Cisco Secure Access: Overview and End-to-end flow review

Jaki Hasan
Solutions Engineer

Fay Lee
Technical Marketing Engineer

Session ID: 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, 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

Agenda

1. Session introduction
2. Setting the scene for Cisco Secure Access
3. What have we built?
4. Architecture and flow
5. Recent innovations and demos
6. Summary and Q&A

Let’s Set the Scene and Session Expectations

Today’s businesses depend on a new approach

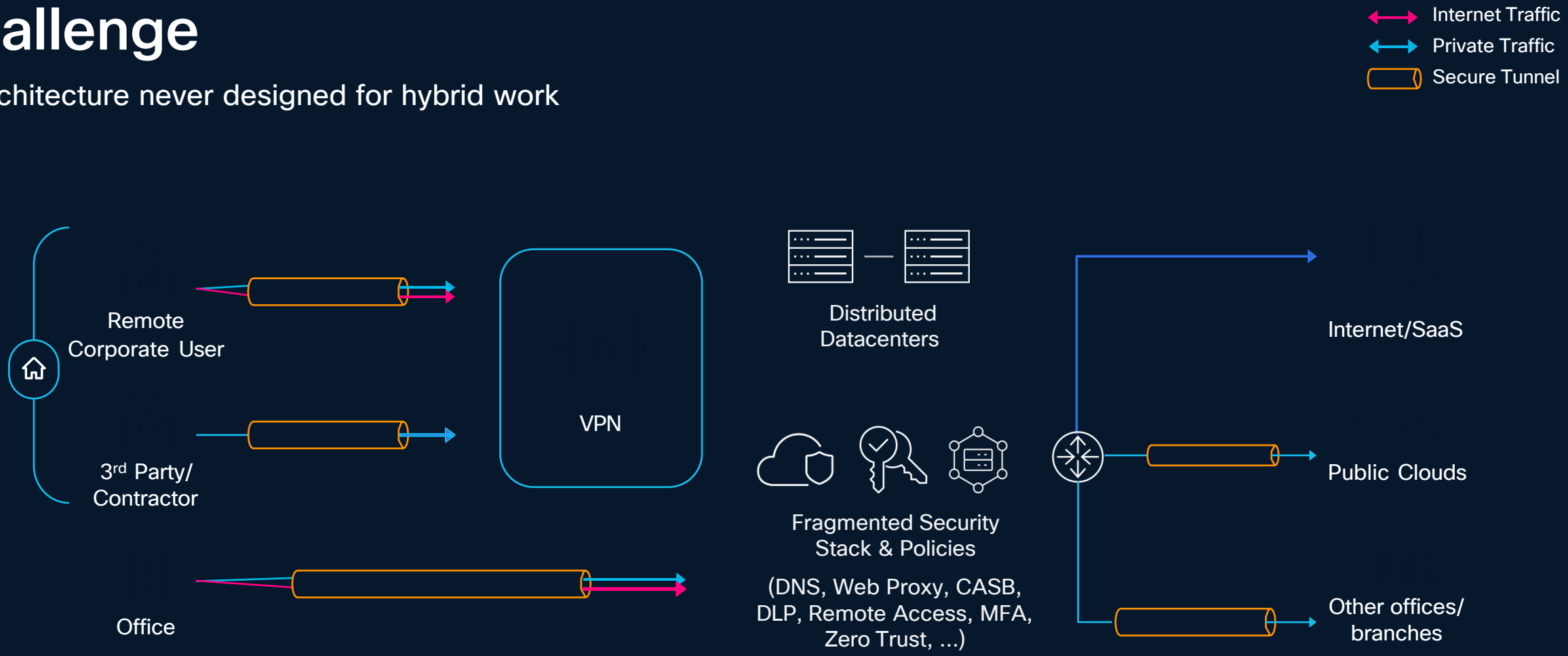
Cisco Secure Access, Cisco’s SSE

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

cisco

Challenge

An architecture never designed for hybrid work

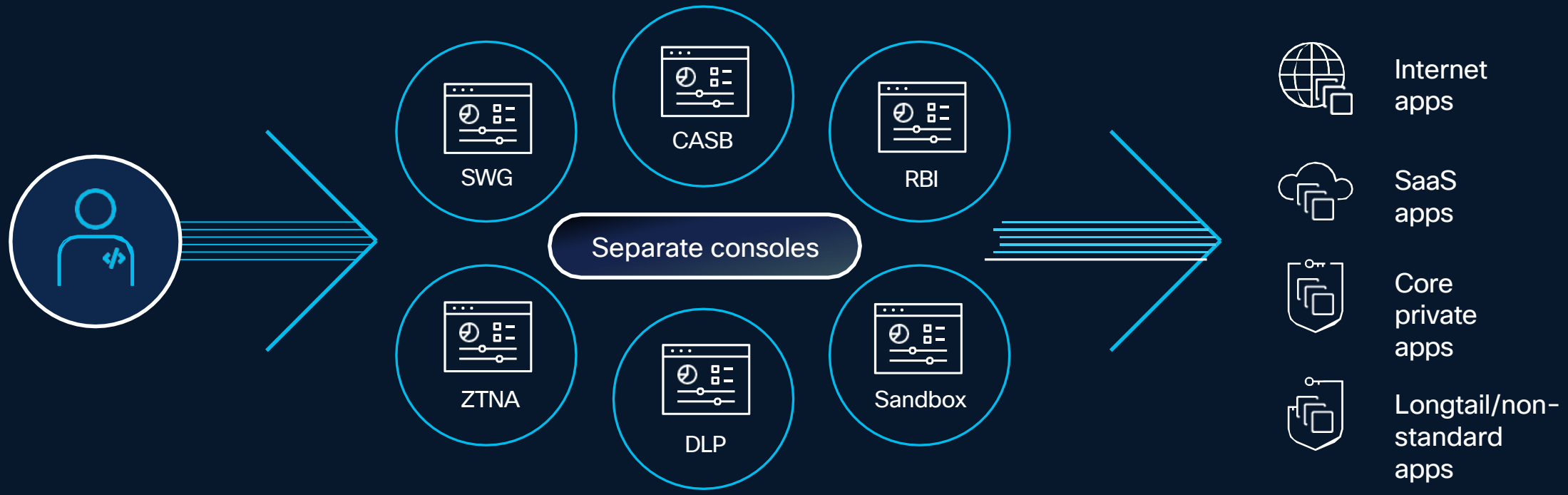


Poor user experience
Lower productivity

Large sets of individual solutions and vendors
Complexity of operations and costs

Gaps in security posture born out of complexity and fragmentation

The multi-vendor approach is problematic



New threats spawn new vendors, putting the burden on customers

What have we built?

