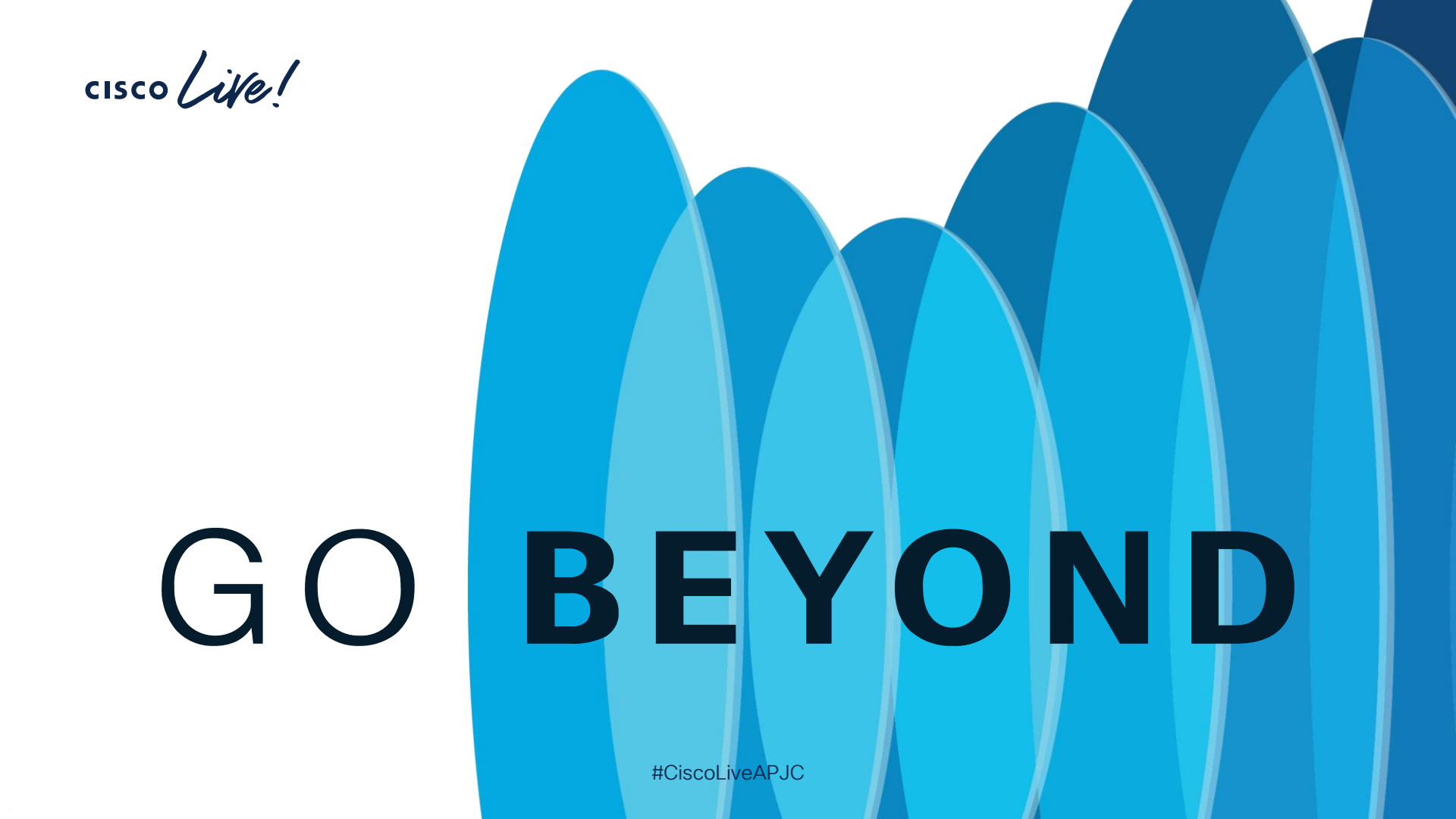

cisco Live!
GO BEYOND
#CiscoLiveAPJC

"Reconciliation"- Dustin Koa Art

Cisco Secure Access

Overview and End-to-End Flow Review

Jonny Noble – Director, Technical Marketing
@JonnyNoble3

BRKSEC-1708

Cisco Webex App

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

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 November 15, 2024.

cisco Live!

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

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, VPN as a Service, simplified policy management, and a unified client that removes the frustration of securely connecting for your hybrid workforce, all coming together to protect your users and internal resources
- 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, and concluding with demos of the latest innovations
- Ample time will be kept for QA and an open discussion with the audience

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

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 organisations
- 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

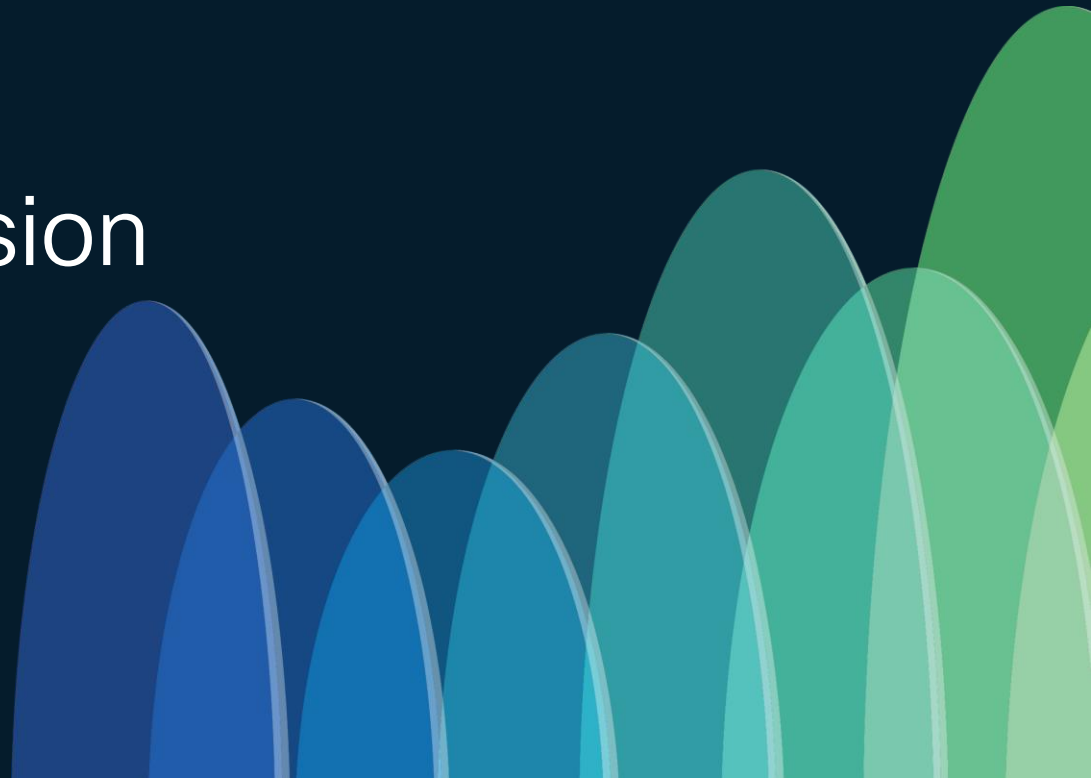
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Agenda

- Session introduction
- Setting the scene for Cisco Secure Access
- What have we built?
- Architecture and flow
- Recent innovations and demos
- Summary and Q&A

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Let’s Set the Scene, and Session Expectations



cisco Live!

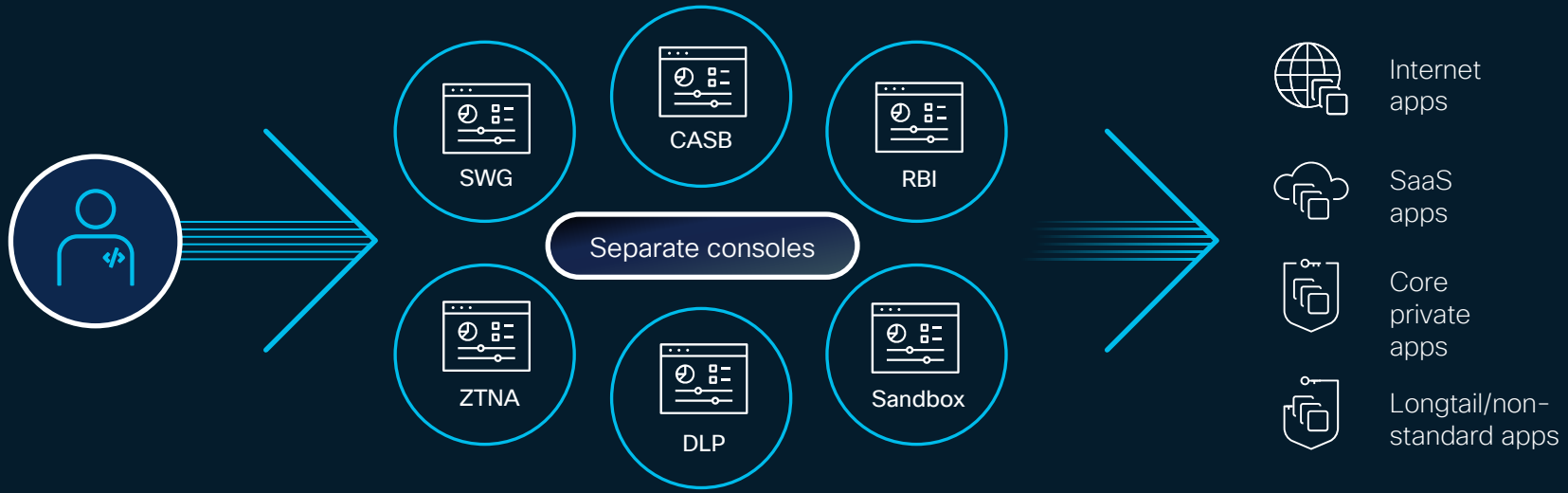
Today’s businesses depend on a new approach

Cisco Secure Access, Cisco’s SSE

1. Zero Trust Architecture (ZTA)
2. Secure Internet Access and SDWAN
3. ZTNA and Secure Remote Access from Anywhere

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

The multi-vendor approach is problematic



New threats spawn new vendors, putting the burden on customers

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

What have we built?

