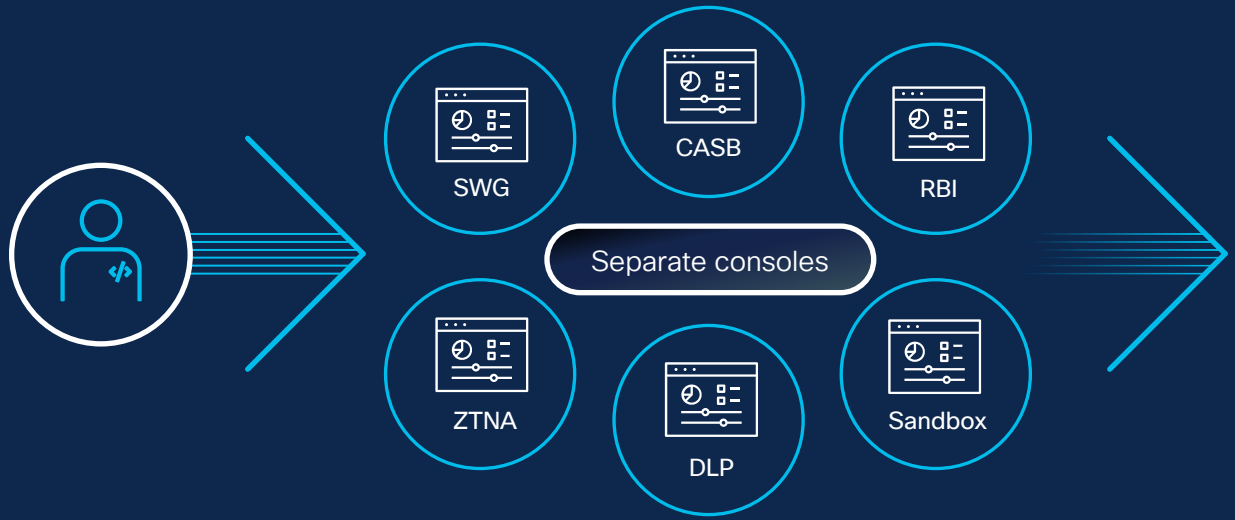
Hybrid work era creates unmanageable risk

Your organization's security wasn't designed for a hyper-distributed model



* Source: Cybersecurity Readiness Index – Cisco: March 2023

The multi-vendor approach is problematic



Internet apps

SaaS apps

Core private apps

Longtail/non-standard apps


Lookout
COALFIRE
red canary
clearswift
proofpoint
solarwinds
sophos
Ping Identity
deepwatch
paloalto
hackerone
axio
GoGuardian
NowSecure
DARKTRACE
CROWDSTRIKE
VARONIS
RAPID7
KnowBe4
U410
passbase
Prove
CHECK POINT
FusionAuth

Current patchwork approach intensifies the problem

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

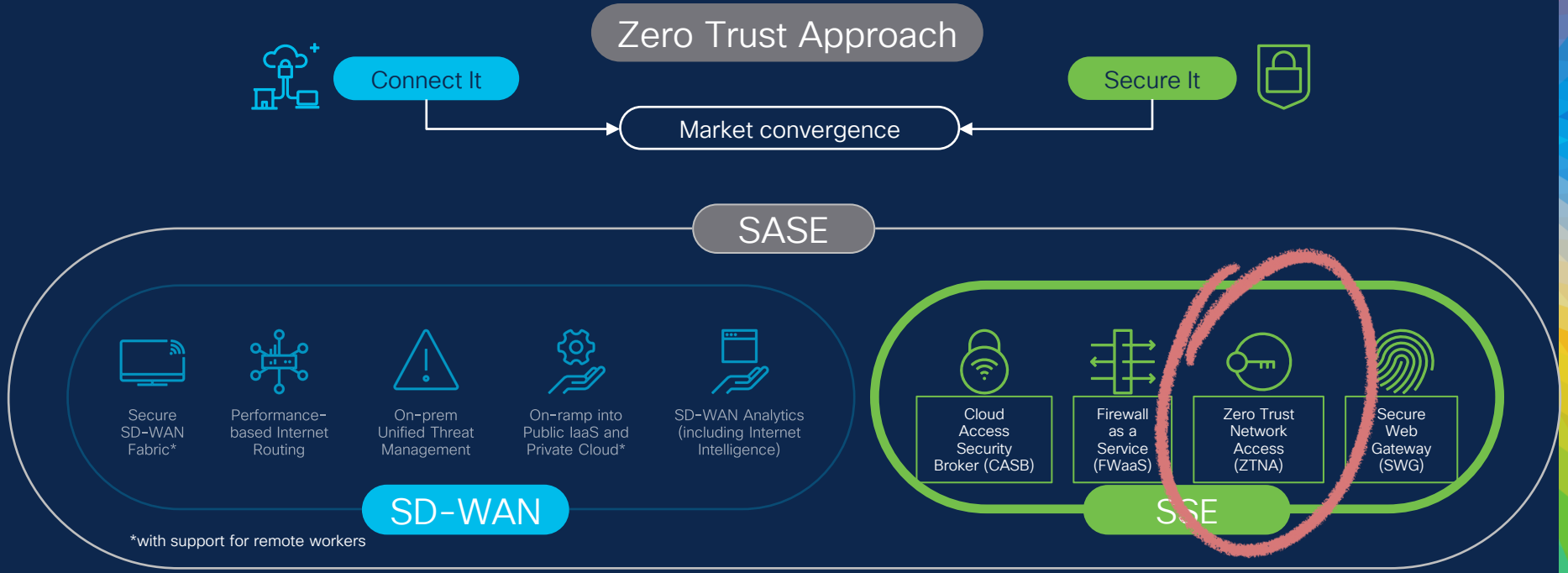
New threats spawn new vendors, putting the burden on customers

Customer care-abouts

Visibility and Control	No visibility in direct-to-Internet traffic. Siloed, disaggregated dashboards
Simplified Remote Access	Many on-prem, private applications. Need for simplified end user experience
ZTNA is a journey	Need user access control, security posture management, application and user group policies
Segmentation	Granular segmentation and zero trust policies for applications

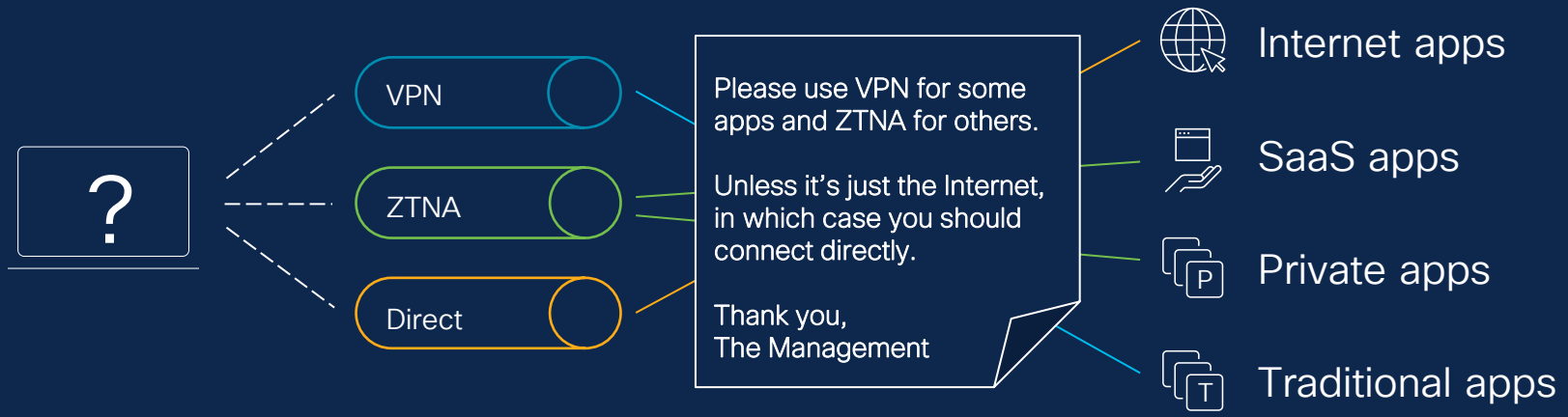
SASE/SSE approach is the technology foundation