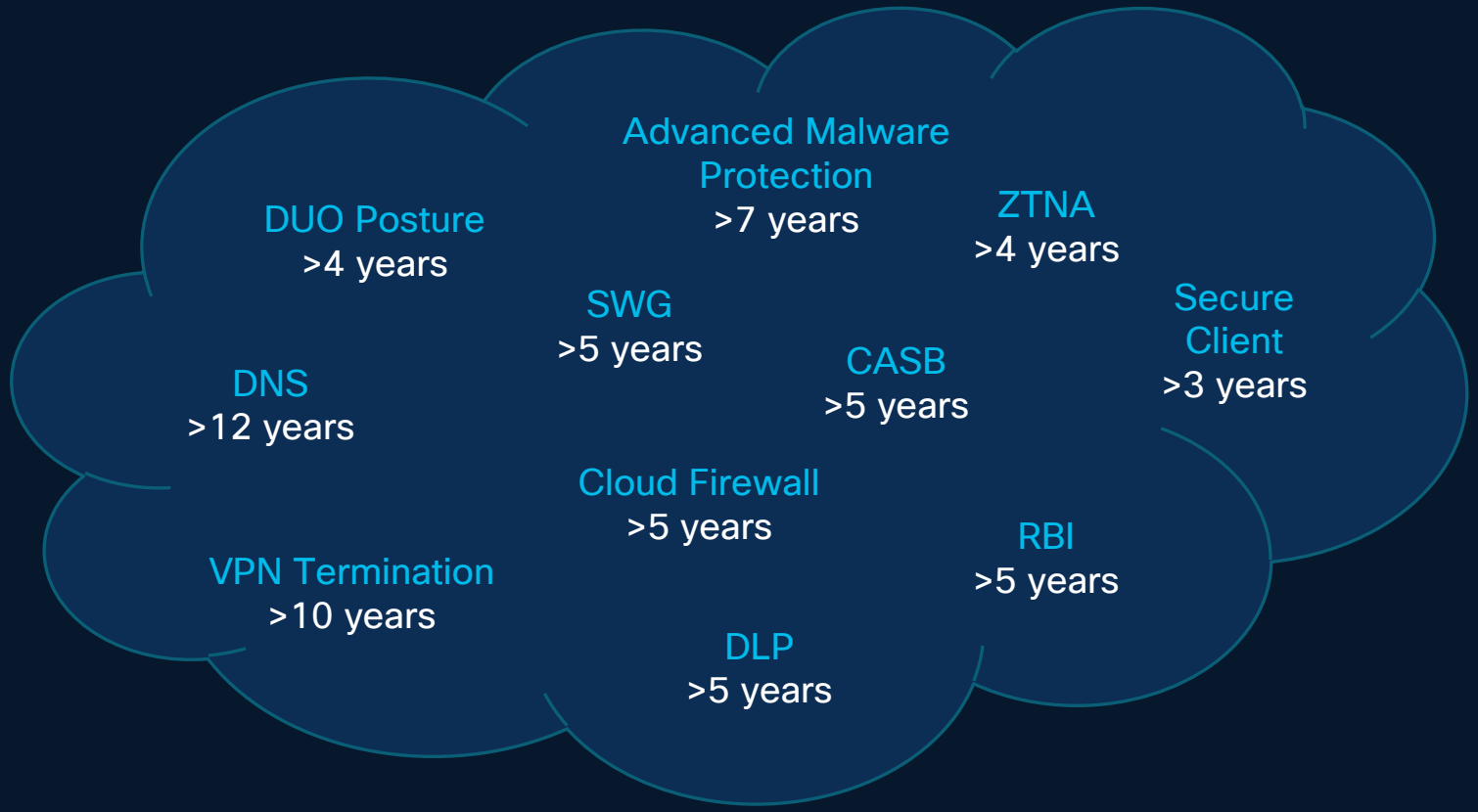
Cisco Secure Access
Better for users, easier for IT, and safer for everyone

Cisco Secure Access

Extended SSE security grounded in “identity first” zero trust

Cisco Secure Access

Proven cloud-native security converged into one service

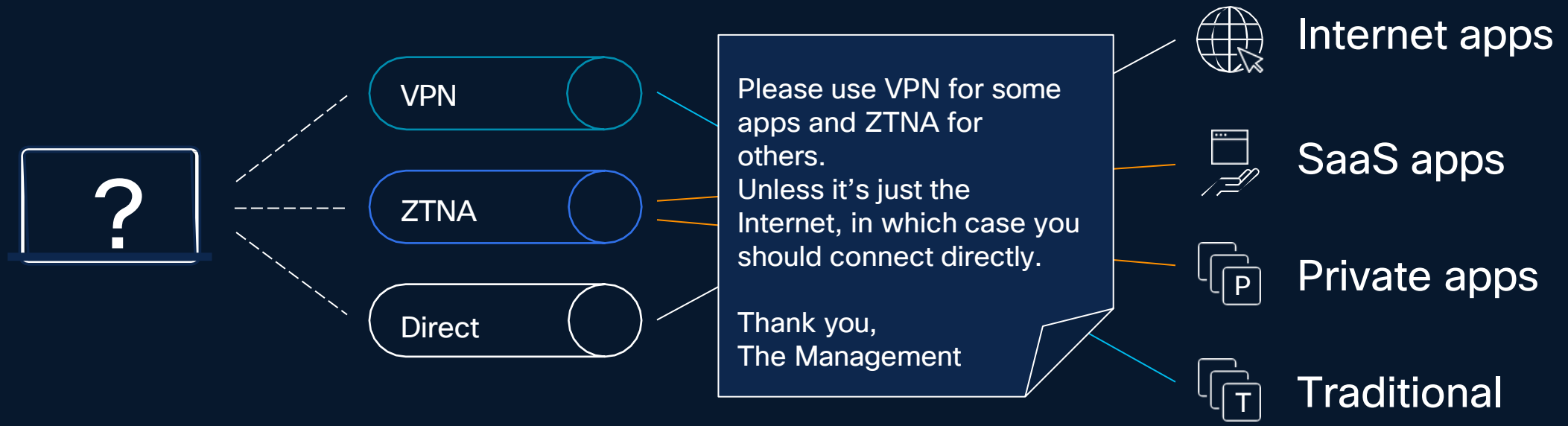


- Single Console
- Single Client
- Unified Policies

Protecting 30,000+ customers | More than 220M endpoints

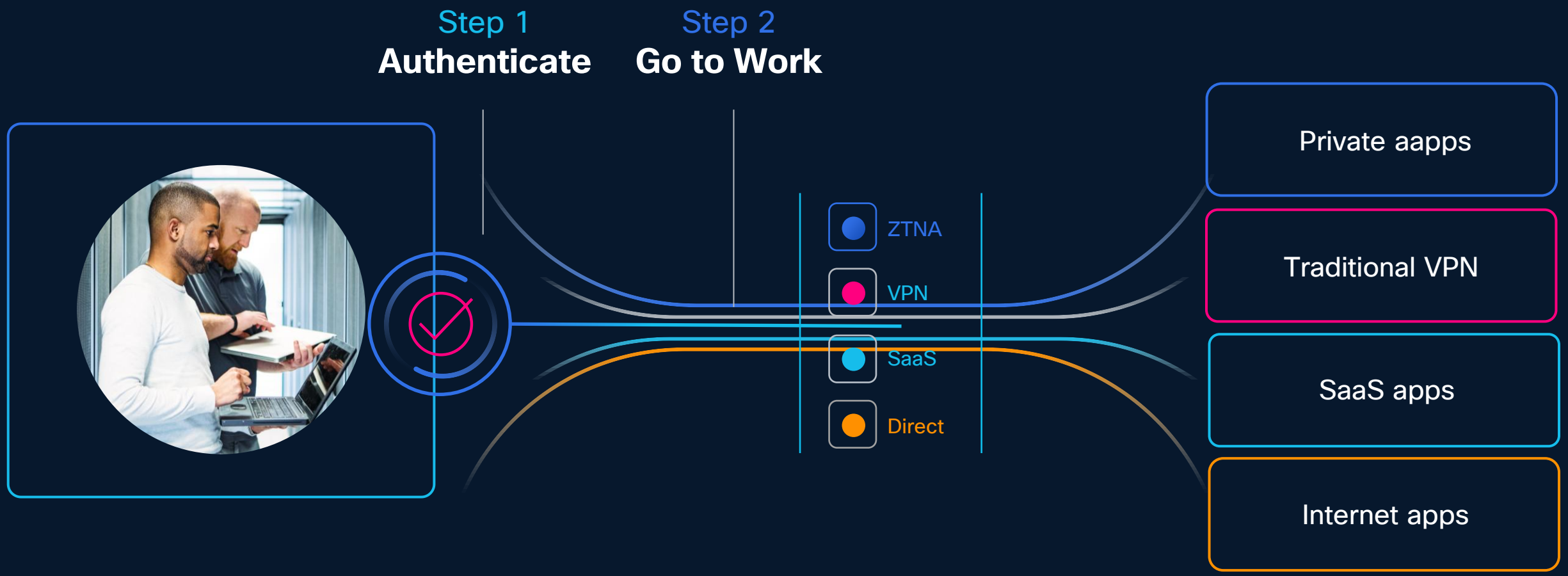
Eliminate unnecessary end-user decisions

How would you like to connect to your applications?