Cisco Secure Access

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

Cisco Secure Access

Converged cloud security in a single subscription Size 18, left aligned

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

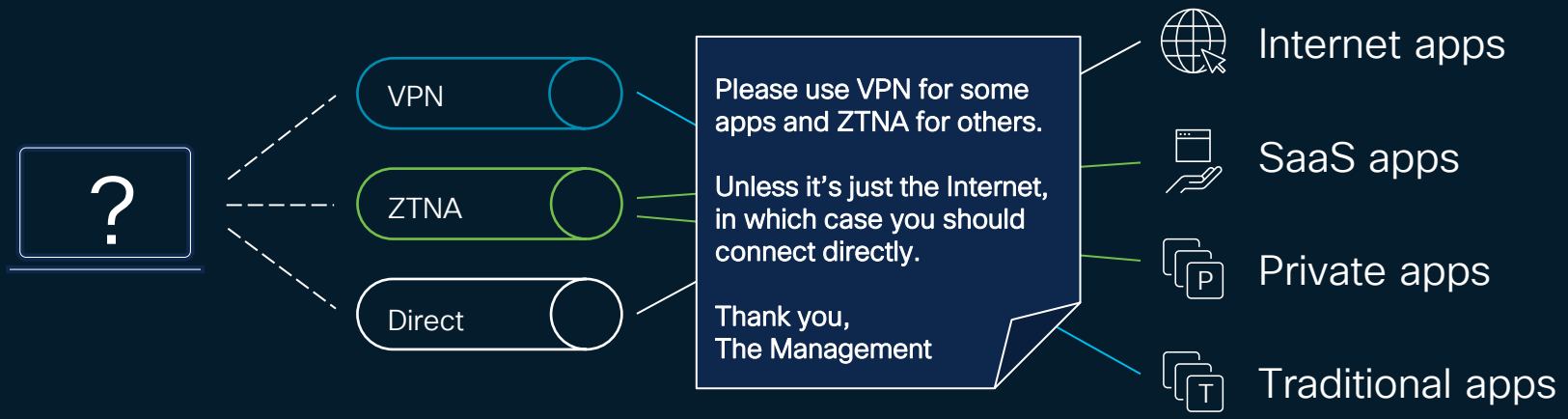
Imagine cybersecurity that's

safer and easier for everyone

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Eliminate unnecessary end-user decisions

How would you like to connect to your applications?



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

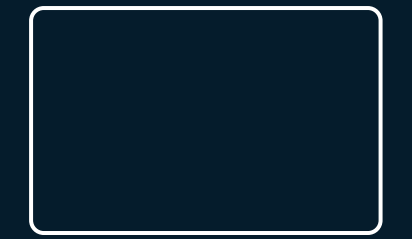
Reimagine the user experience

Cisco Secure Access makes the connections you need

Size: 18, left aligned

1 Connect to a network

2 Get to work



Note: Supports both client and clientless connectivity

Internet apps

Protected by Umbrella

SaaS apps

Protected by CASB

Private apps

ZTNA gives controlled access to selected applications

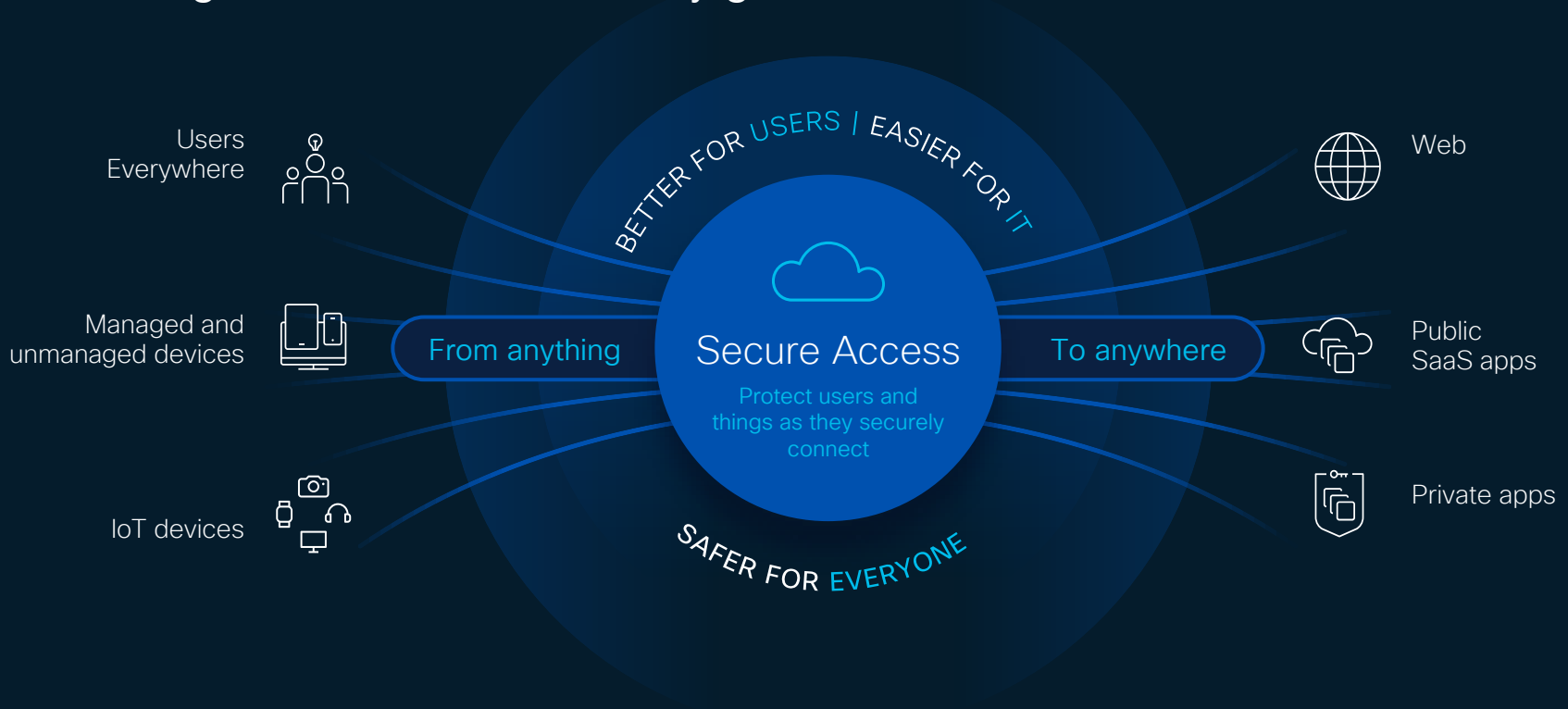
Traditional apps

VPN gives network access for existing applications

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Modernise your defense with Cisco Secure Access

Converged cloud-native security grounded in zero trust



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

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

From anywhere

Remote users

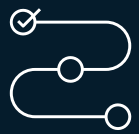
Managed and unmanaged devices

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 analyse 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

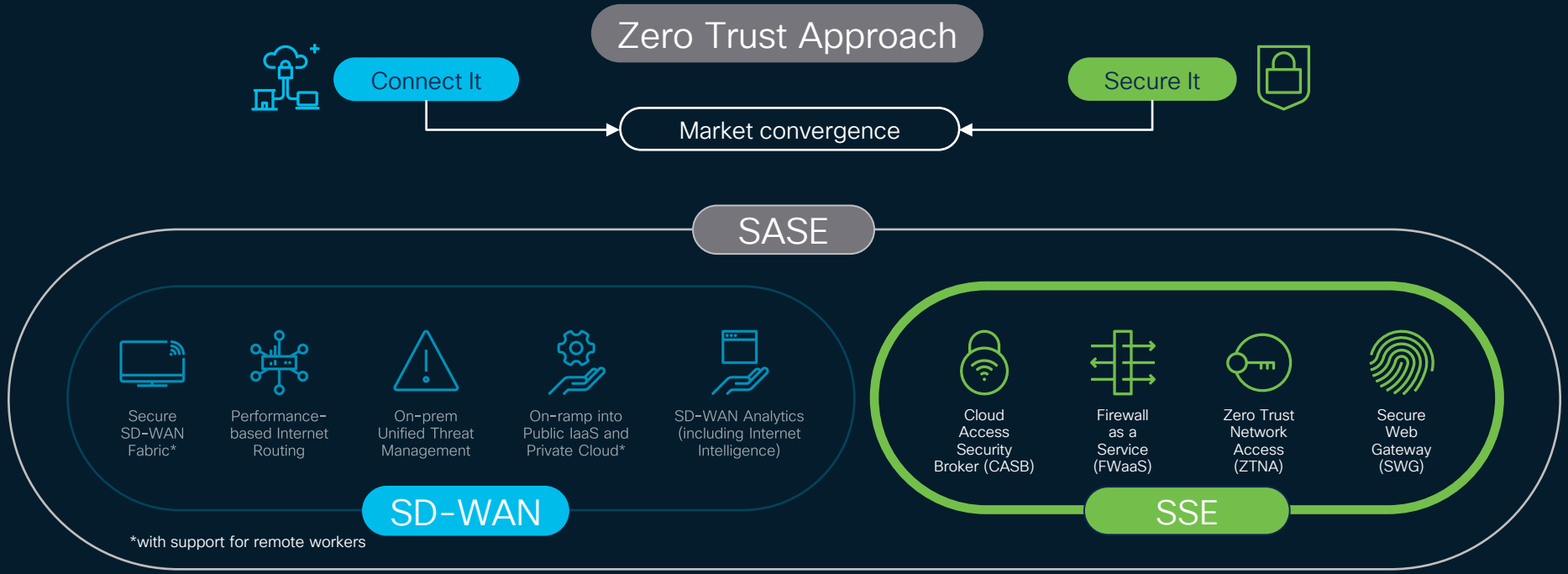
Public SaaS apps

Private apps

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

SASE/SSE approach is the technology foundation

Fundamental to your security strategy for a hyper-distributed world



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

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...

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Going beyond core security service edge

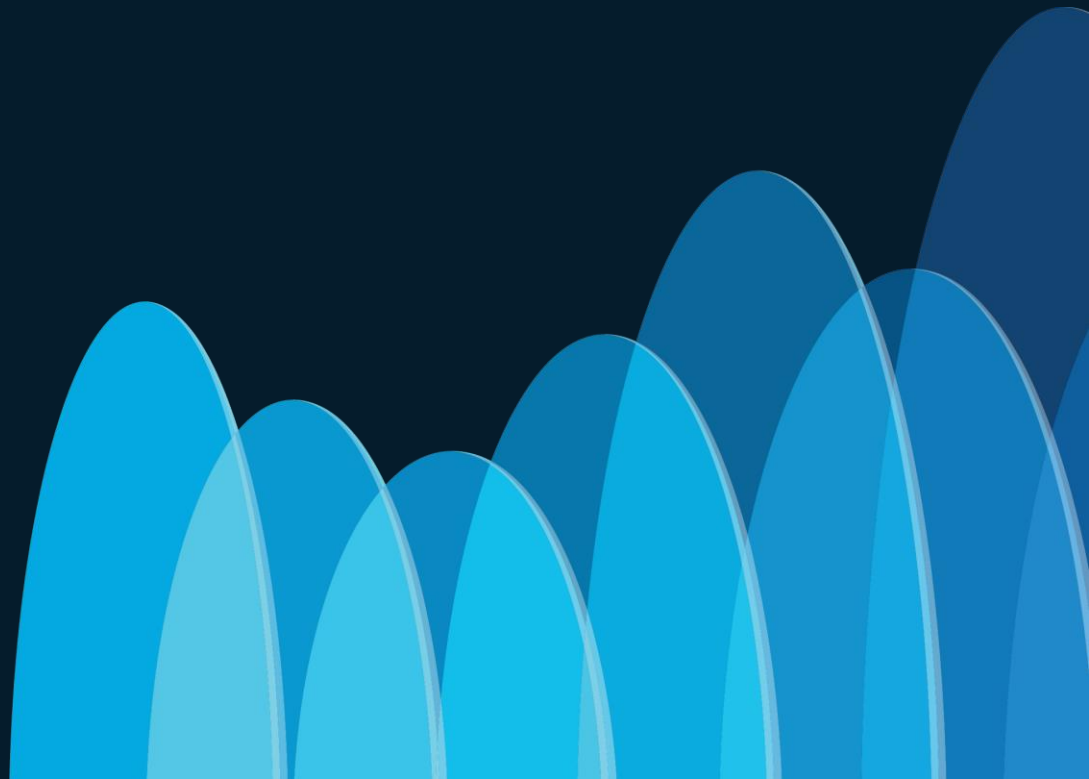
Cisco Secure Access

- 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

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Architecture and Flow Drill-down