Fundamental to your security strategy for a hyper-distributed world



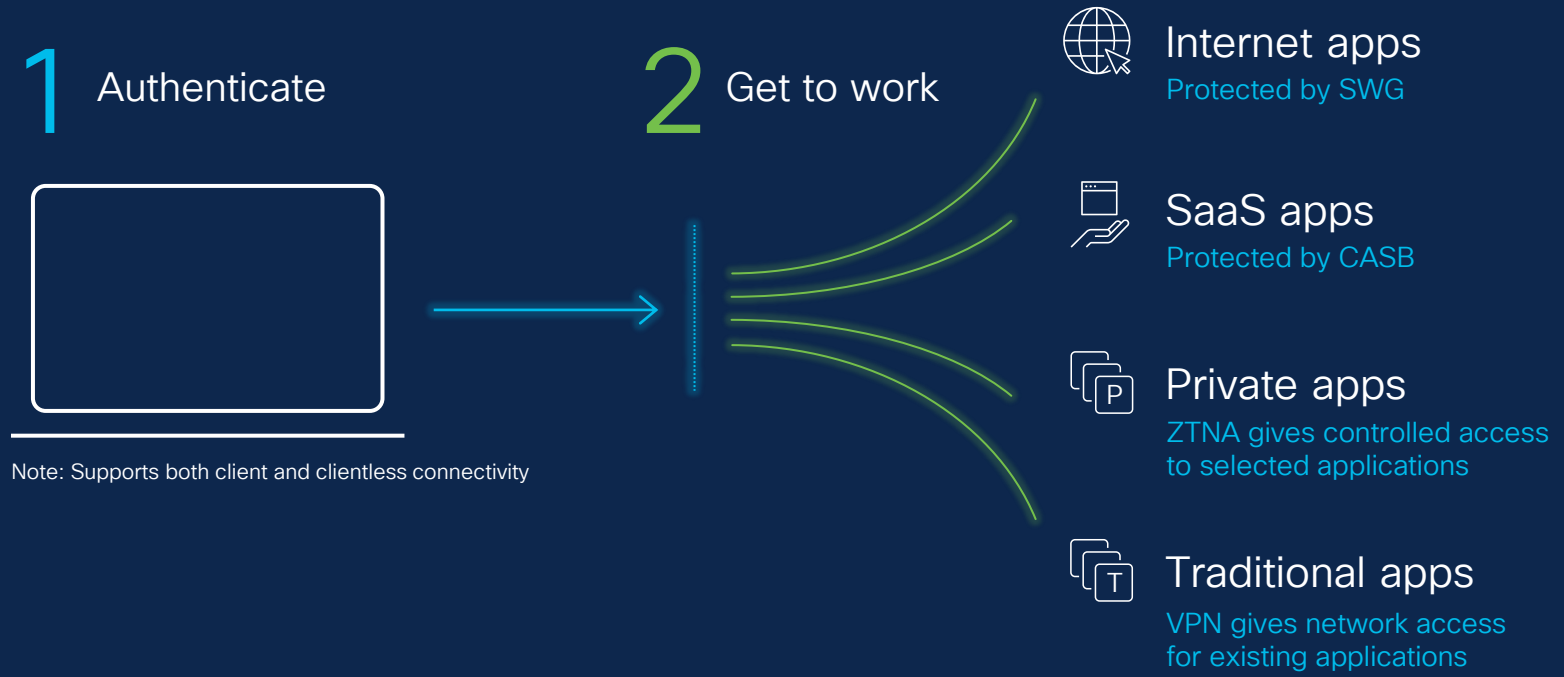
Eliminate unnecessary decisions

How would you like to connect to your applications?



Reimagine the user experience:

Cisco Secure Access makes the connections you need



What have we built?

Cisco Secure Access

Better for users, easier for IT,
and safer for everyone

Cisco Secure Access

Modernize your defense with converged cloud security in a single subscription

Better for Users

Facilitate a frictionless workforce experience

Easier for IT

Lower cost and increase efficiencies

Safer for Everyone

Reduce risk and improve business resilience

Imagine cybersecurity that's

safer and easier for everyone

Unique secure access that is easier and safer for everyone...

From anywhere

Remote users

Managed and unmanaged devices

Cisco Secure Access

Better for Users
Exceptional User Experience

Users Login and get to work

Easier for IT
Simplified IT Operations

IT has one dashboard to see traffic, set policies, and analyze risk

Safer for Everyone
Tighter Security

Converged, cloud-native security defends against the unknown

Converged cloud-native security on a single platform

To anything

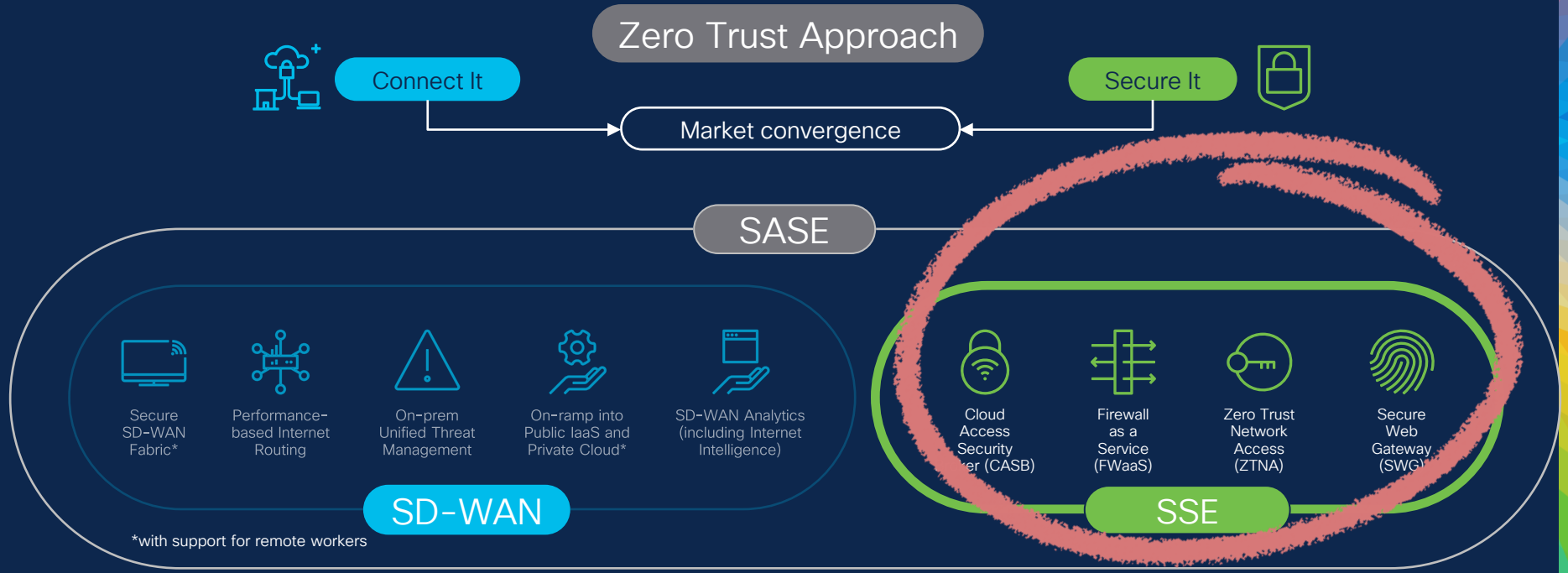
Web

Public SaaS apps

Private apps

SASE/SSE approach is the technology foundation

Fundamental to your security strategy for a hyper-distributed world



Cisco Secure Access

A comprehensive Security Service Edge (SSE) solution to accelerate your SASE journey

Core SSE Capabilities

Firewall as a Service (FWaaS)

+

Secure Web Gateway (SWG)

+

Cloud Access Security Broker (CASB)

+

Zero Trust Network Access (ZTNA)

and so much more in one subscription...