Reimagine the user experience

Cisco Secure Access makes the connection you need



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

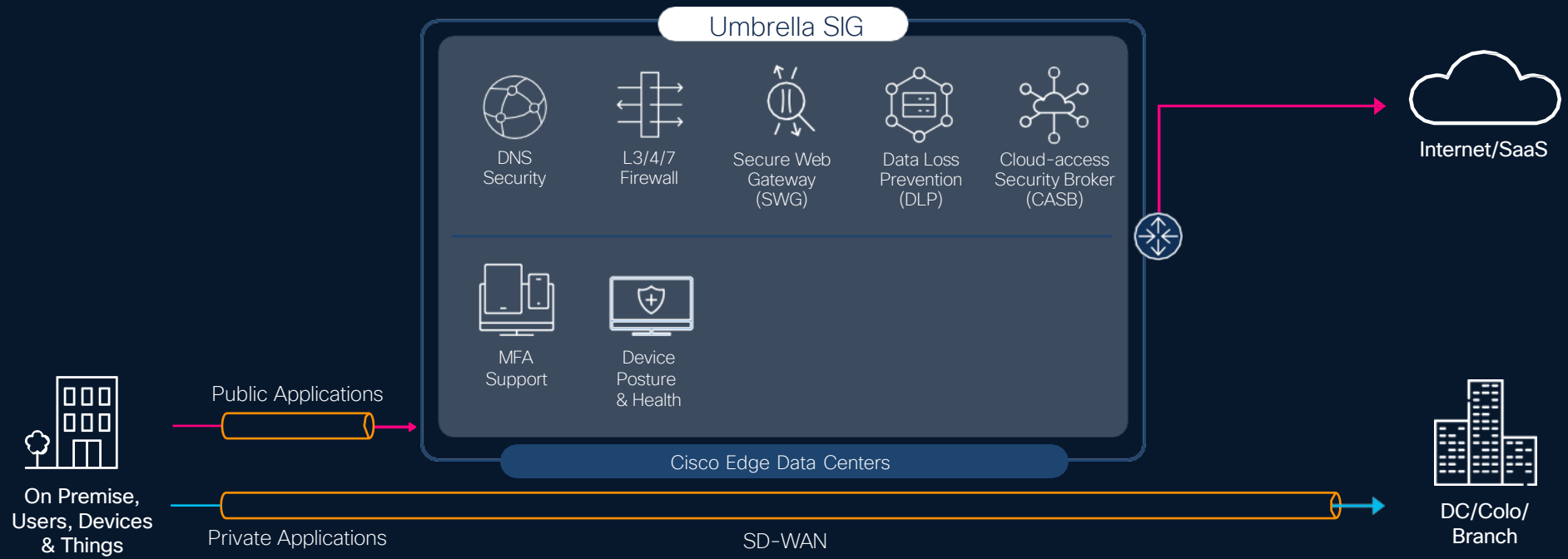
Architecture and Flow Drill-down

Evolution from Cisco Umbrella SIG

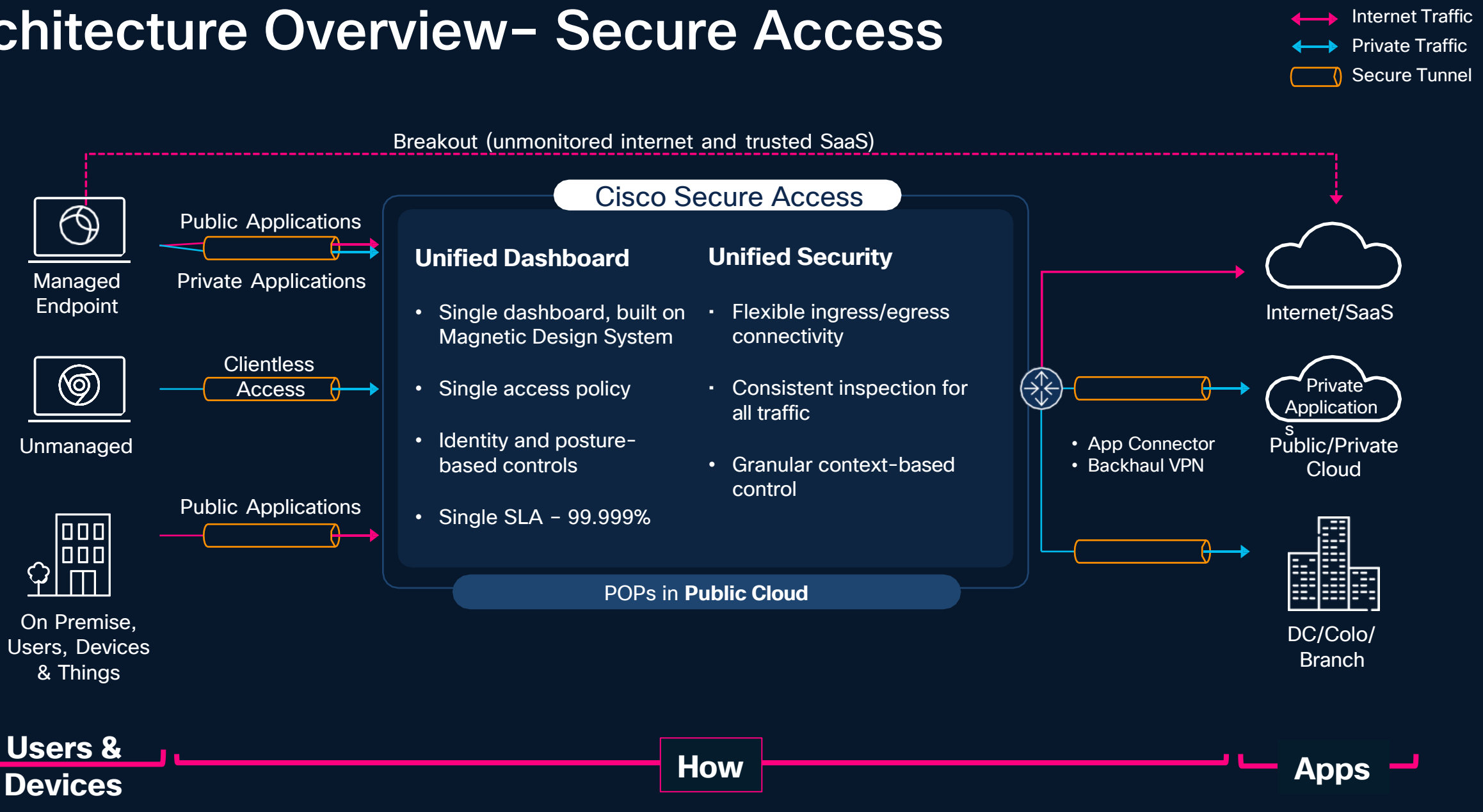
Internet Traffic
Private Traffic
Secure Tunnel