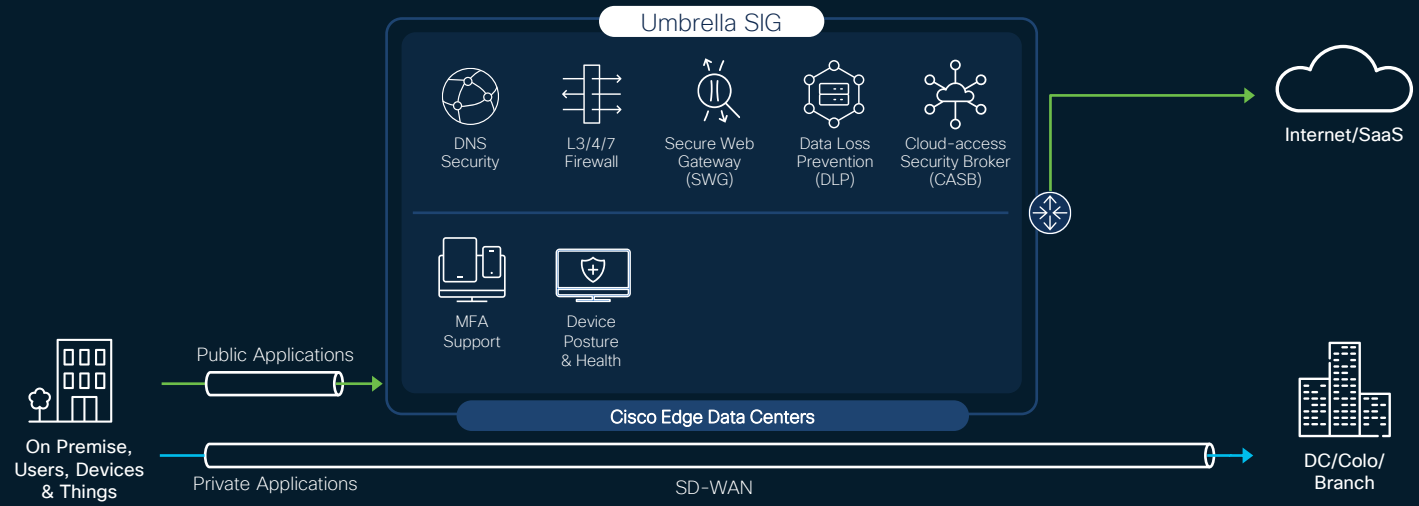


cisco Live!

Evolution from Cisco Umbrella SIG

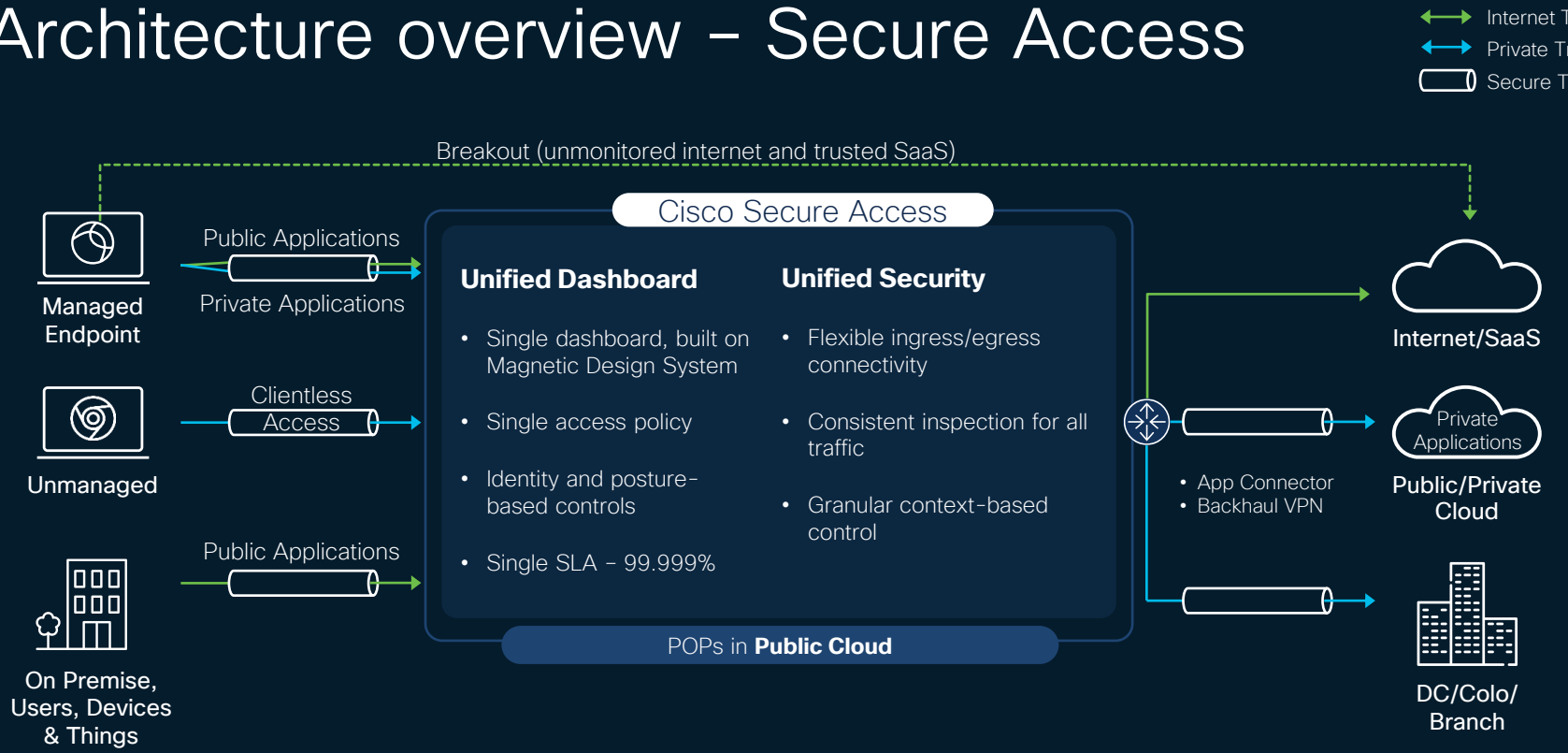
Main use-cases

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



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

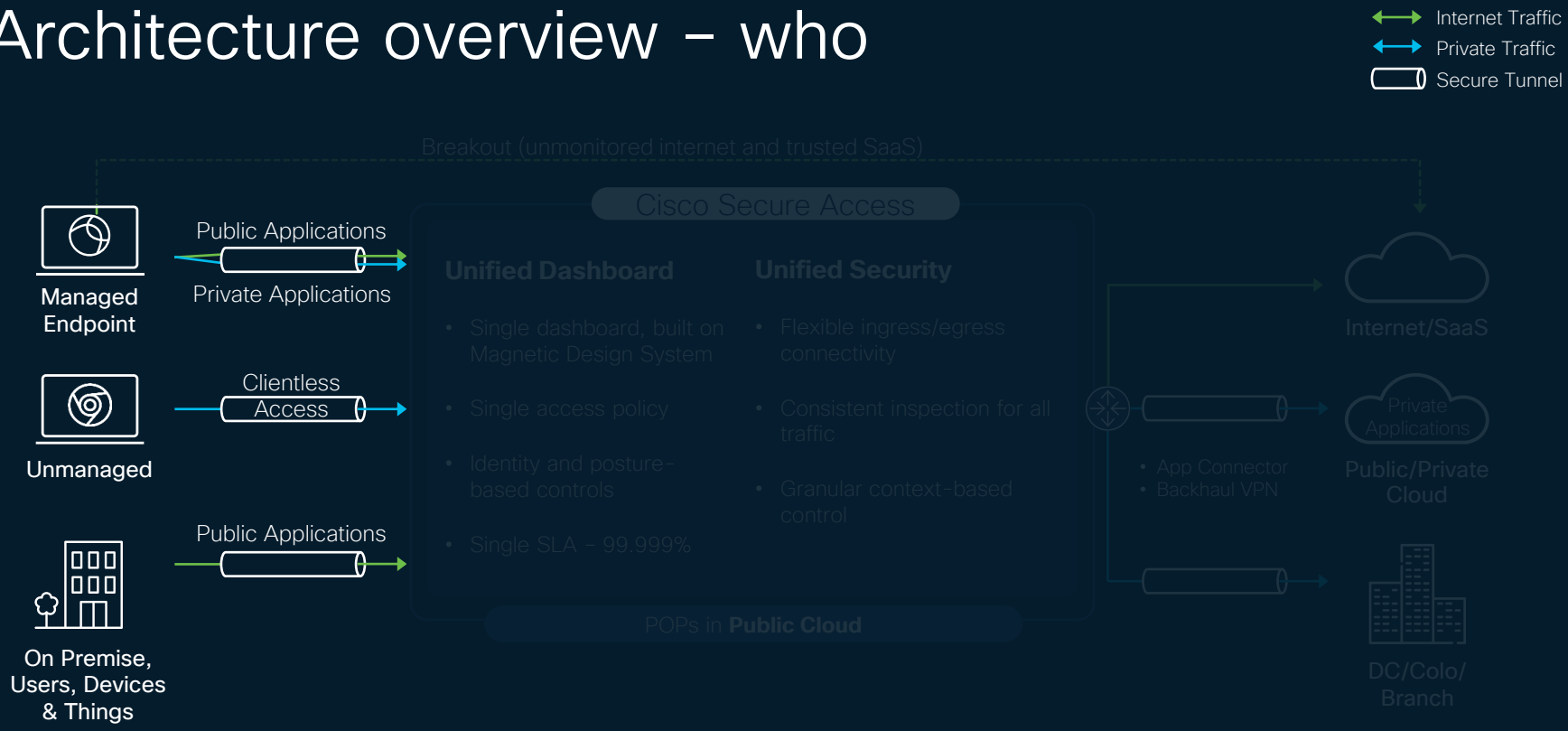
Architecture overview – Secure Access



Users & Devices — **How** — **Apps**

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Architecture overview – who

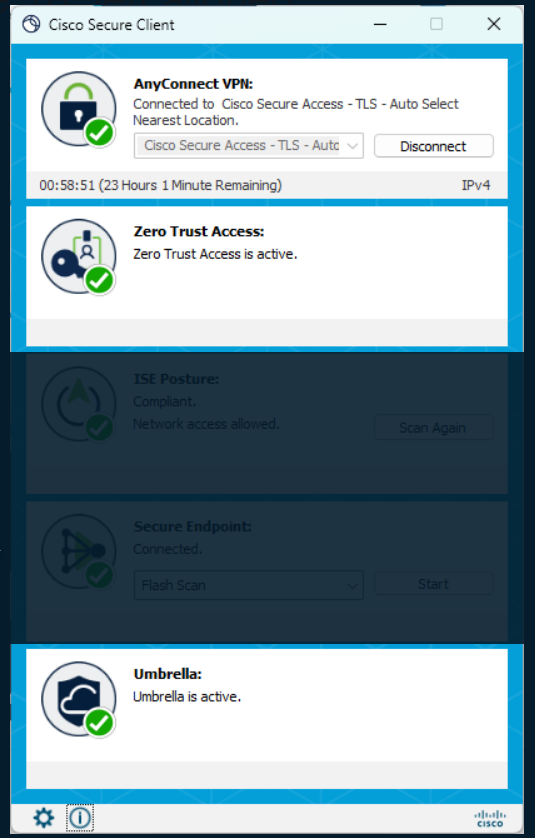


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

AnyConnect > Cisco Secure Client

Suite of security service enablement modules

- AnyConnect VPN (Core)
- ZTA Module (new!)
- ISE Posture
- Secure Endpoint (AMP)
- Roaming Module
- Thousand Eyes (No UI)
- Cloud Management Module (No UI)
- Diagnostic and Reporting (DART)