- Cisco SD-WAN integration
- 3rd party integrations (IdP, MDM (posture), and other security tools)
- Global scale with Cisco data centers and public cloud locations

Going beyond Core Security Service Edge

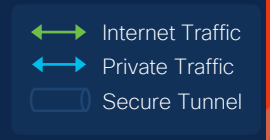
Cisco Secure Access

- VPNaaS
- Digital Experience Monitoring
- DNS Security
- Remote Browser Isolation
- Data Loss Prevention
- Advanced Malware Protection
- Sandbox
- Talos Threat Intelligence
- AI-powered Platform

Consolidate security into one cloud solution with a single subscription

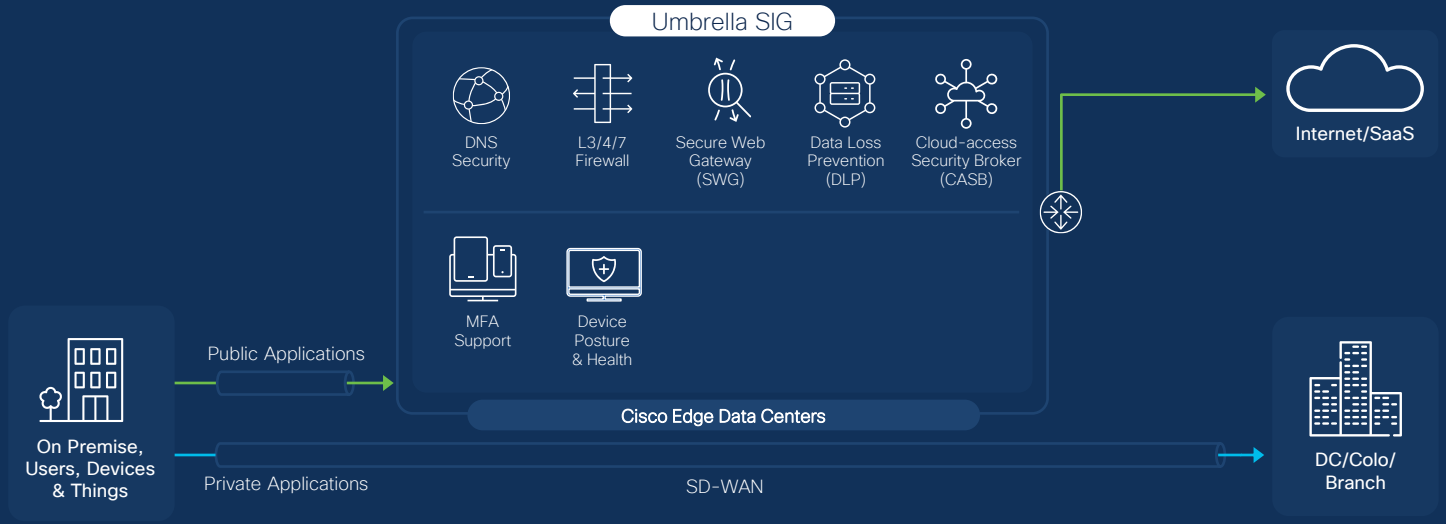
Architecture and flow drill-down

Evolution from Cisco Umbrella SIG

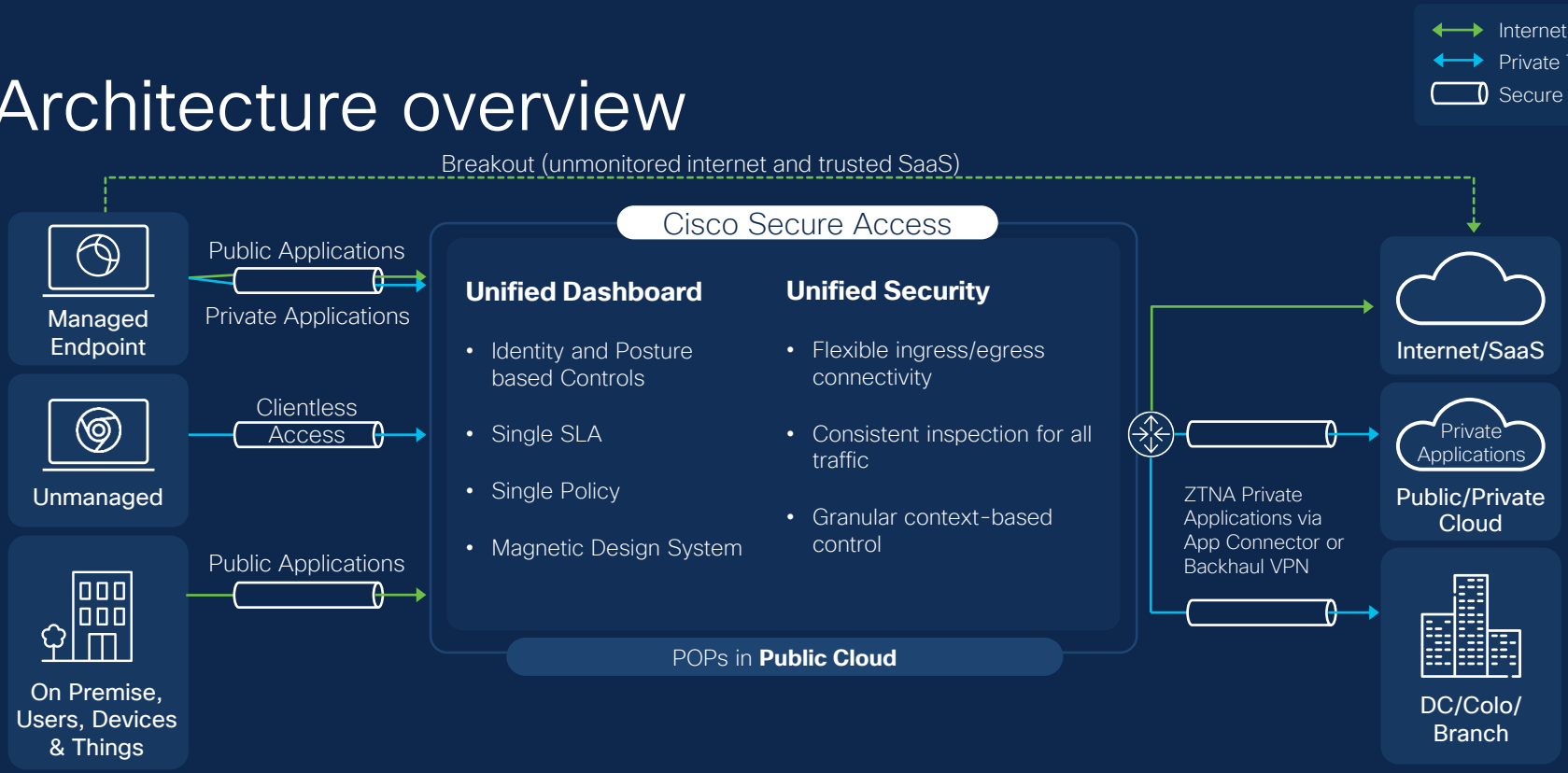


Main use-cases

- Secure Internet Access
- POPs in Cisco Edge Data Centers
- Meraki and Viptela SD-WAN Integration from DIA to SIA



Architecture overview



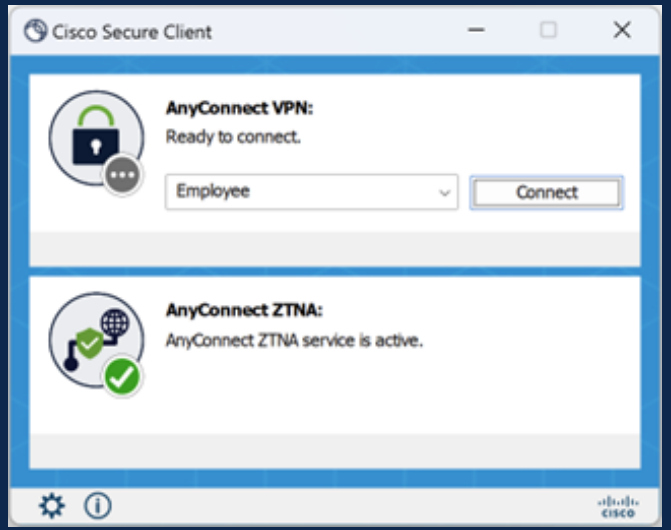
Users & Devices — **How** — **Apps**

Architecture overview: Who

Users & Devices — How — Apps

Zero Trust Access Module
New in Cisco Secure Client

- Transparent user experience
- Proxied resource access with coarse-grained or fine-grained access control
- Service managed client certificates with TPM/hardware enclave key storage
- Support for both TCP and UDP applications
- Cisco and third-party VPN client interop
- Next-generation protocol (QUIC & MASQUE)



What are QUIC and MASQUE?