Main use-cases

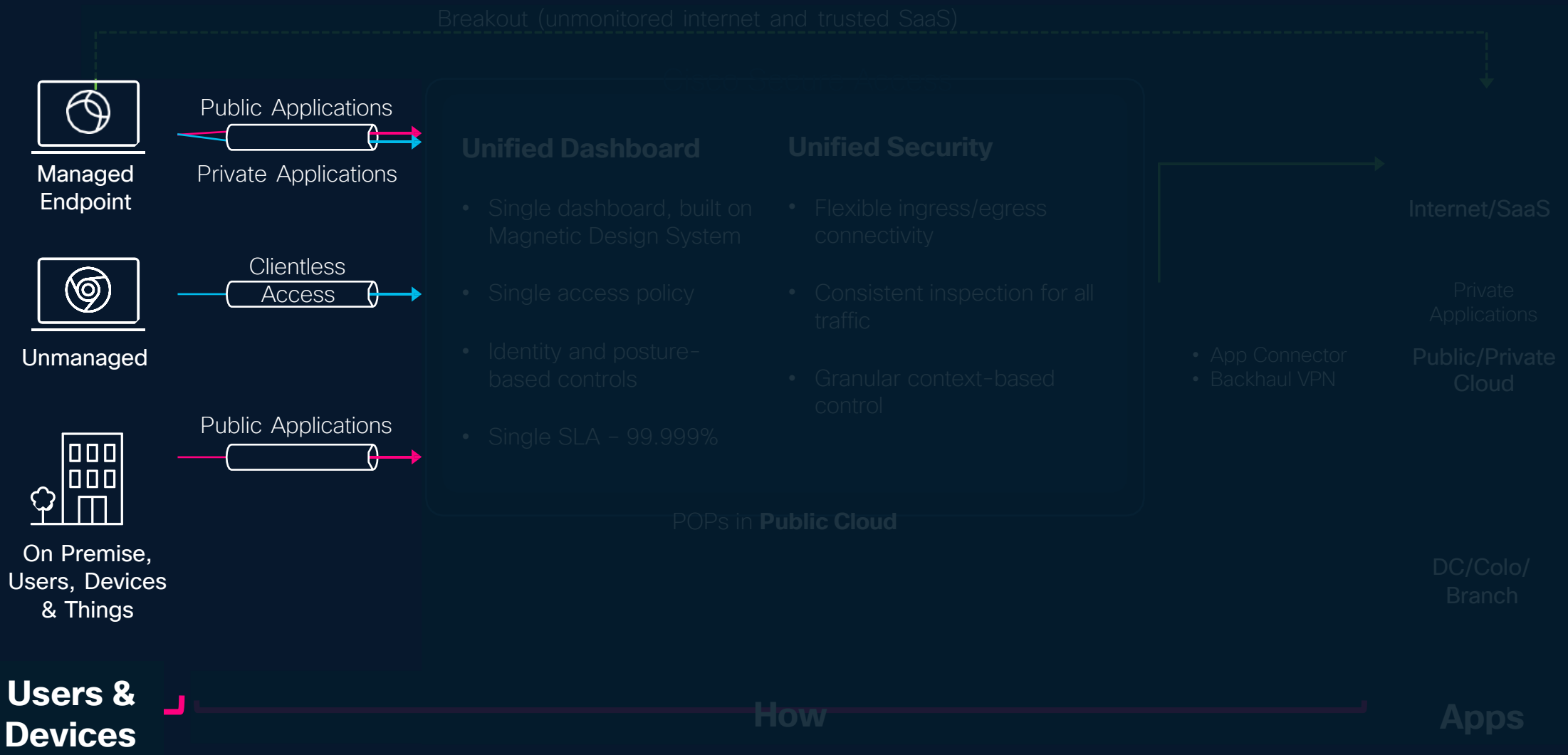
- Secure Internet Access
- POPs in Cisco Edge Data Centers
- Meraki and Viptela SD-WAN Integration from DIA to SIA



Architecture Overview- Secure Access



Architecture Overview – Connecting Who & What



Any connect>>Cisco Secure Client

Suite of security service enablement modules

AnyConnect VPN (Core)

ZTA Module

ISE Posture

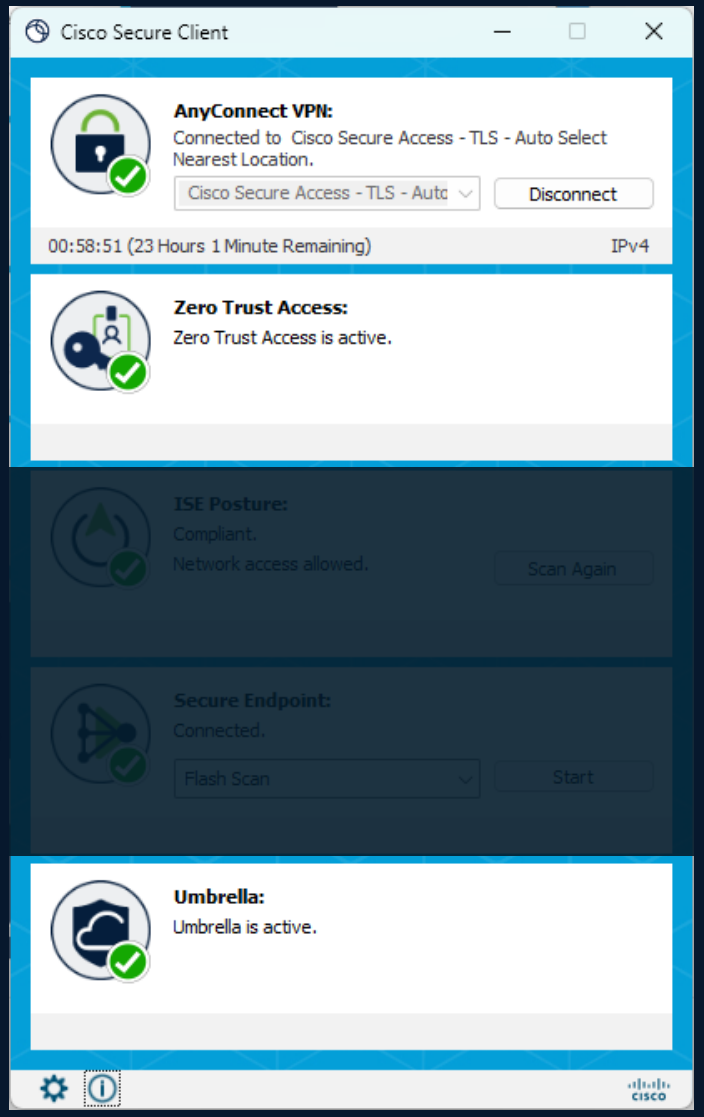
Secure Endpoint (AMP)

Roaming Module

Thousand Eyes (No UI)

Cloud Management Module (No UI)

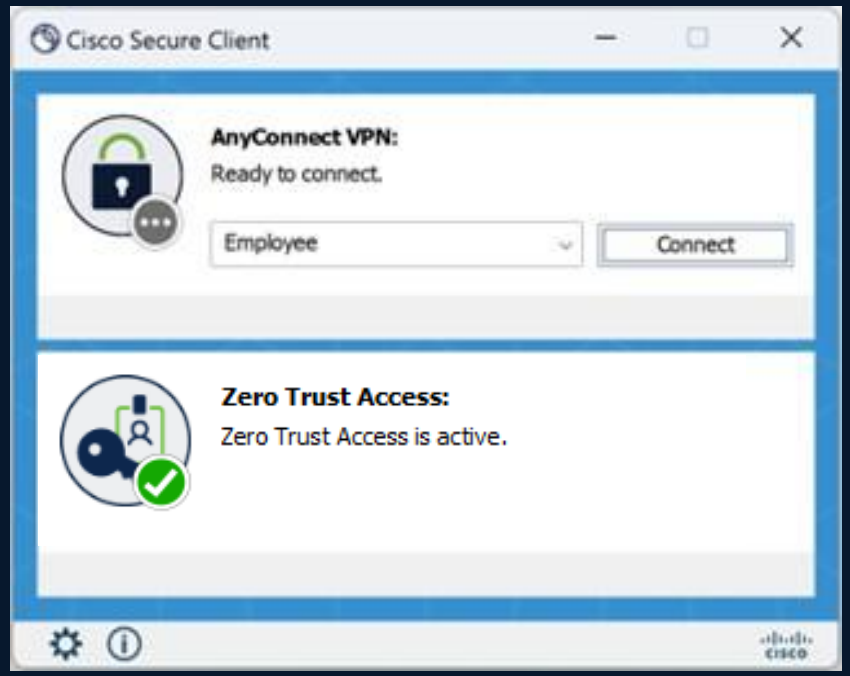
Diagnostic and Reporting (DART)