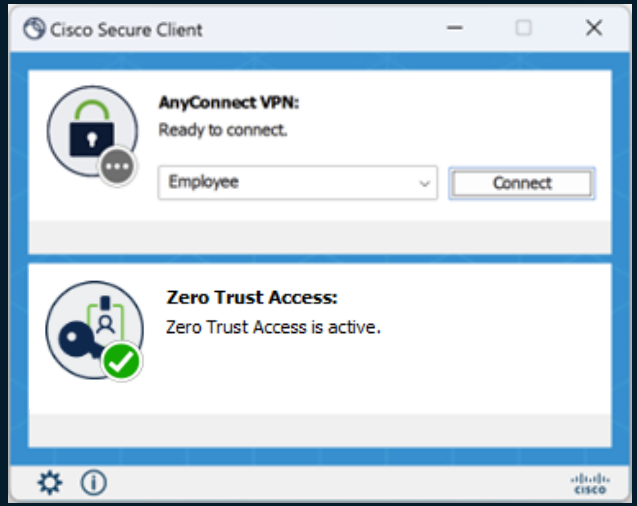


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

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)

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

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.
- Optimised 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

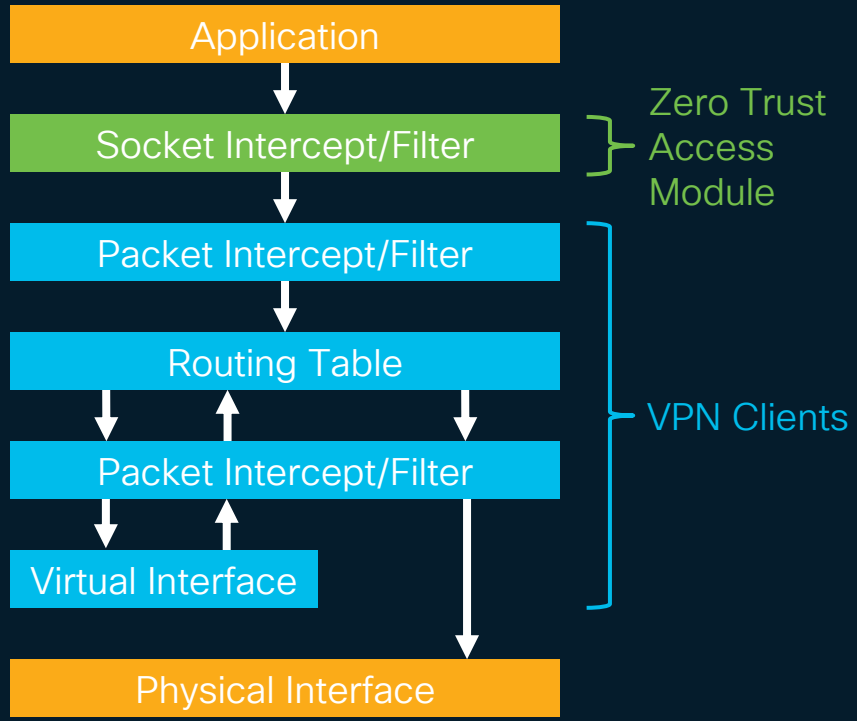
When combined, MASQUE + QUIC provides an efficient and secure transport mechanism for TCP, UDP and IP traffic for both web and non-web protocols

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Zero trust access module – socket intercept

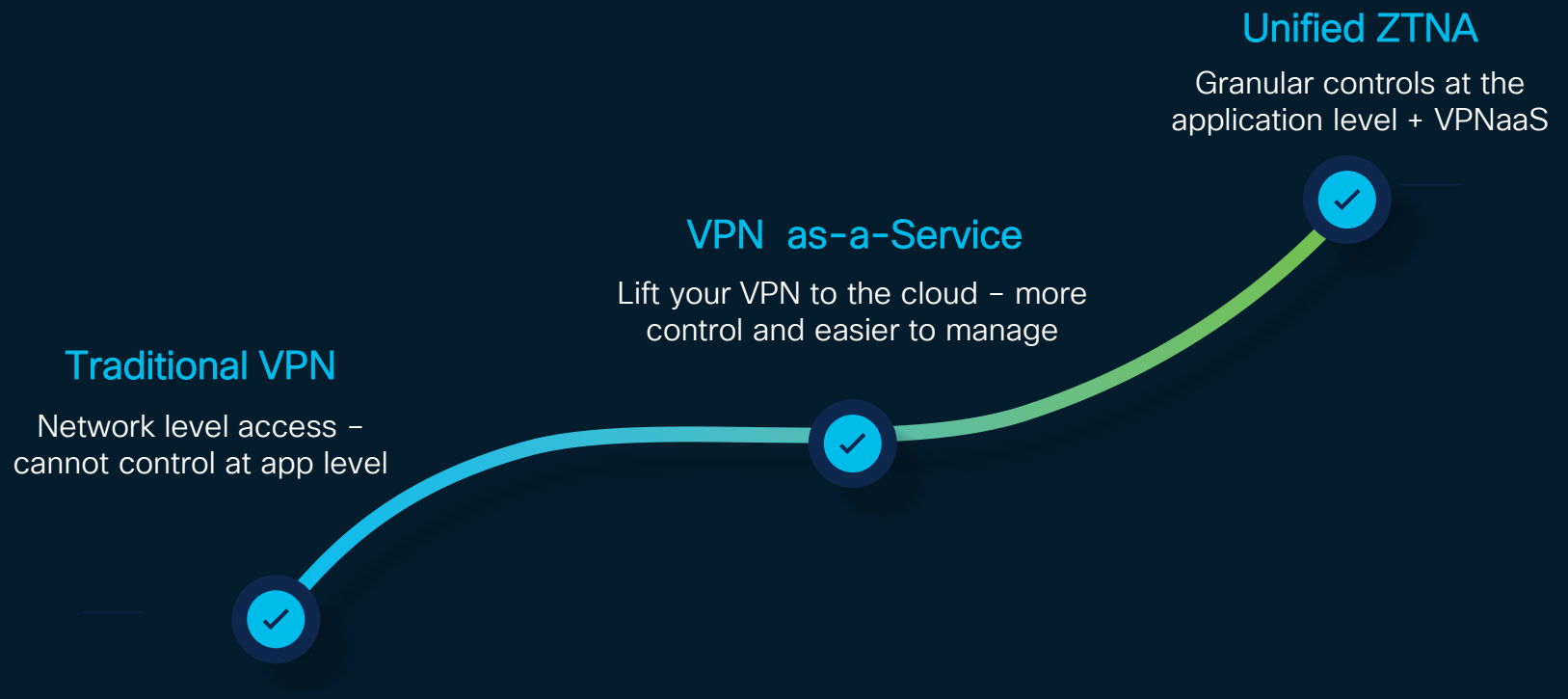
Why use socket intercept?

- 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
- Interoperability with Cisco and non-Cisco VPNs



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Simplify the journey to zero trust with migration



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

App compatibility with zero trust

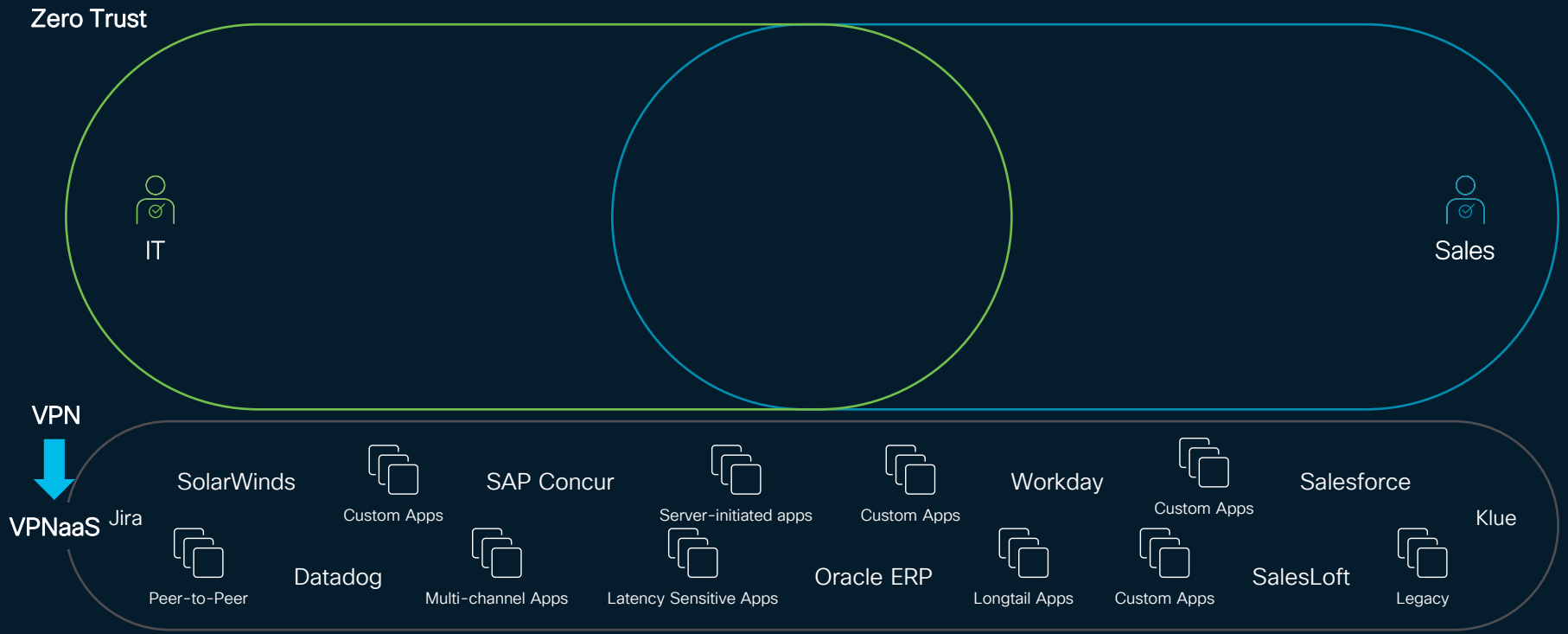
Examples of private apps that don't work well with Zero Trust