QUIC (not an acronym)

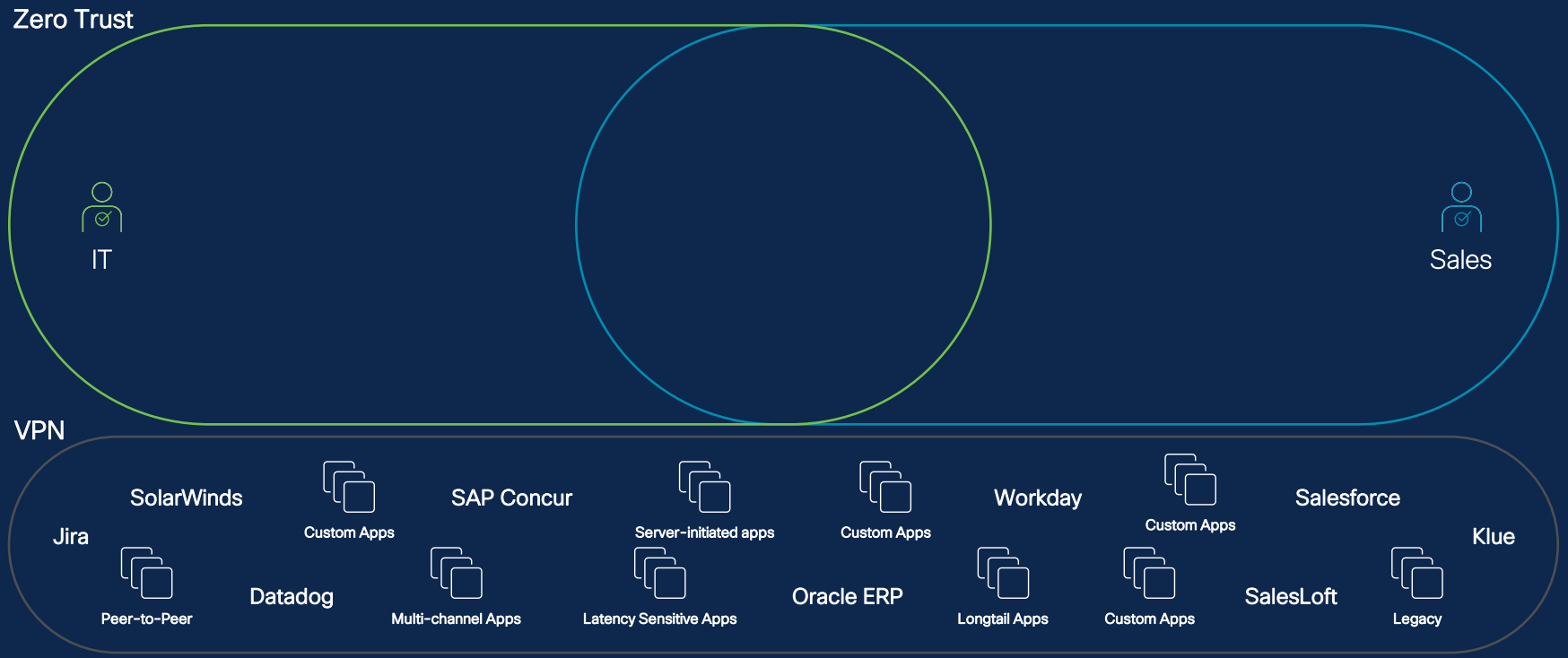
- UDP-based, stream-multiplexing, encrypted transport protocol
- First used in Google Chrome in 2012
- Used for HTTP/3, Apple iCloud Private Relay, SMB over QUIC, DNS over QUIC, etc.
- Optimized for the next generation of internet traffic with low latency and high capacity, compared to TLS over TCP
- Supports micro-tunnels

MASQUE (Multiplexed Application Substrate over QUIC Encryption)

- IETF working group focused on next generation proxying technologies on top of the QUIC protocol
- Provides the mechanisms for multiple proxied stream and datagram-based flows inside HTTP/2 and HTTP/3
- Used by iCloud Private Relay since 2021
- HTTP/2 and HTTP/3 extensions allow for the signaling and encapsulation of UDP and IP traffic

When combined, MASQUE + QUIC provides an efficient and secure transport mechanism for TCP, UDP and IP traffic for both web and non-web protocols

Challenges with the journey to Zero Trust

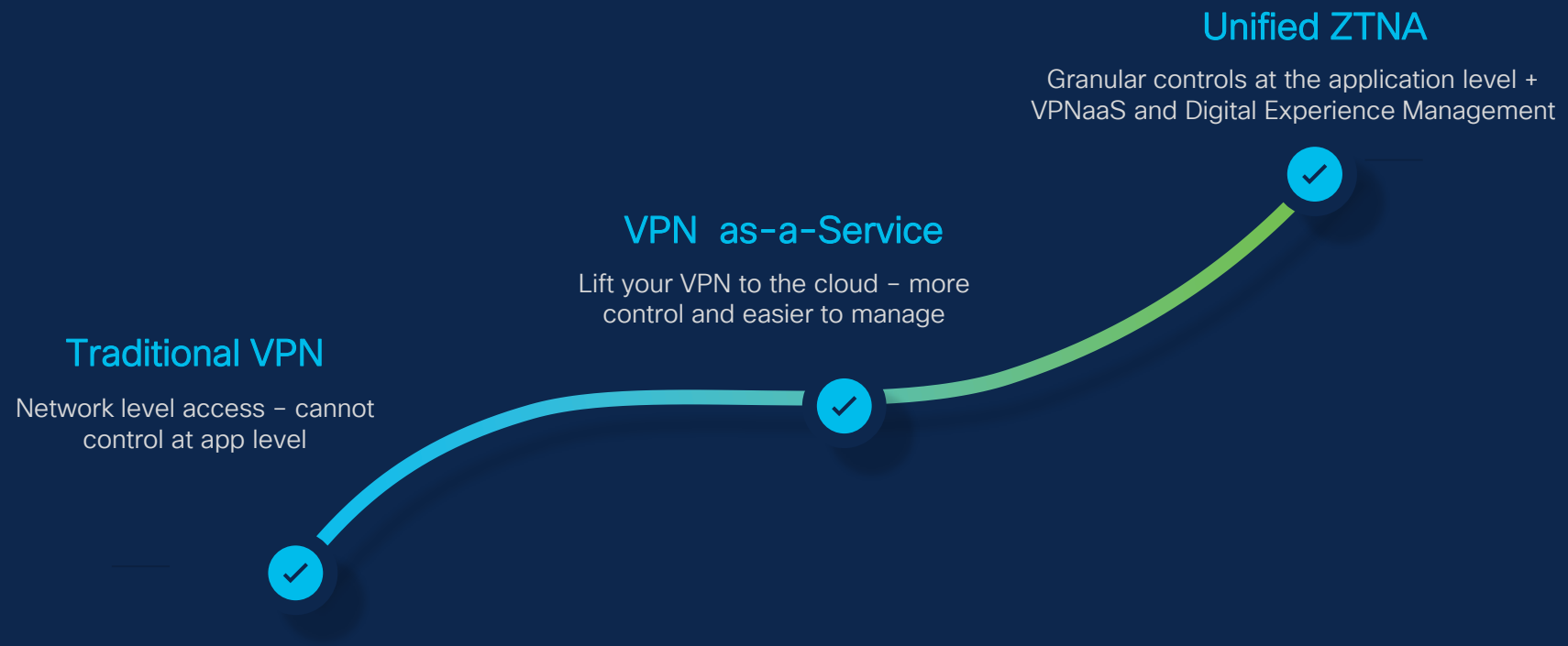


App compatibility with Zero Trust

Examples of private apps that don't work well with Zero Trust

- Client-to-client traffic (i.e. peer-to-peer VoIP)
- Server-to-client traffic (i.e. remote desktop; remote assistance)
- Applications that require a unique client IP (i.e. SMBv1)
- Applications that require SRV DNS records (i.e. Active Directory, Kerberos, SCCM)
- Applications that require the server to send a data payload (after the TCP 3-way handshake), before the client will send a data payload (i.e. MySQL Studio)
- Applications that perform an ICMP connectivity check prior to connecting via TCP or UDP

Simplify the journey to Zero Trust with migration



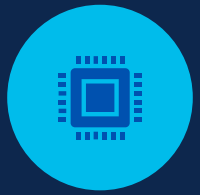
Why QUIC?