Zero Trust Access Module

- 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 (for private and Internet
- 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.
- 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)

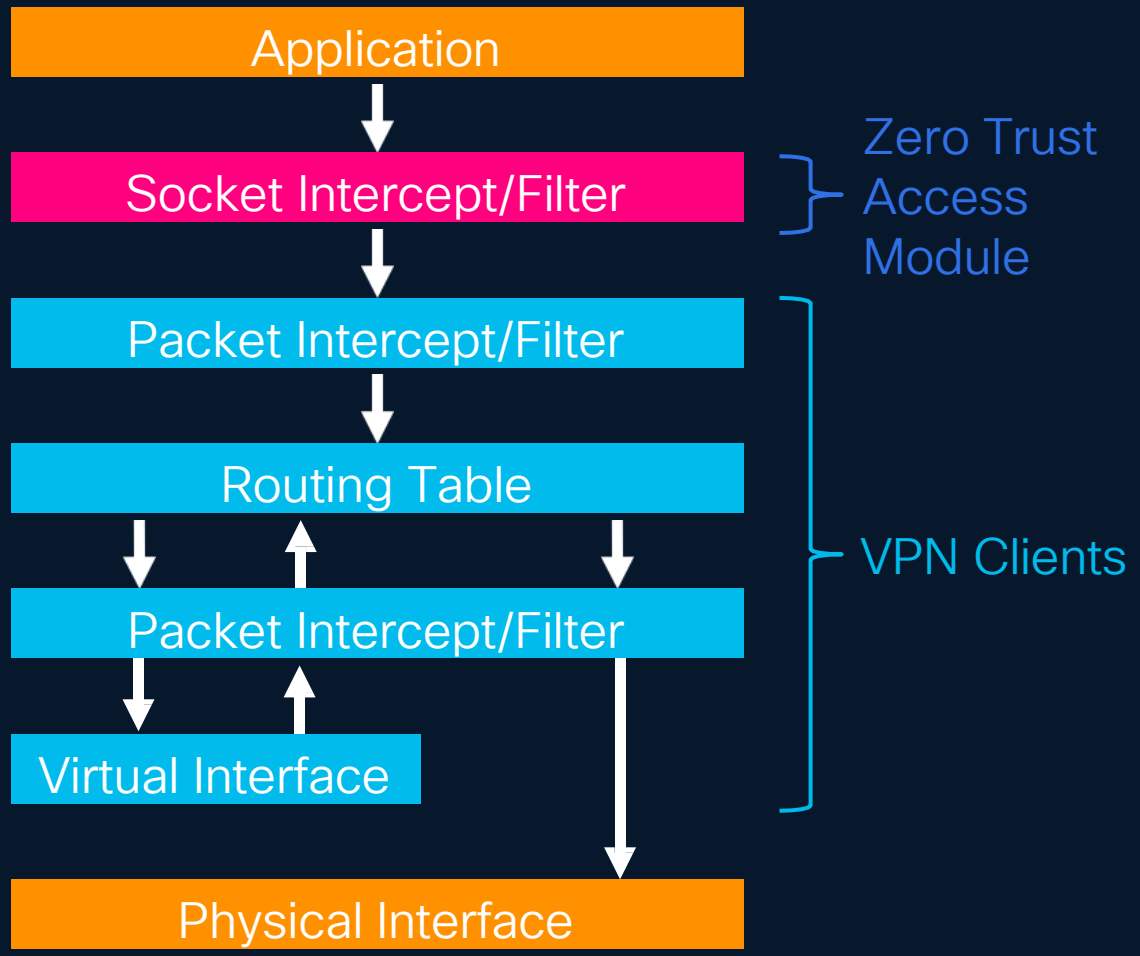
- IETF working group focused on next generation proxying technologies on top of the QUIC protocol
- Provides the mechanisms for multiple proxied stream and datagram-based flows inside HTTP/2 and HTTP/3
- Used by iCloud Private Relay since 2021
- HTTP/2 and HTTP/3 extensions allow for the signaling and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

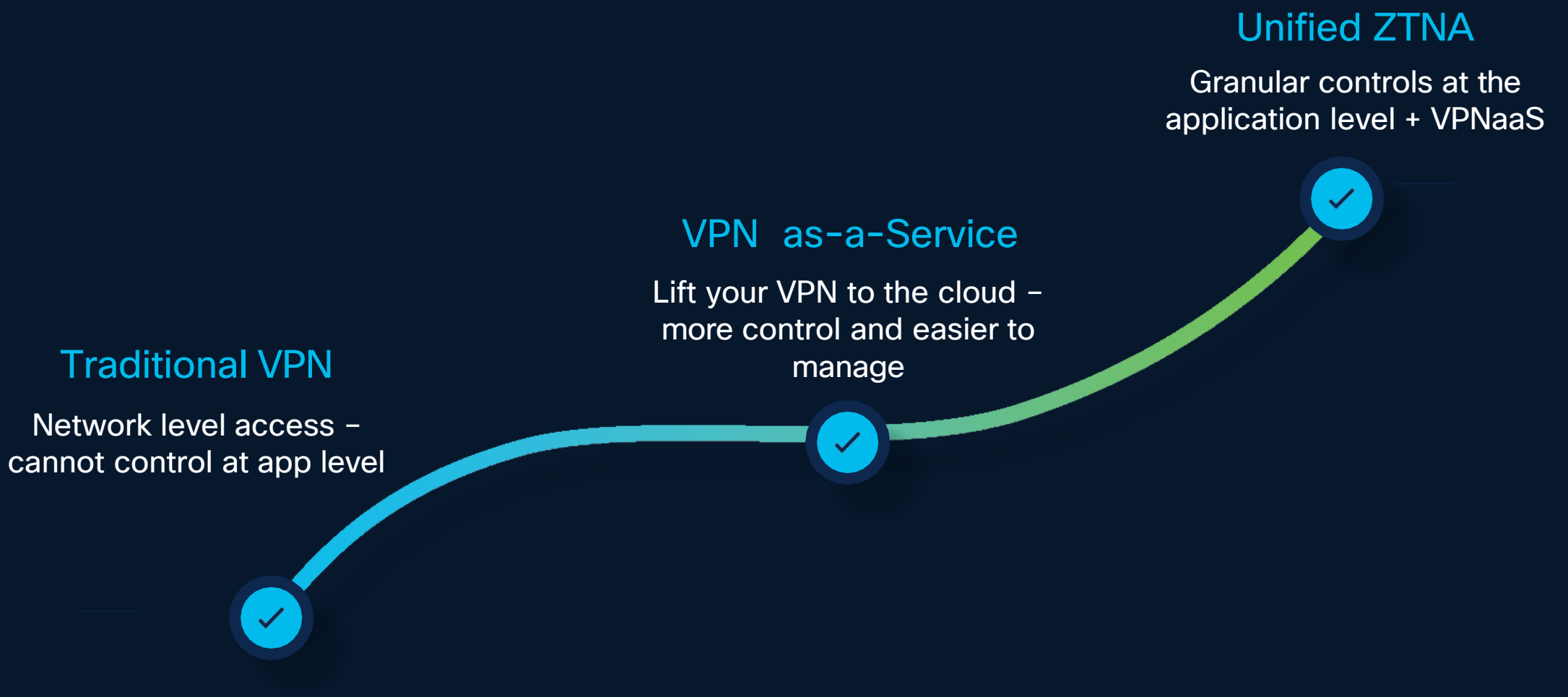
Zero Trust Access Module- socket intercept