- 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, MS Configuration Manager, SCCM)
- Apps that perform an ICMP connectivity check prior to connecting via TCP or UDP

Users can continue to connect to these apps via Cisco Secure Access VPN

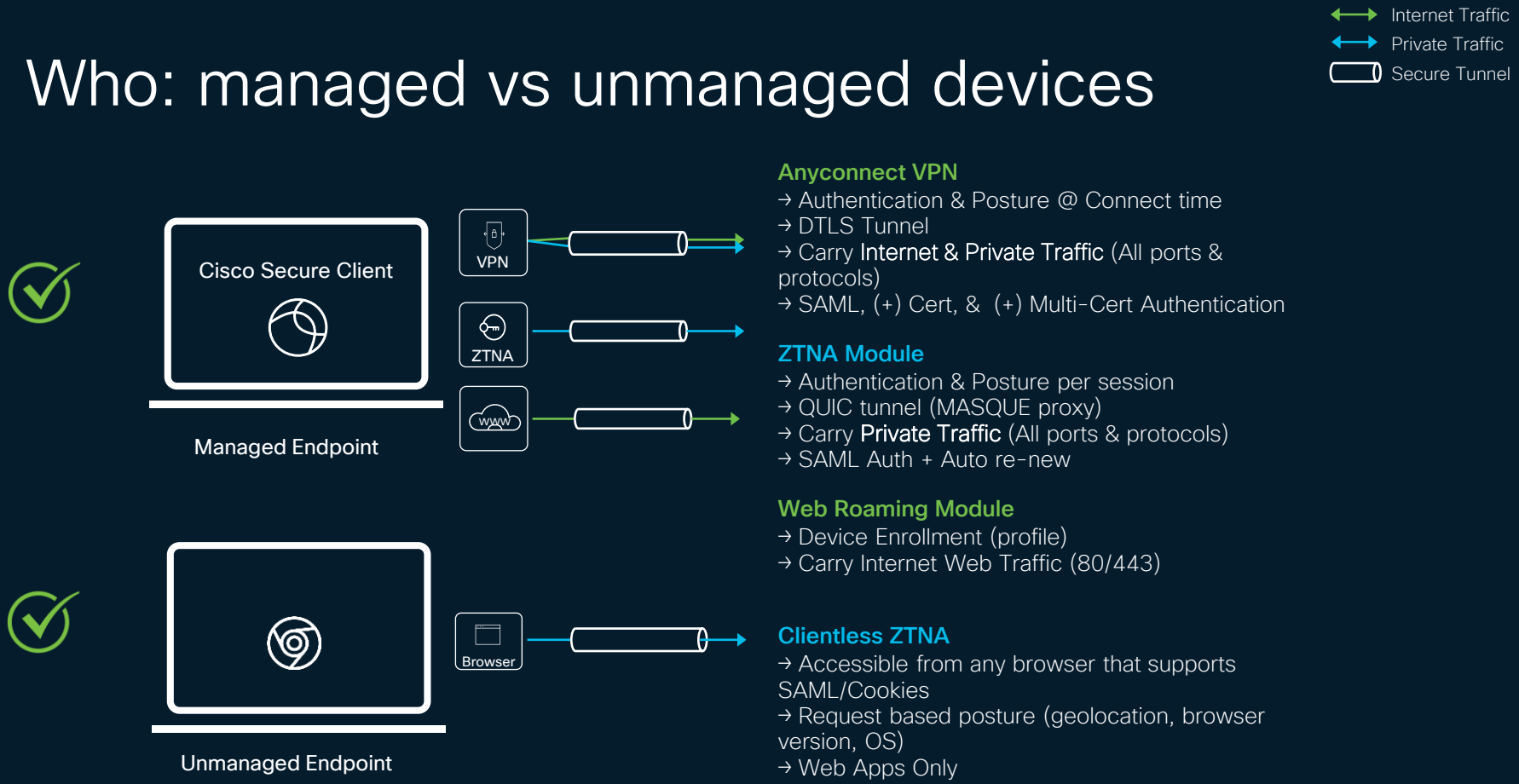
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Simplifying the journey to zero trust



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Who: managed vs unmanaged devices



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

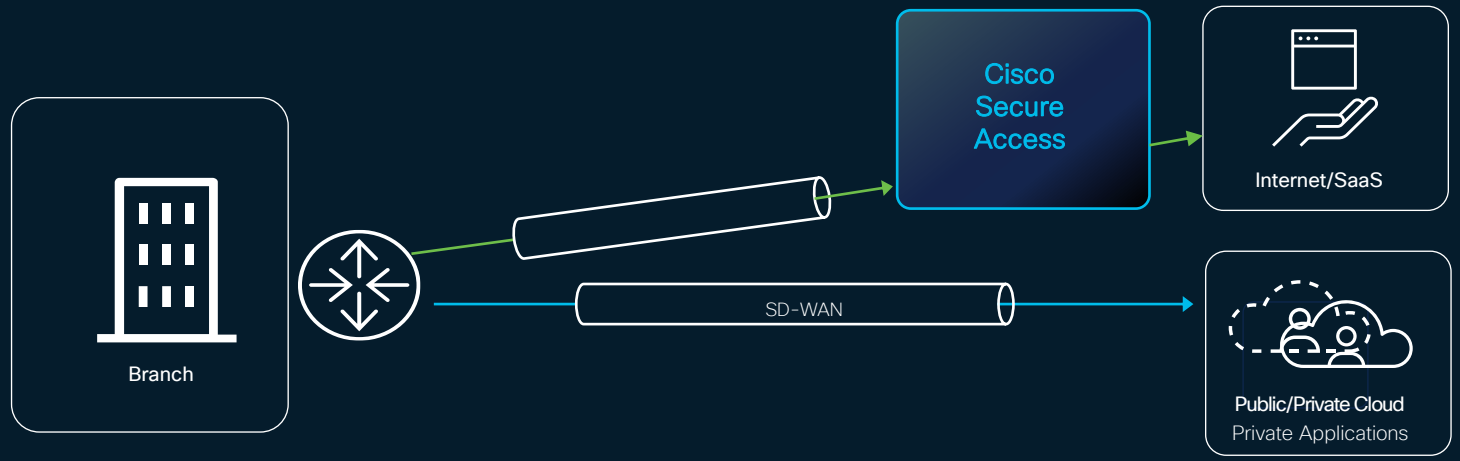
ZTNA Module
→ Authentication & Posture per session
→ QUIC tunnel (MASQUE proxy)
→ Carry Private Traffic (All ports & protocols)
→ SAML Auth + Auto re-new

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

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Who: branch users connectivity



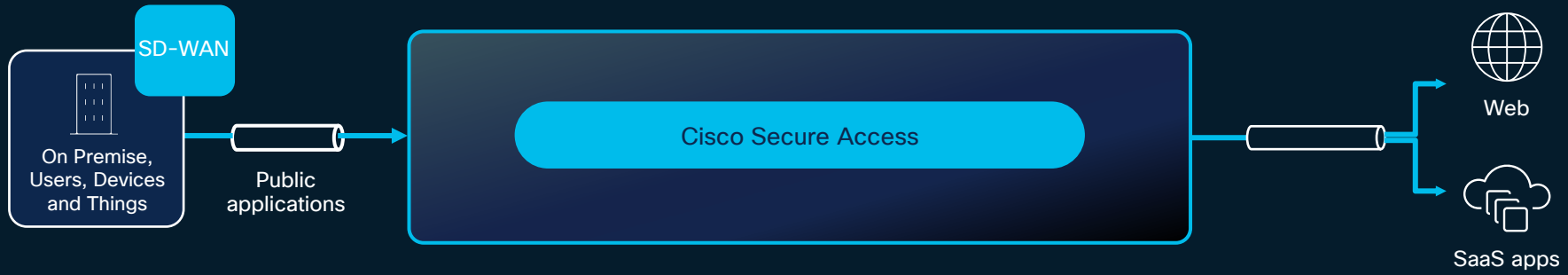
Branch Devices

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

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco Catalyst SD-WAN + Secure Access integration

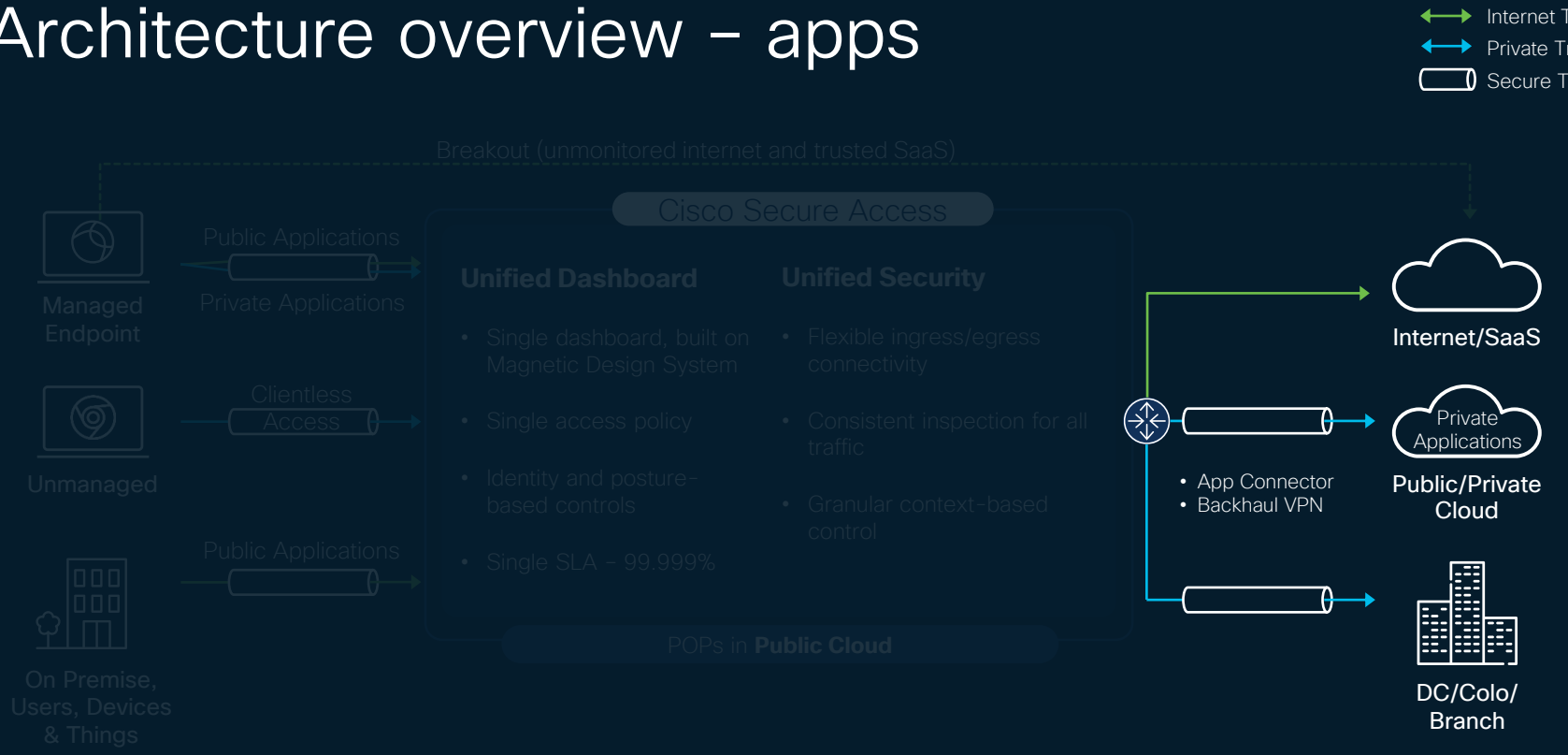
Increase security for Internet/SaaS traffic