- Fast connection establishment (0-RTT)
- Ability to change IPs without renegotiation (Connection migration)
- No waiting for partially delivered packets (Individually encrypted packets)
- Not vulnerable to TCP meltdown (UDP transport)
- No head-of-line blocking (Stream multiplexing)
- Can simultaneously use multiple interfaces (Multipath)

Why MASQUE?

No direct resource access (Proxy architecture)

Broad application support (TCP, UDP and IP)



Fallback to HTTP/2 (TCP 443) if QUIC (UDP 443) is blocked

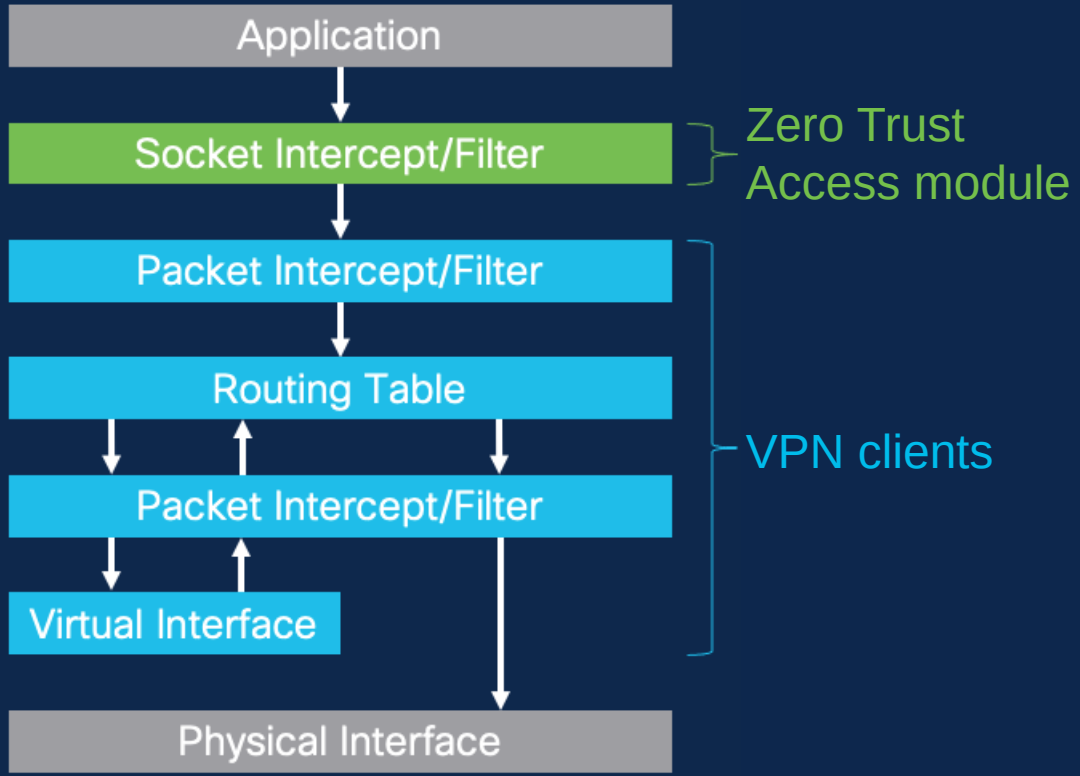
Flexibility to support per-connection, per-app or per-device tunnels

Native OS support

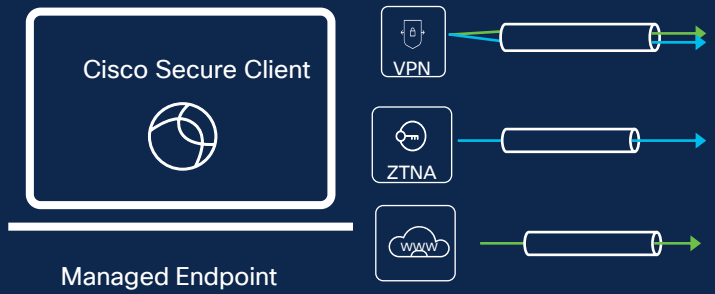
Zero Trust Access module – Socket intercept

Why use socket intercept?

- Control of DNS and application traffic *before* VPN clients (interoperability with Cisco and non-Cisco VPNs)
- No route table manipulation
- Ability to capture traffic by IP, IP subnet, FQDN, and FQDN wildcard



Who: Remote User Connectivity



Anyconnect VPN
→ Authentication & Posture @ Connect time
→ DTLS Tunnel
→ Carry **Internet & Private Traffic** (All ports & protocols)
→ SAML, (+) Cert, & (+) Multi-Cert Authentication

ZTNA Module
→ Authentication & Posture per session
→ QUIC tunnel (MASQUE proxy)
→ Carry **Private Traffic** (All ports & protocols)
→ SAML Auth + Auto re-new

Web Roaming Module
→ Device Enrollment (profile)
→ Carry Internet Web Traffic (80/443)

Clientless ZTNA
→ Accessible from any browser that supports SAML/Cookies
→ Request based posture (geolocation, browser version, OS)
→ Web Apps Only

Posture

* Roadmap

Authorization check prior to application access

Authorization and access check per session

	VPN Client-based	ZTNA Client-based	ZTNA unmanaged (browser only)
Operating System	✓	✓	✓
Geolocation Check (moved to access policy)	✓	✓	✓ *
Firewall	✓	✓	
Disk Encryption	✓	✓	
Browser Check	✓		✓
Anti-Malware	✓	✓	
File Check	✓		
Registry Check (windows only)	✓		
Process Check	✓		
System Password		✓	
Certificate Check	✓		

Supported AV vendors – Client-based ZTNA

Windows 10/11

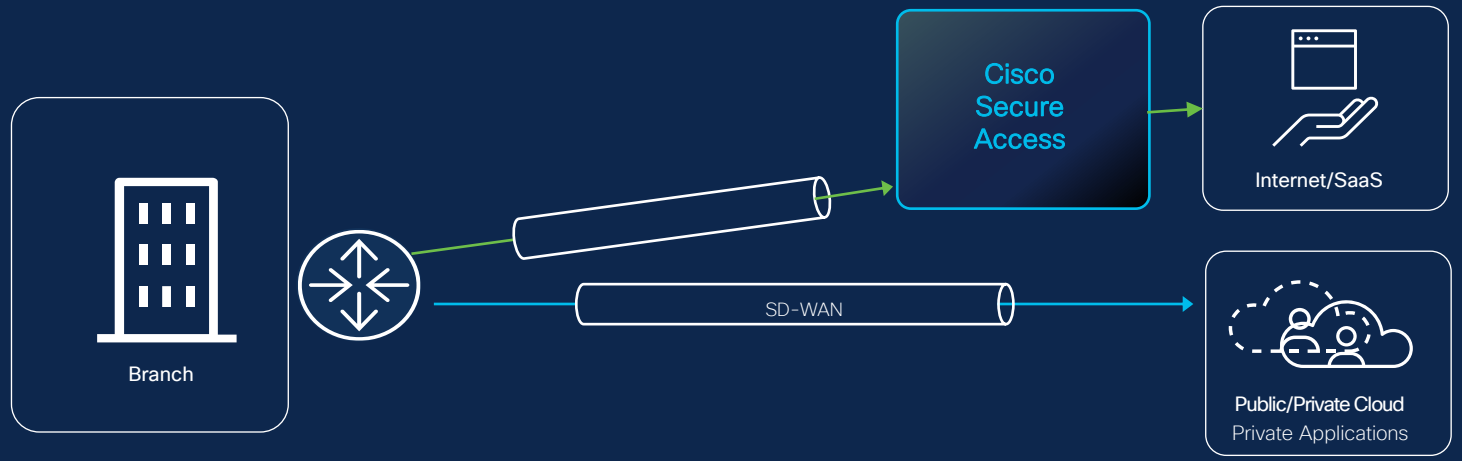
- BitDefender Endpoint Security
- Cisco Secure Endpoint
- CrowdStrike Falcon Sensor
- McAfee Endpoint Security
- SentinelOne
- Sophos AV (Intercept X)
- CylancePROTECT
- Symantec Endpoint Protection
- Trend Micro Apex One
- VMWare Carbon Black Cloud
- Microsoft Defender
- Palo Alto Cortex XDR

macOS

- BitDefender Endpoint Security
- Cisco Secure Endpoint
- CrowdStrike Falcon Sensor
- McAfee Endpoint Security
- SentinelOne
- Sophos AV (Intercept X)
- Symantec Endpoint Protection
- Trend Micro Apex One
- VMWare Carbon Black Cloud
- CylancePROTECT
- Palo Alto Cortex XDR