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



Simplify the journey to zero trust with migration



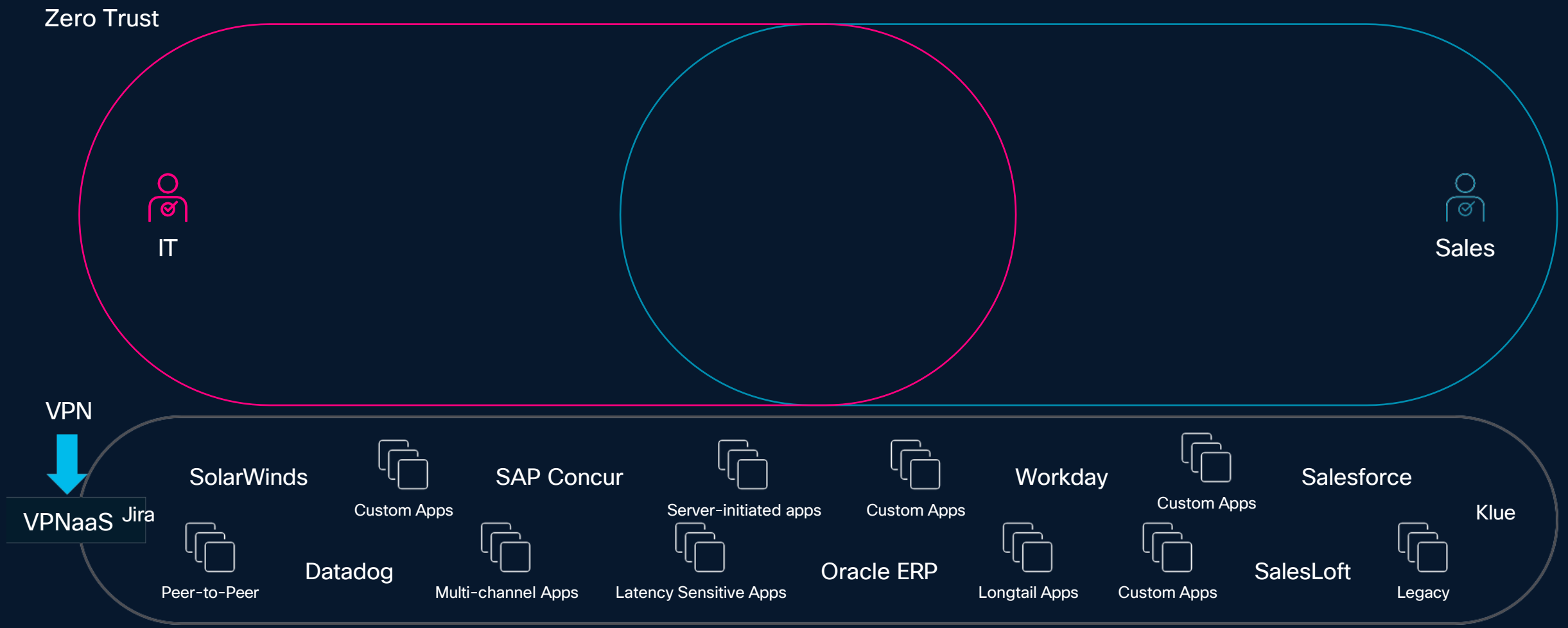
App compatibility with zero trust

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

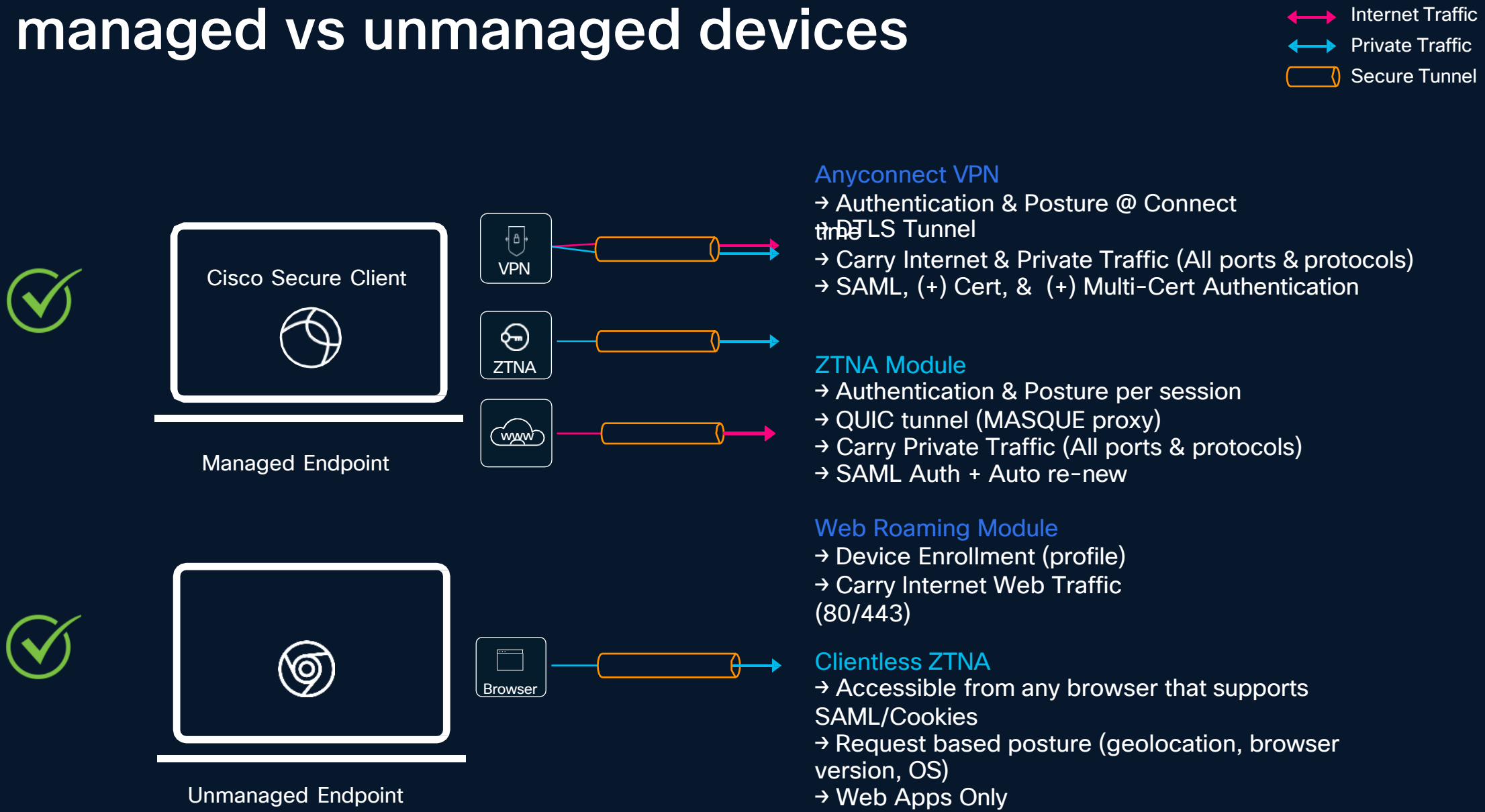
- Client-to-client traffic (i.e. peer-to-peer VoIP)
- Server-to-client traffic (i.e. remote desktop; remote assistance)
- Applications that require a unique client IP (i.e. SMBv1)
- Applications that require SRV DNS records (i.e. Active Directory, Kerberos, MS Configuration Manager, SCCM)
- Apps that 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