- More consistent end-user experience – remote/roaming or in branch office
- Easily scale up/down and relieve capacity constraints
- Increase protection with robust, multi-layer security

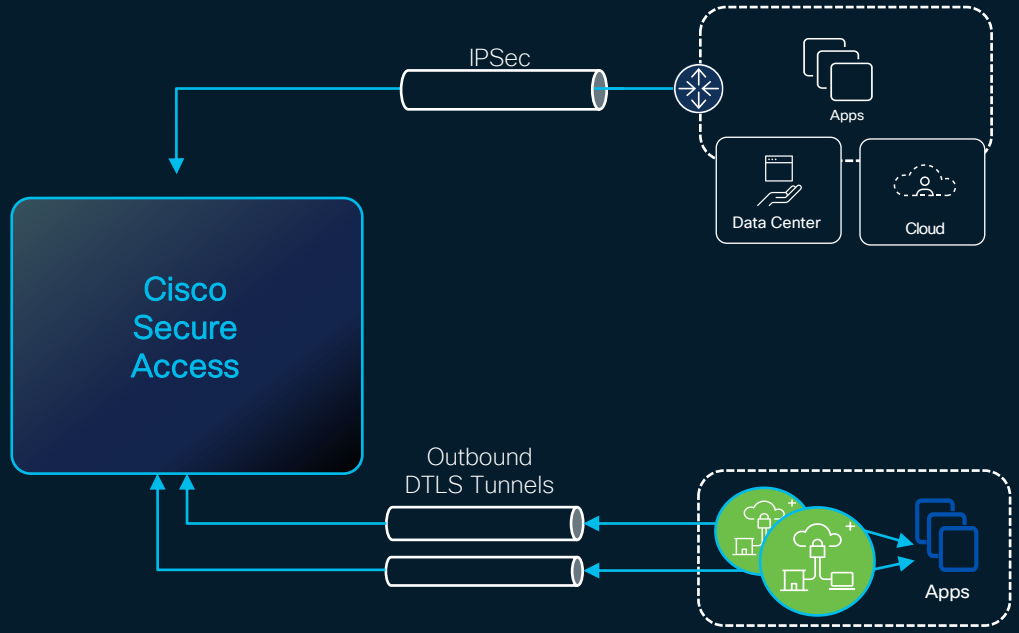
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Architecture overview – apps



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Apps: private applications



Network Tunnel

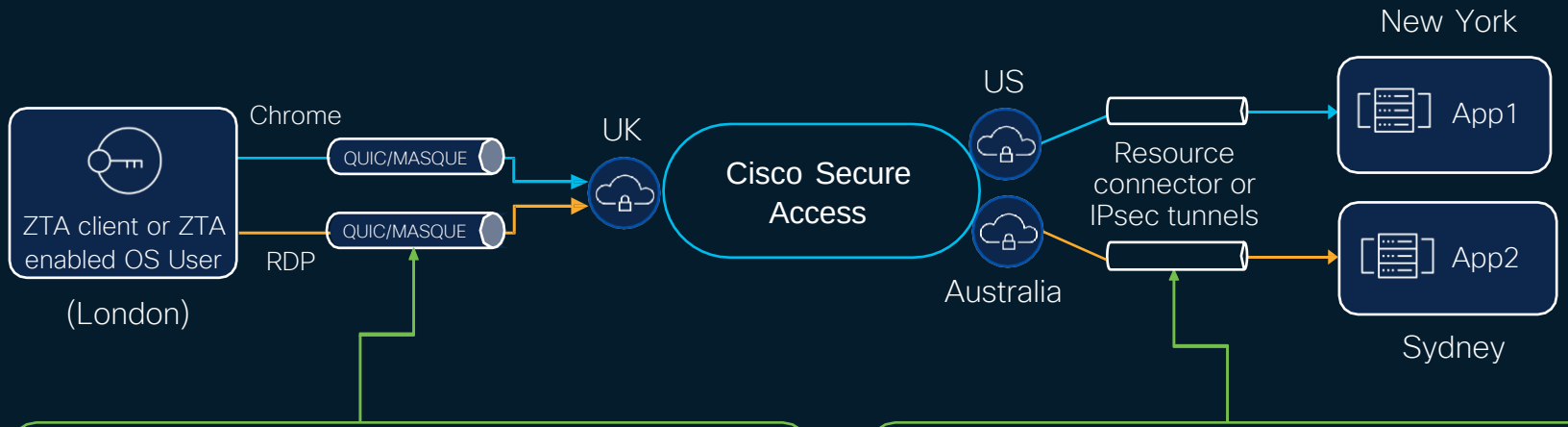
→ IPSec Backhaul
→ Static or BGP based routing
→ Auto Failover/ Redundancy

Application Connector (AC)

→ Software deployment (AWS, Azure, ESXi)
→ Deploy closest to application
→ Outbound connectivity (no holes in firewall)
→ Auto failover / load balancing

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Zero trust access – traffic flow summary

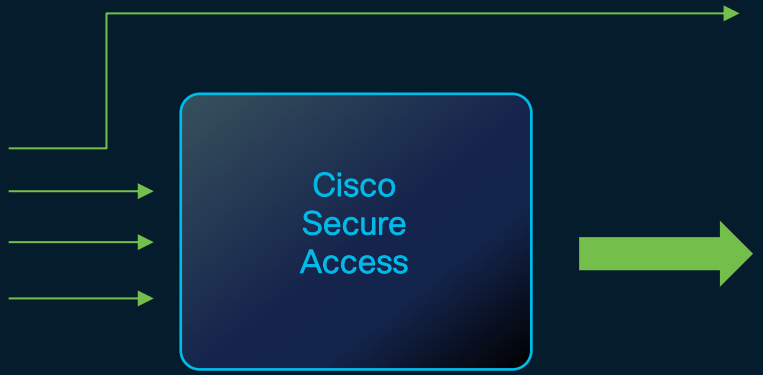


- No click seamless access
- Advanced protocols reduce latency and speed content delivery

- Full separation between users and the enterprise network
- Fast deployment with no firewall setting changes

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Apps: Internet/SaaS applications



Trusted SaaS/Bypass

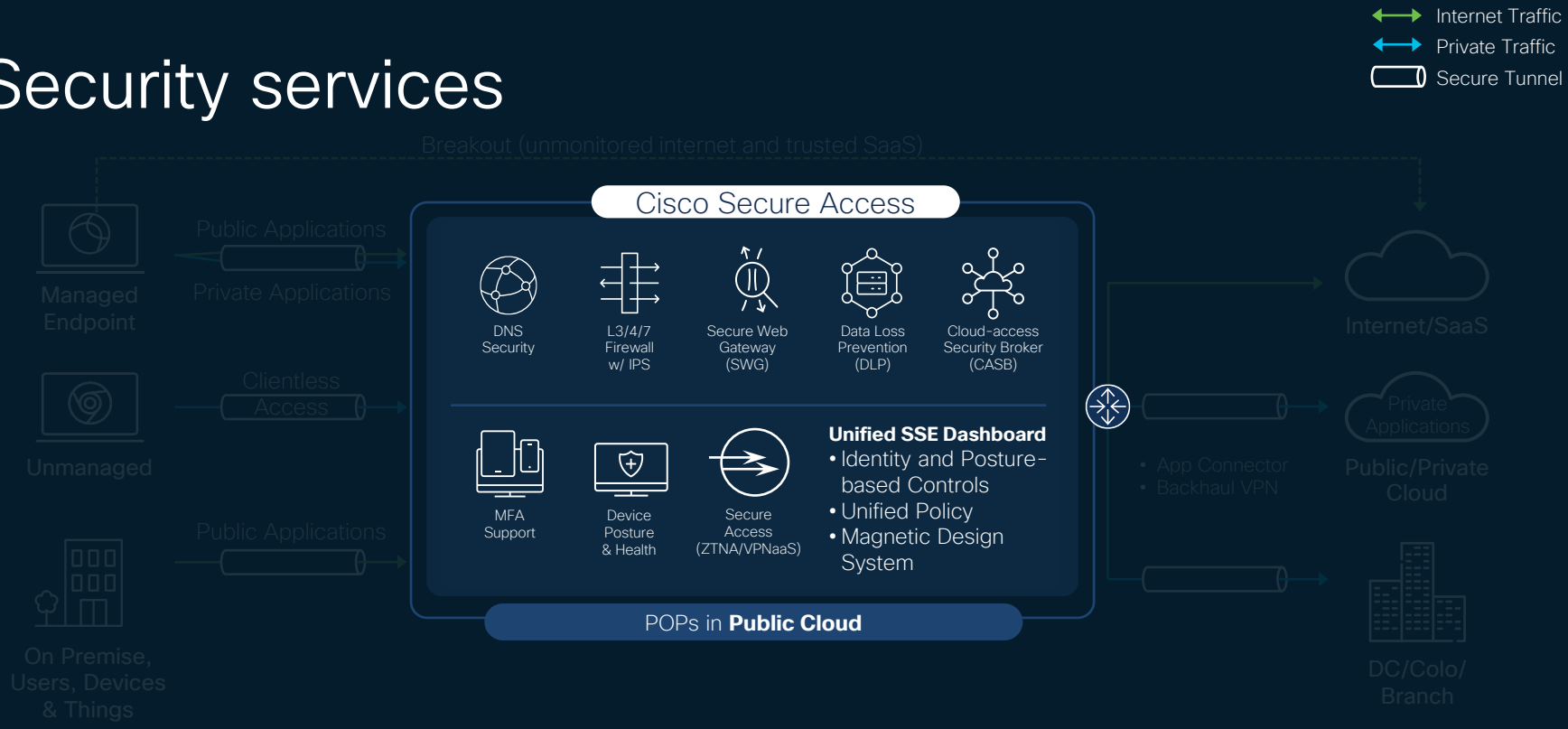
→ Bypass inspection for trusted web apps
→ route traffic directly from host to internet

Secure Internet Access

→ All traffic filtered through Secure Access
→ Branch traffic routed via IPSec tunnel
→ Remote user traffic acquired via Secure Client
→ Reserved IP available (unique per customer)