Supported AV vendors, RA VPN:
https://www.opswat.com/partners/certification/certified-products

Who: Branch Users Connectivity

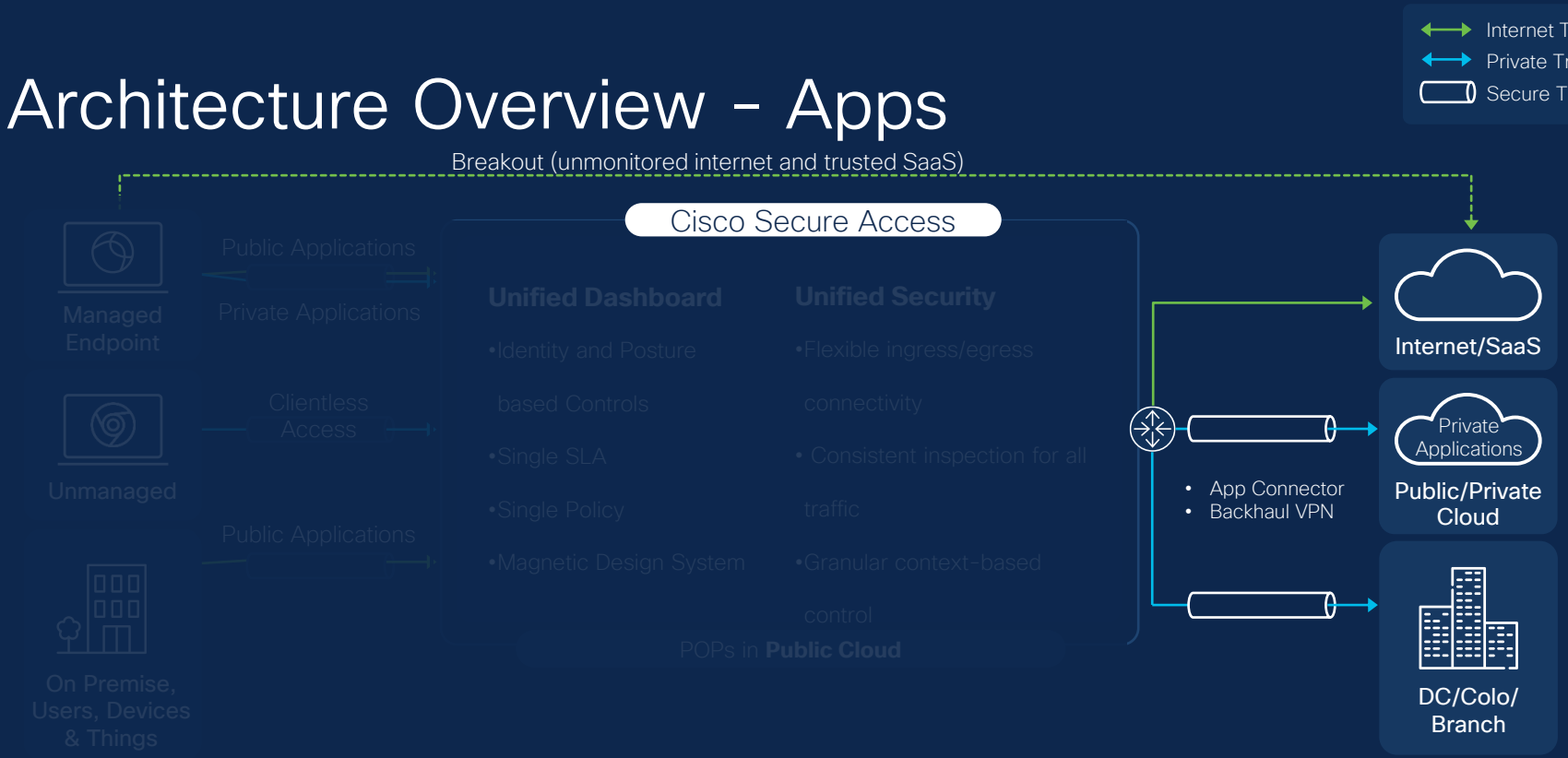


Branch Devices

→ 1GB throughput (edge device tunnel to Secure Access)
→ All internet traffic is routed to Secure Access
→ Auto Tunnels with Viptela SD-WAN SIA branches [1]

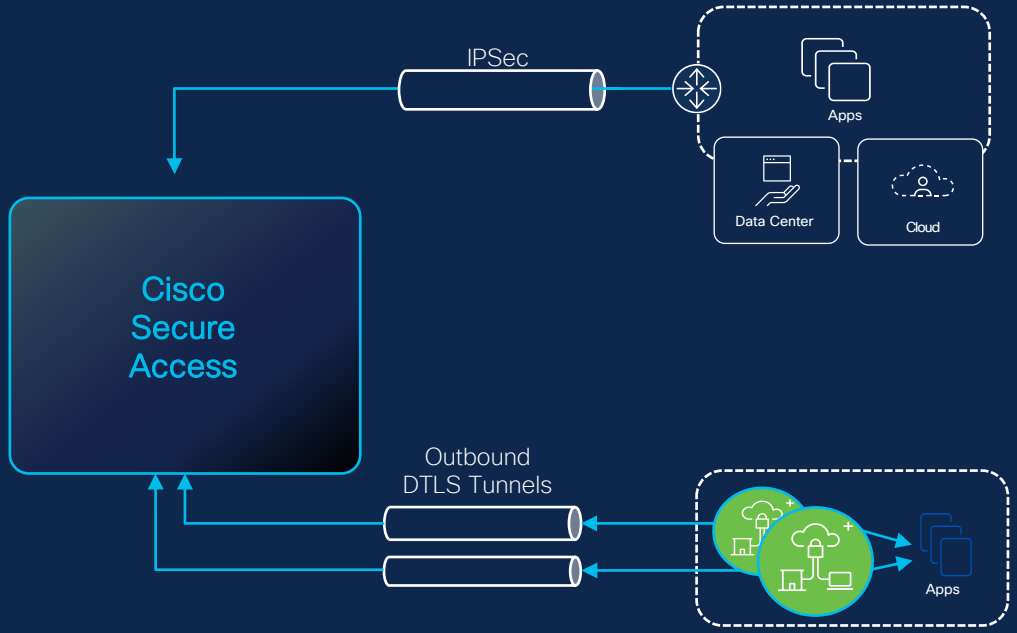
[1] Available Dec 2023 (requires Viptela code upgrade)

Architecture Overview – Apps



Users & Devices — How — Apps

Apps: Private Applications



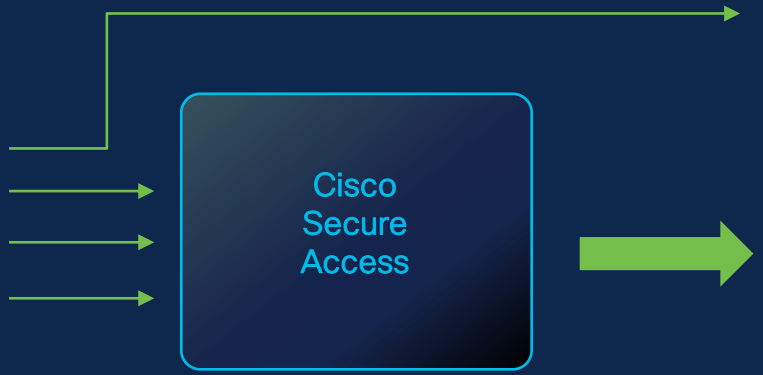
Network Tunnel

→ IPSec Backhaul
→ Static or BGP based routing
→ Auto Failover/ Redundancy

Application Connector (AC)