Simplifying the journey to zero trust



Who: managed vs unmanaged devices



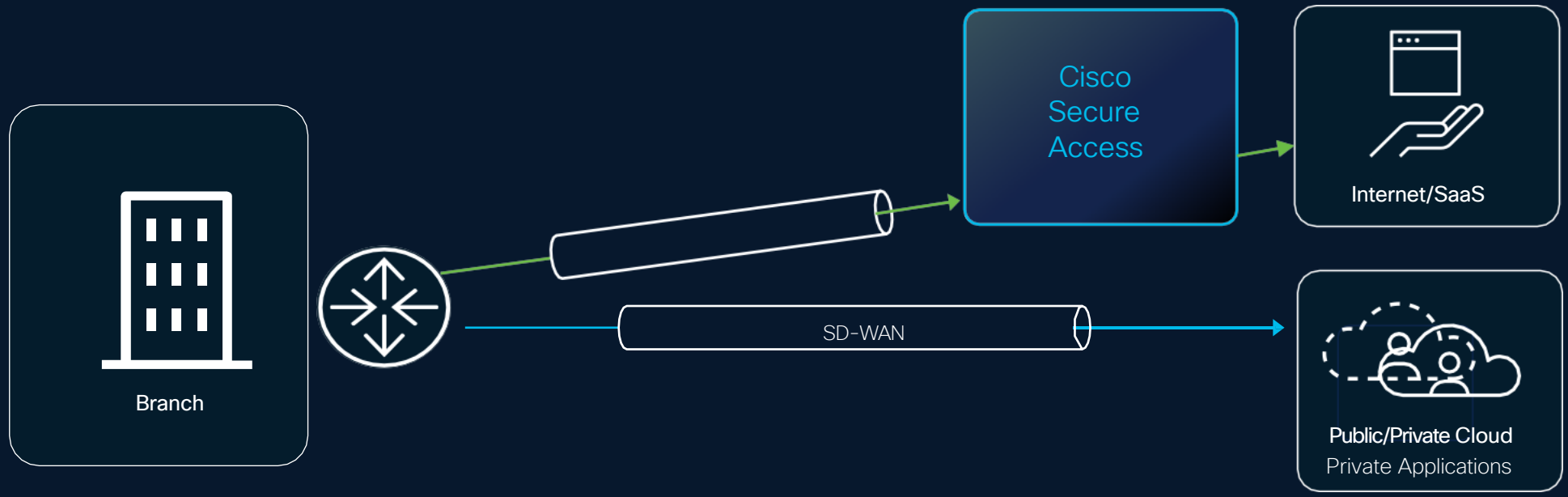
Anyconnect VPN
→ Authentication & Posture @ Connect time
→ DTLS Tunnel
→ Carry Internet & Private Traffic (All ports & protocols)
→ SAML, (+) Cert, & (+) Multi-Cert Authentication

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

Who & What: branch users and devices connectivity

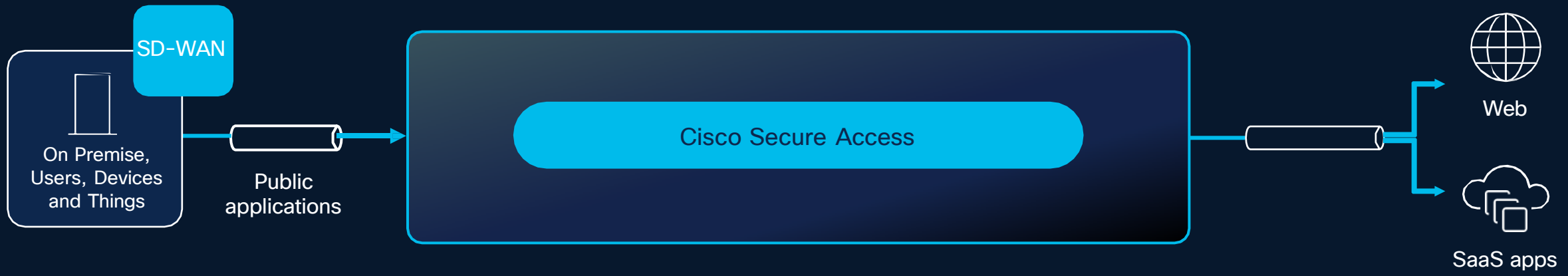


Branch Devices

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

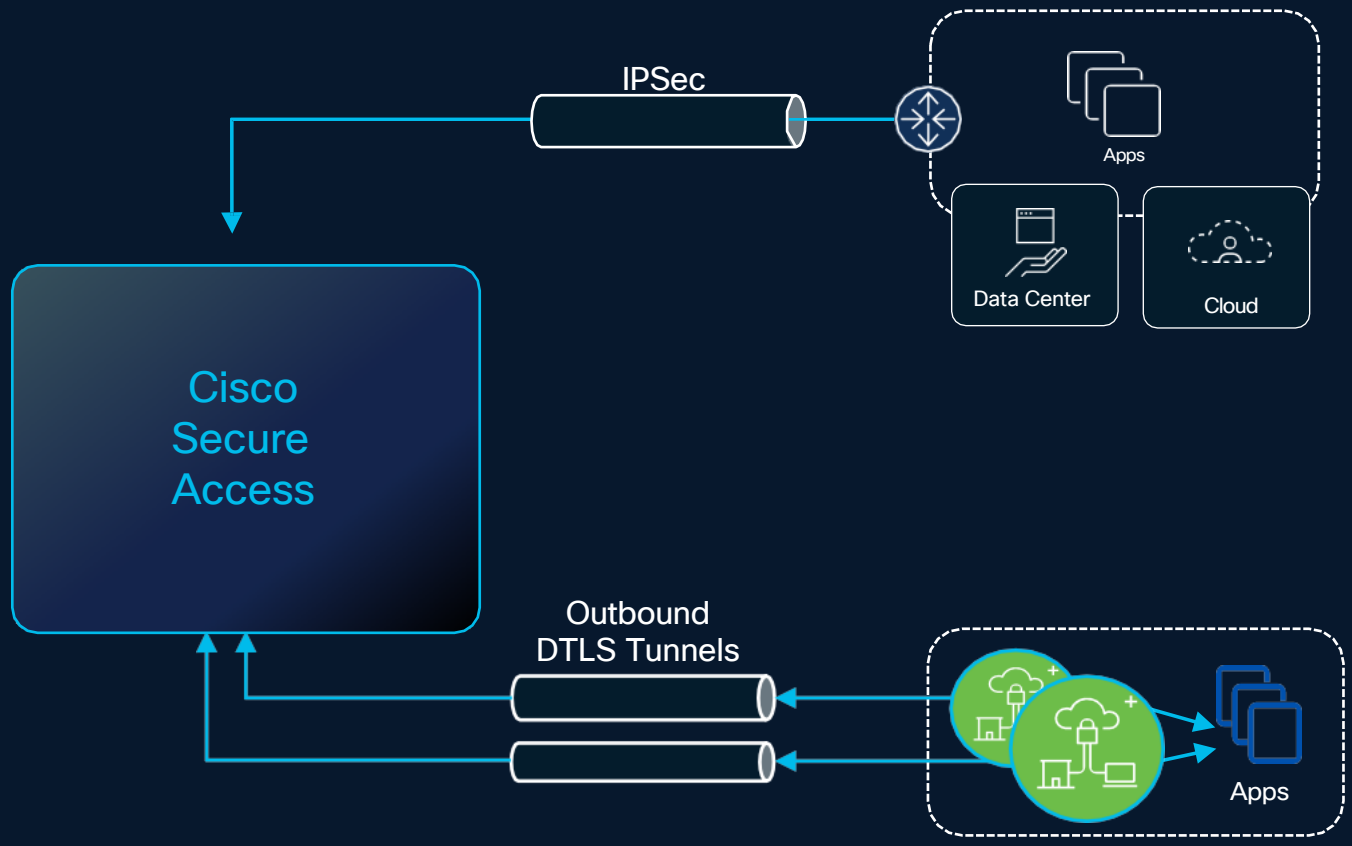
Cisco Catalyst SD-WAN & Secure Access integration