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Security services



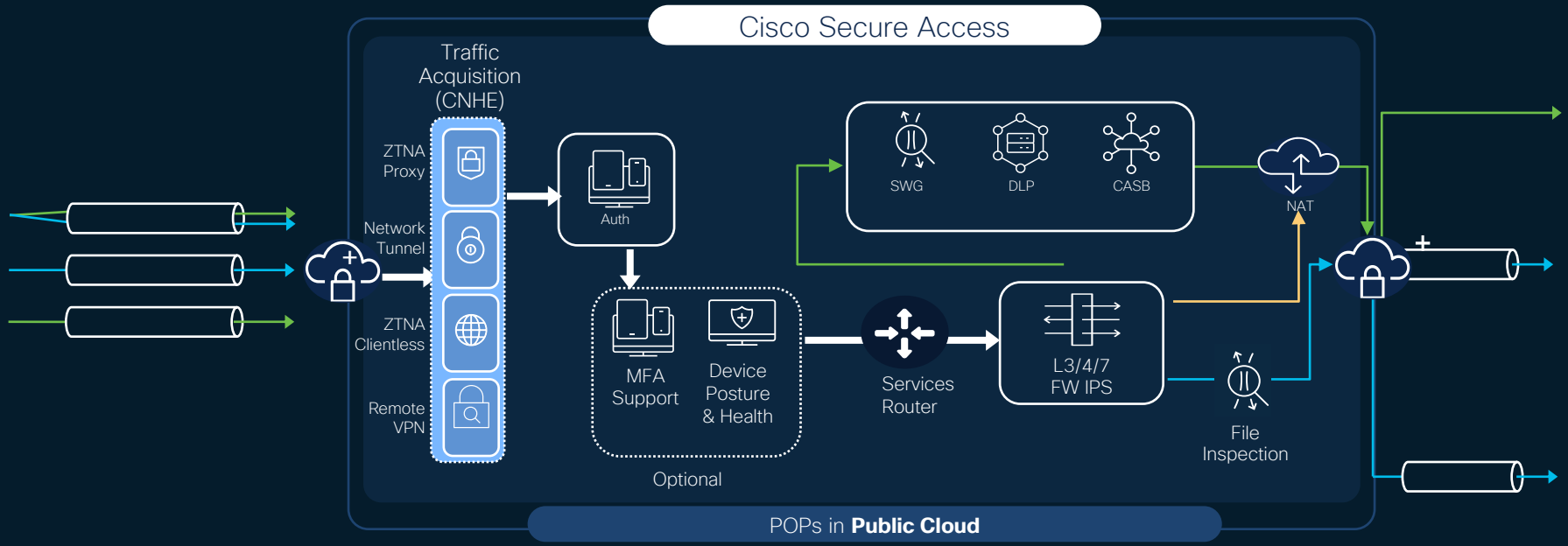
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Proven security capabilities converged in one cloud service

Single console, single client, unified policies, and single subscription

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

The glue: security services & policy flow



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Secure access regions – AWS coverage

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Secure Access Regions – SSE on Edge DCs

In Development & Coming Soon
Kingdom of Saudi Arabia (Dec.'24)

Legend

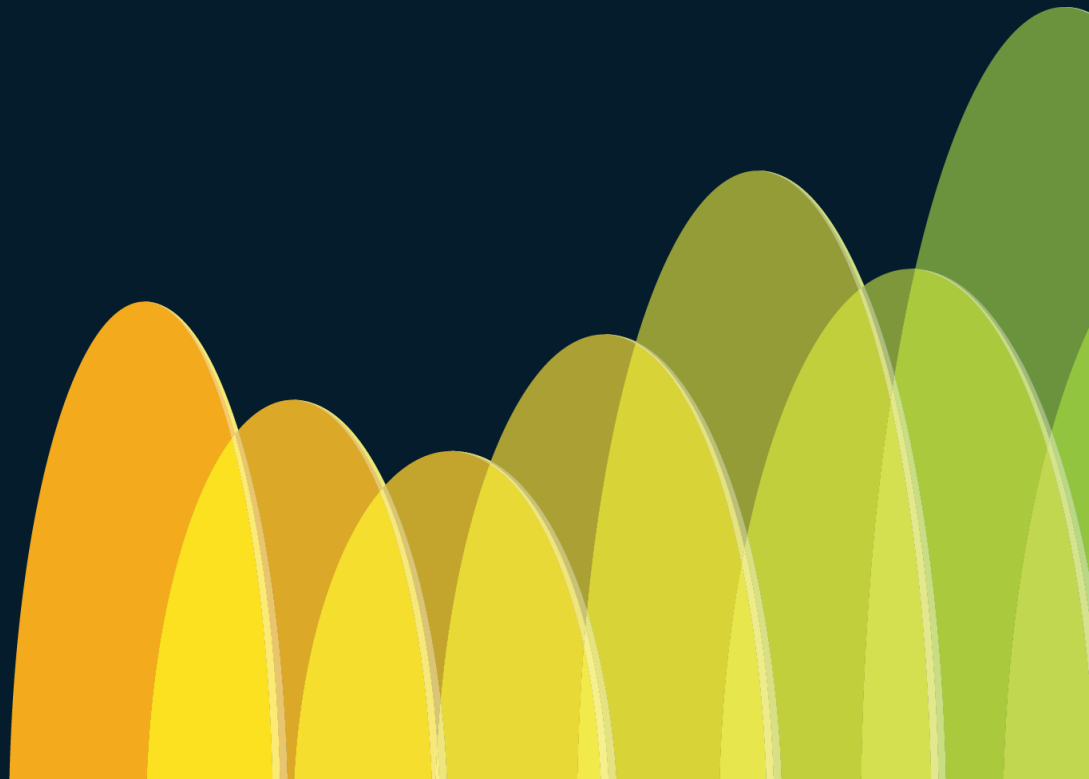
- Available
- In Development

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Secure Access Regions – Combined coverage

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Recent Innovations and Demos



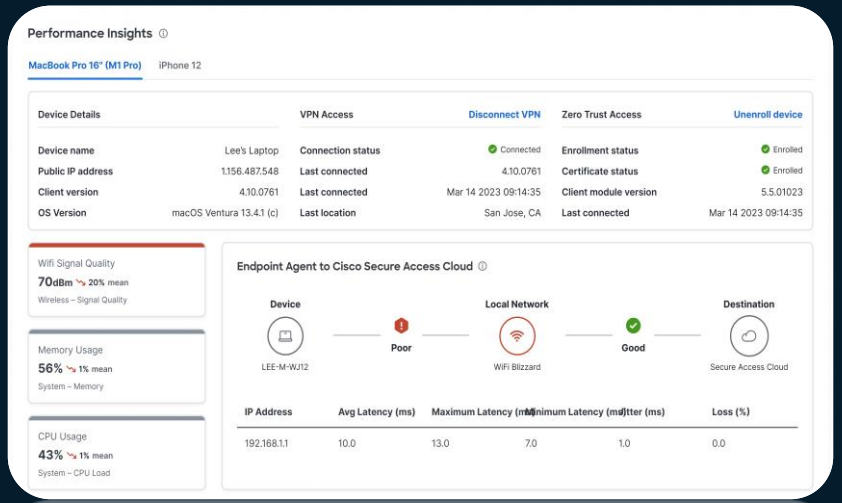
cisco Live!

POWERED BY ThousandEyes

Introducing experience insights

User experience monitoring for applications and users

Monitor health and performance as users access applications and resources



Optimise user productivity by automatically, providing details on the user's experience, enabling faster issue detection and resolution

Monitoring examples:

- Endpoint performance – CPU, memory, Wi-Fi
- Network performance – endpoint to Secure Access
- Top SaaS applications performance
- Collaboration performance monitoring
- User specific events

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

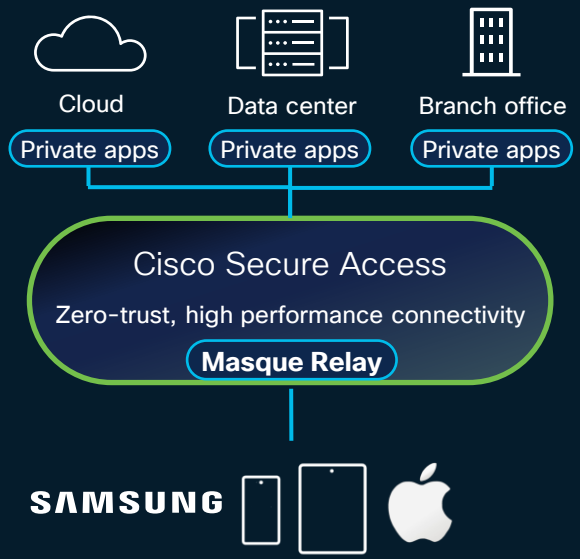
Proven reliability and strong service level agreement (SLA)

- Continuous availability of DNS and Secure Internet Access since 2006
- Modern architecture with built-in technical redundancy
- 24 X 7 Rapid Response support organisation

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Zero trust secure access from mobile devices

Apple iOS and Android on Samsung



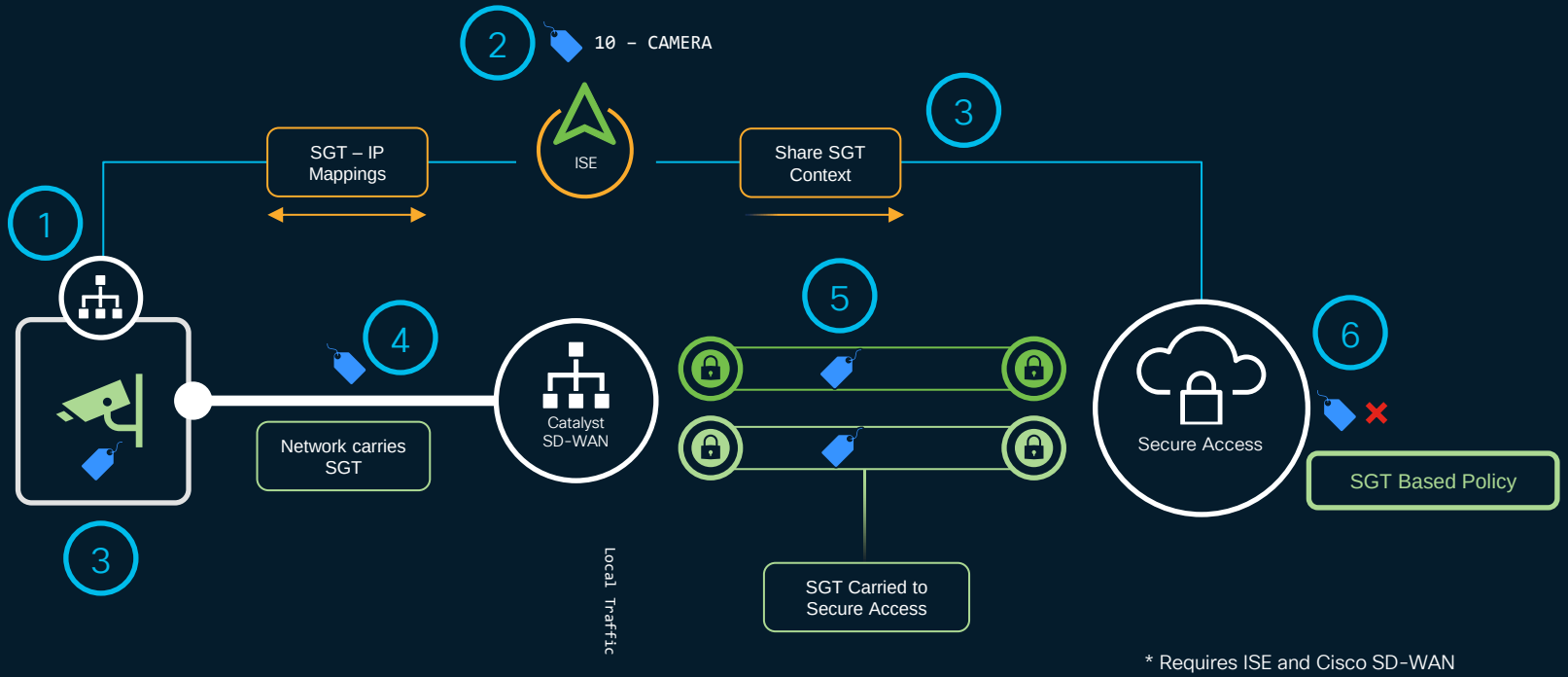
Cisco and major mobile providers collaborated to develop the industry's first zero-trust architecture for mobile devices