→ Software deployment (VM or Cloud Instance)
→ Deploy closest to application
→ Outbound connectivity (no holes in firewall)
→ Auto failover / load balancing

Apps: Internet/SaaS Applications



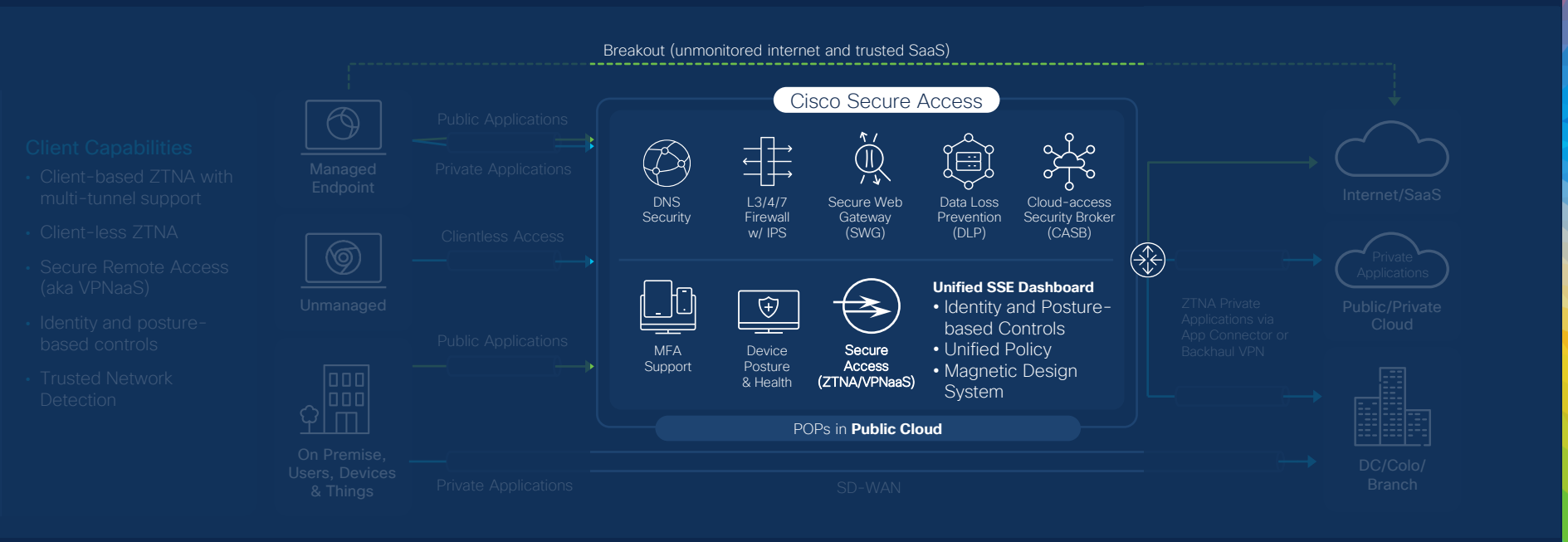
Trusted SaaS/Bypass

→ Bypass inspection for trusted web apps
→ route traffic directly from host to internet

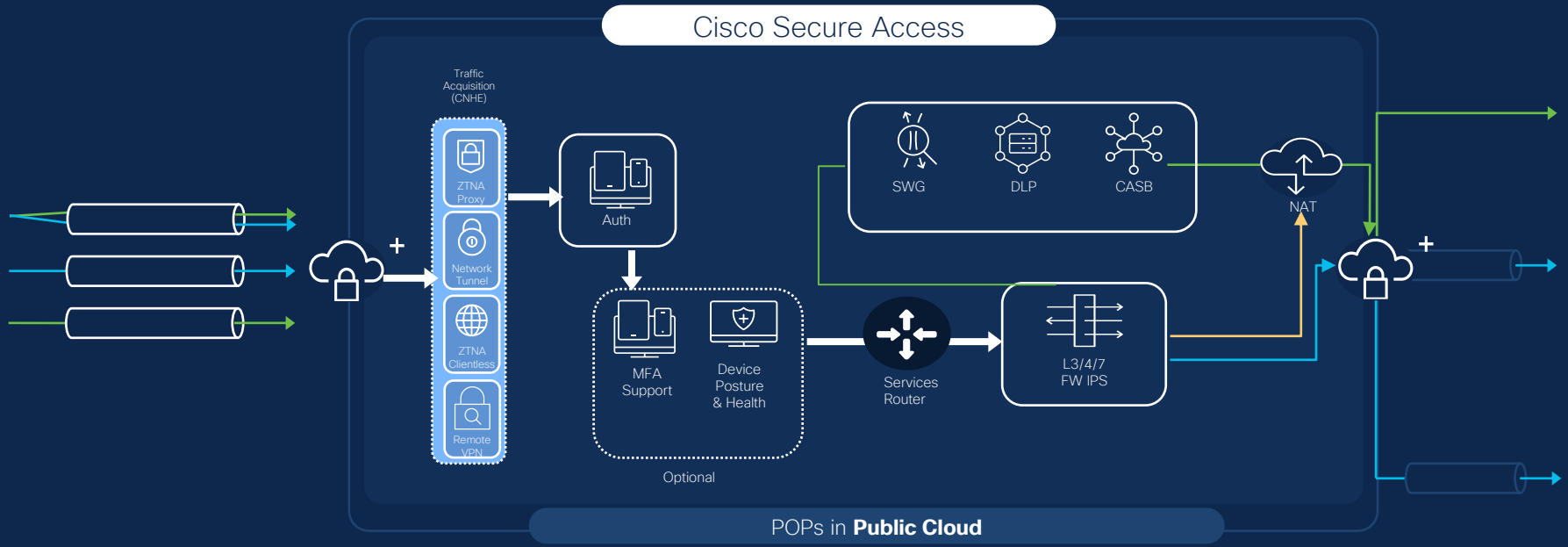
Secure Internet Access

→ All traffic filtered through Secure Access
→ Branch traffic routed via IPSec tunnel
→ Remote user traffic acquired via Secure Client

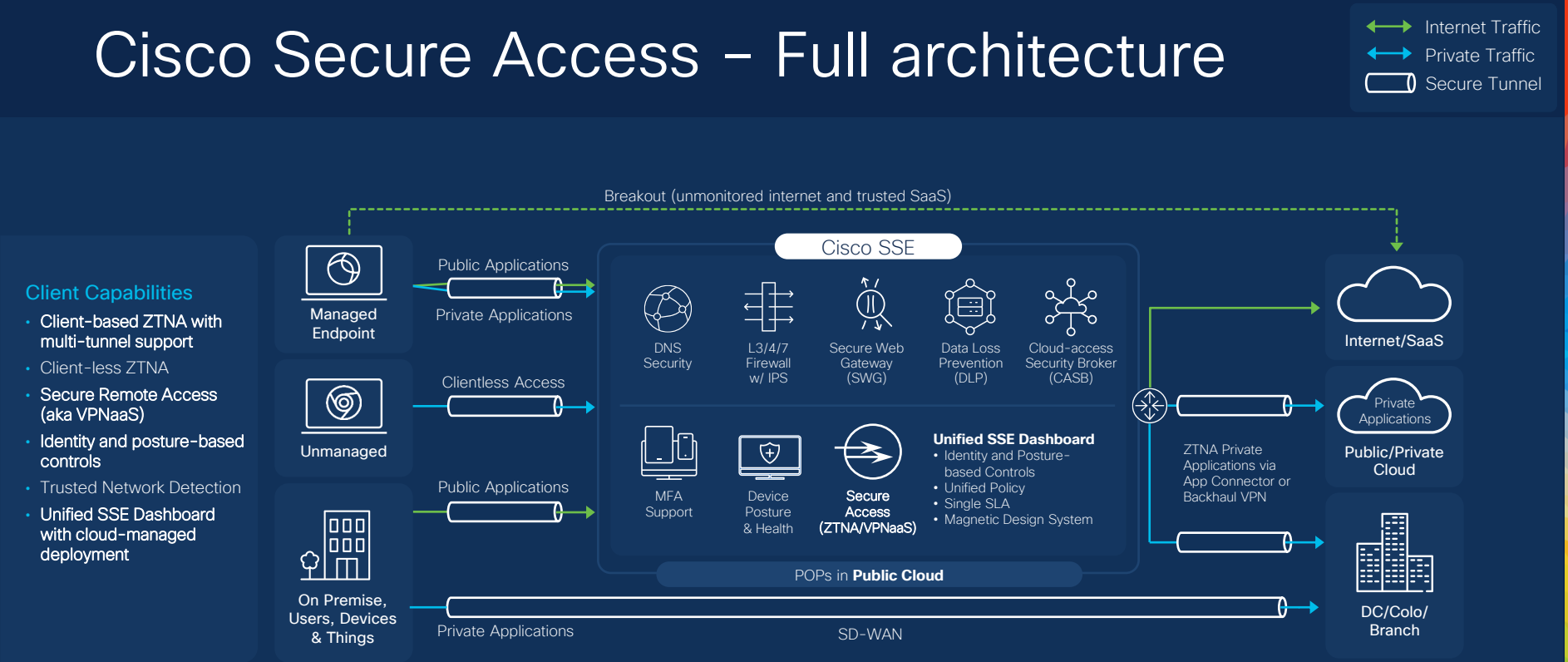
Security services



The Glue: Security Services & Policy Flow



Cisco Secure Access – Full architecture



Select Cisco Innovations

- ZTNA for Any Application, Any Port, Any Protocol with per user, per application controls
- Unified Client with Multi-tunnel ZTNA, VPNaaS, Posture
- Secure Internet Access – single in-line inspection with application policy
- POPs in Public Cloud and Cisco Edge Data Centers
- Unified SSE Dashboard – simplify administration to reduce risk and improve efficiency

Initial AWS Region coverage since GA

- Asia Pacific (Mumbai)
- Asia Pacific (Singapore)
- Asia Pacific (Tokyo)
- Australia (Sydney)
- Europe (Frankfurt)
- Europe (London)
- Middle-East (Tel Aviv)
- US East (Northern Virginia)
- US West (Oregon)

Datacenter architecture targets

- Initially in AWS regions
  - Ability to reach wide coverage, quickly (81 availability zones* in 31 regions)
  - New locations available within ~2 weeks
  - Close to customers' users and app locations
- After initial release will further expand
  - Additional public cloud locations: GCP, Azure, Gov cloud, customer private cloud
- Further expansion: Full hybrid
  - Seamless integration between public cloud and Cisco's existing cloud edge DCs (~40)
  - Ability to run private instance on customer's network (hybrid integration with cloud)

* Excludes availability zones in China and gov-cloud

Demos

1. Dashboard and Admin Experience
2. Resource Connectors
3. Experience Insights

Summary

Q&A

Summary and call to action...

- Secure Access provides the best end-user and admin experiences
- Differentiators:
  - Single dashboard/policy
  - Single agent
  - VPNaaS
- Easy to get started; migration options, POV
- Product experts at Cisco Live from Product Management, Technical Marketing, and Sales Architects
- Product demos, MTE, related breakout sessions
  - BRKSEC-2729, ZTNA deep dive: Room 212 / Thursday, 16:00

cisco Live!

Did you know?

You can have a
one-on-one session with
a technical expert!

Visit Meet the Expert in The HUB
to meet, greet, whiteboard & gain
insights about your unique questions
with the best of the best.

Meet the Expert Opening Hours:

Tuesday	**3:00pm – 7:00pm**
Wednesday	**11:15am – 7:00pm**
Thursday	**9:30am – 4:00pm**
Friday	**10:30am – 1:30pm**

Session Surveys

We would love to know your feedback on this session!

- Complete a minimum of four session surveys and the overall event surveys to claim a Cisco Live T-Shirt

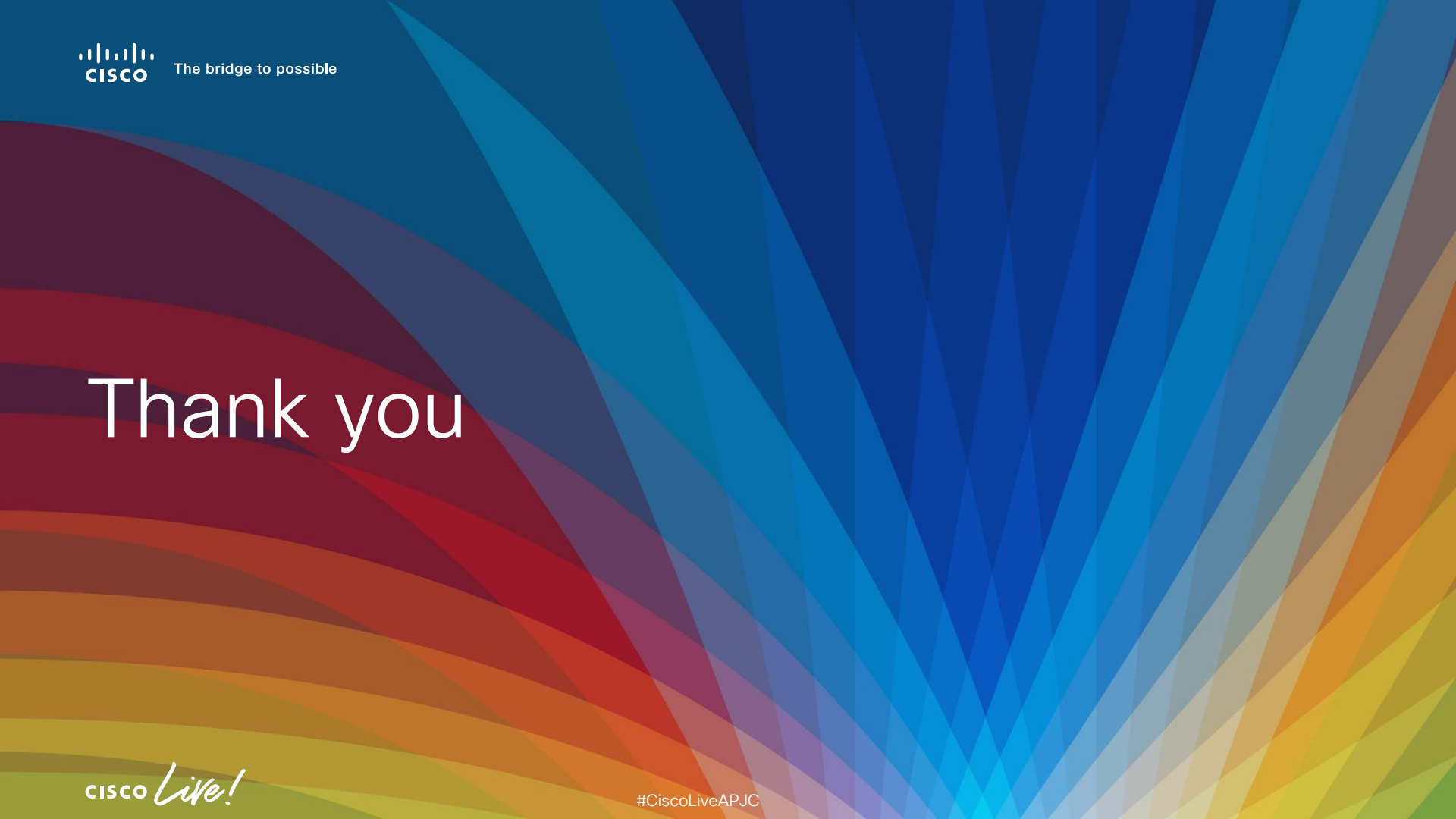
cisco
SECURE

cisco The bridge to possible

Participating in user research gives you a place to share your thoughts and experiences to influence the future of Cisco Secure products.

- You'll hear from us once every 90 days at the most
- Participation is completely optional, and you can opt out at any time

Q&A


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


cisco Live!
Let's go
#CiscoLiveAPJC