Technology innovation and flexibility: Either TCP/TLS or new QUIC/UDP protocols

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Security Group Tags (SGTs)

Support for IOT devices and endpoint, via integration with Cisco ISE



* Requires ISE and Cisco SD-WAN

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

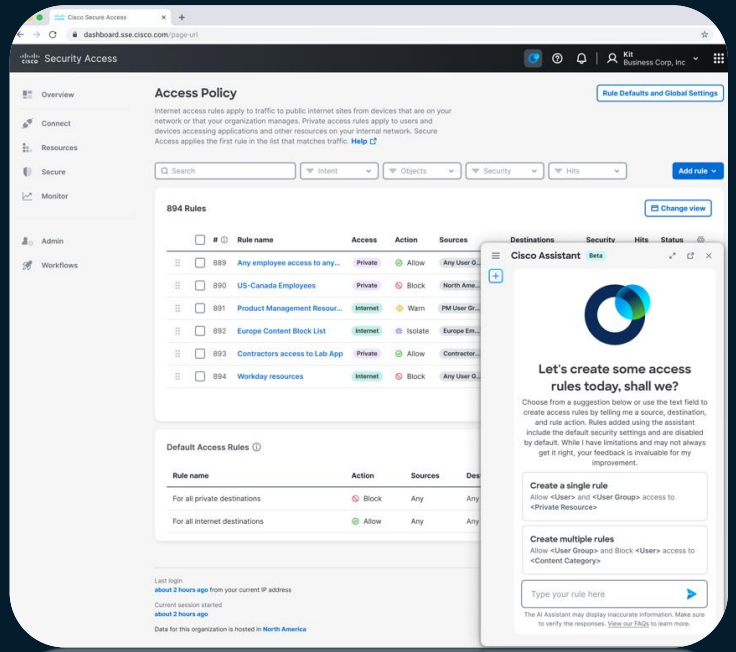
AI for Security
or
Security for AI?

How about both?

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco AI Assistant for secure access
(AI for Security)

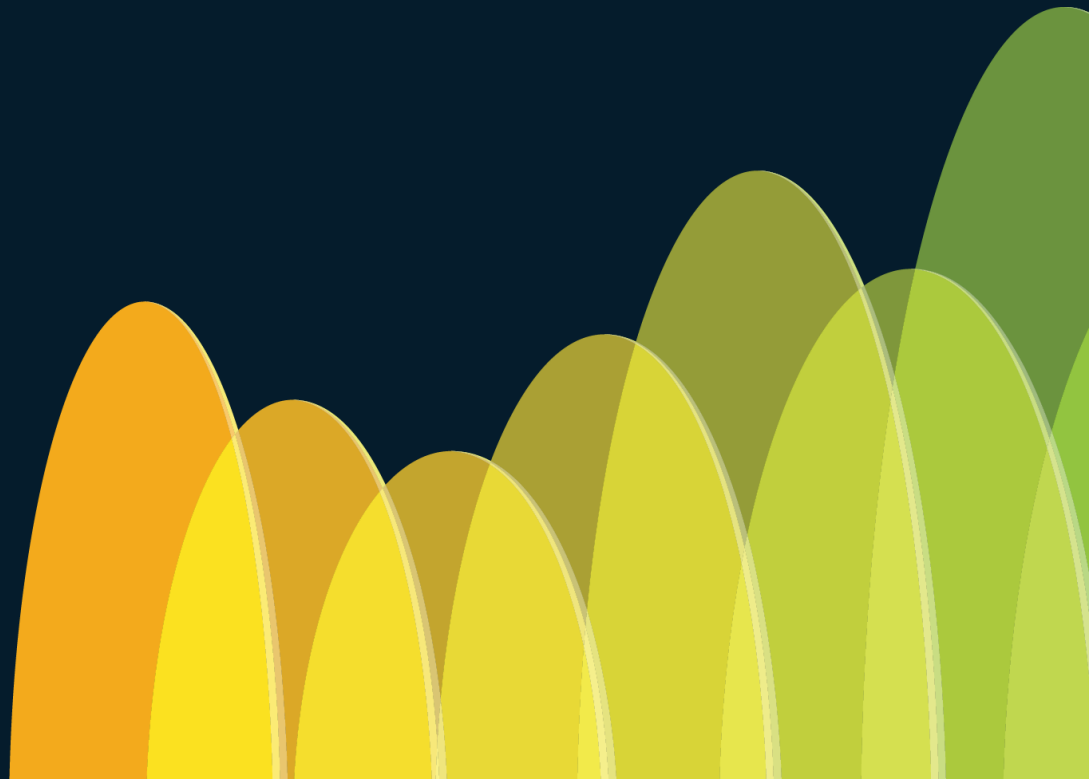
- Built with Generative AI natural language to:
  - Simplify and speed policy administration by up to 70%
  - Reduce human error
  - Improve operational efficiency



Better Efficacy. Better Experience. Better Economics.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Demo:
AI Assistant



Security for AI with Secure Access

Discover and control the usage of over 700 Gen-AI apps

Threat Visibility

Discover and Assess Activities

Leakage Prevention

DLP Inspection of Prompts/Uploads

Threat Prevention

Block Apps and Control Downloads

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Demo: Securing Gen-AI Usage with DLP

cisco Live!

Summary and QA

cisco Live!

Summary and call to action

- Cisco Secure Access: Modern innovations for SSE to solve our customers' current and future use-cases
- Emphasis on simplicity, future-proof cloud architecture to ensure scale, performance, reliability
- Integration of technologies under single dashboard, management through single policy, and simple transparent licensing
- Not the first to market, but researched over 2.5 years to address pain points customers have with other SSE solutions
- Remember, the early bird gets the worm, but...
  the second mouse gets the cheese!

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

cisco Live!

Keynote Deep Dives

Wednesday
10:30am –11:30am

Experiences Amplified: How AI Can Fuel Better Employee and Customer Experiences

Level 1
Room 106

Smart, Secure, Seamless: Transforming Experiences with Next-Generation Networking

Level 2
Room 204

Harness a Bold New Era: Transform Data Centre and Service Provider Connectivity

Level 2
Room 203

Securing User to Application and Everything in Between

Level 2
Melbourne Room 2

Unlocking Digital Resilience through Unified Observability

The HUB
Centre Stage

Complete Your Session Evaluations

Complete a minimum of 4 session surveys and the Overall Event Survey to claim a **Cisco Live T-Shirt**.

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

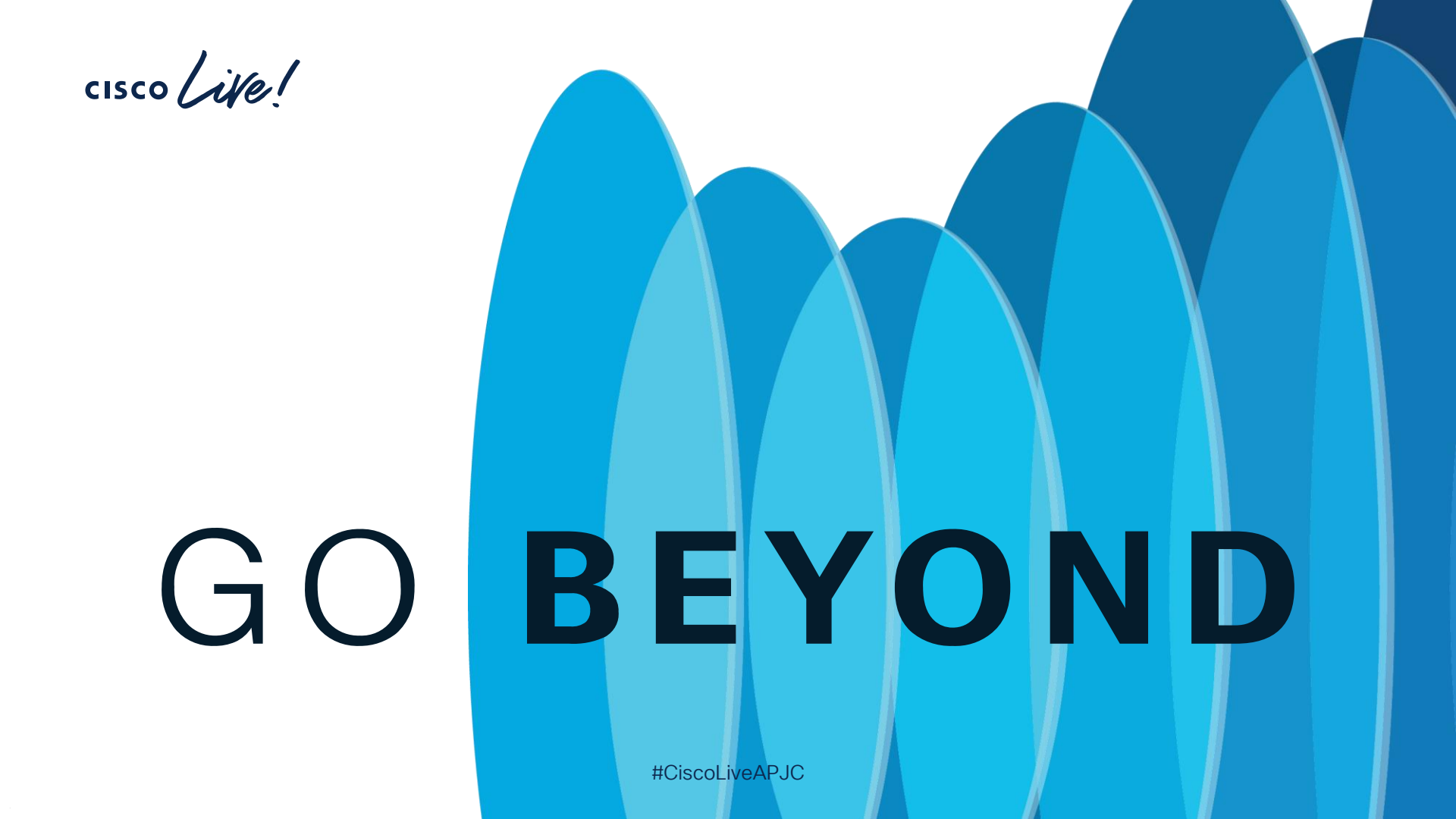
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Continue your education

- Visit the Cisco Stand for related demos
- Book your one-on-one Meet the Expert 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

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

cisco
Thank you
cisco Live!
#CiscoLiveAPJC


cisco Live!
GO BEYOND
#CiscoLiveAPJC