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

Apps: private applications



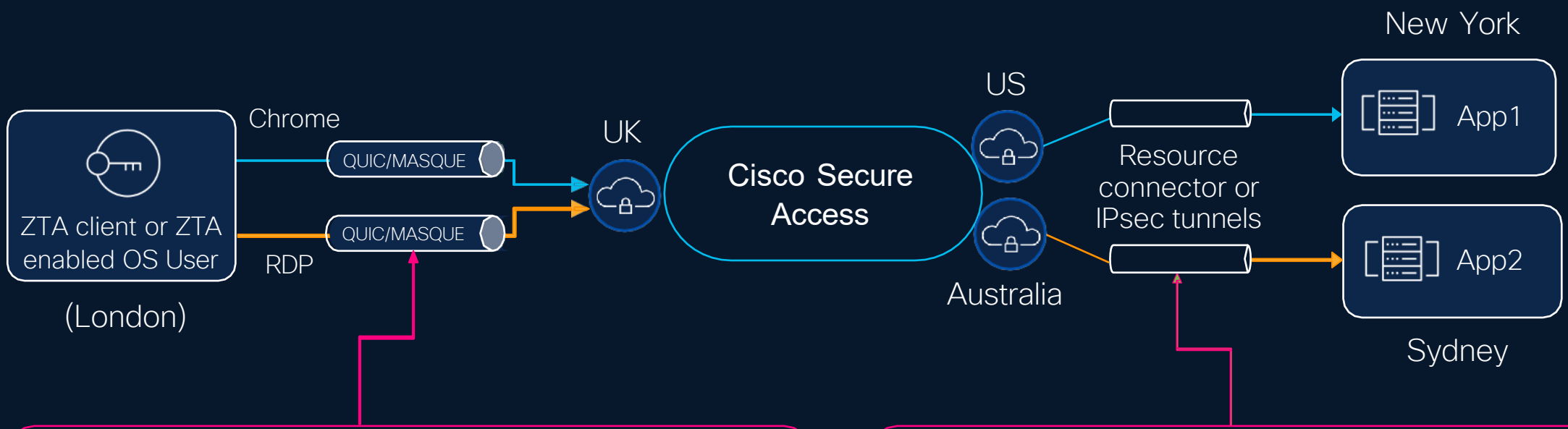
Network Tunnel

→ IPSec/SD-WAN 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

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

Apps: Internet/SaaS applications

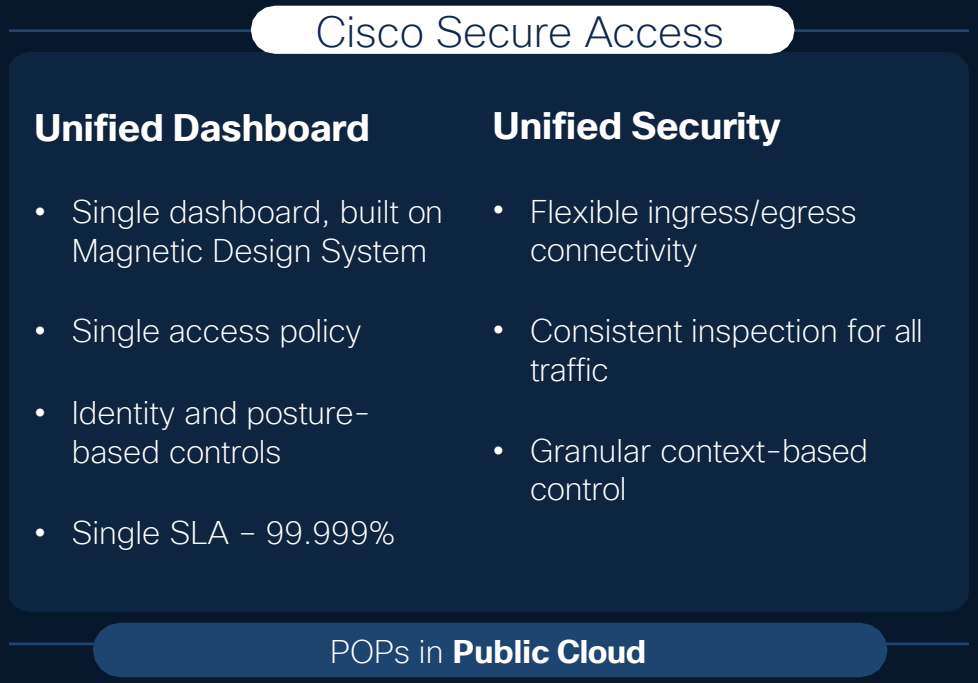
Trusted SaaS/Bypass

→ 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)

Security Services

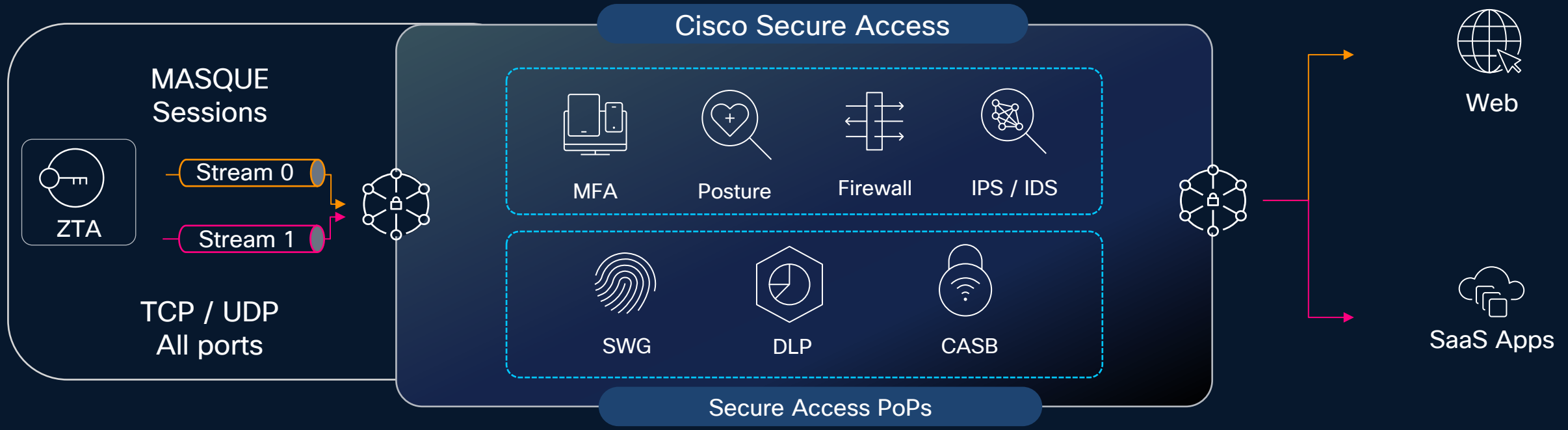


How

Recent Innovations & Demos

Client-based Zero Trust Access

Internet Connectivity



- Transparent user experience
- Trusted Network Detection
- Service managed client certificates with TPM-protected key storage

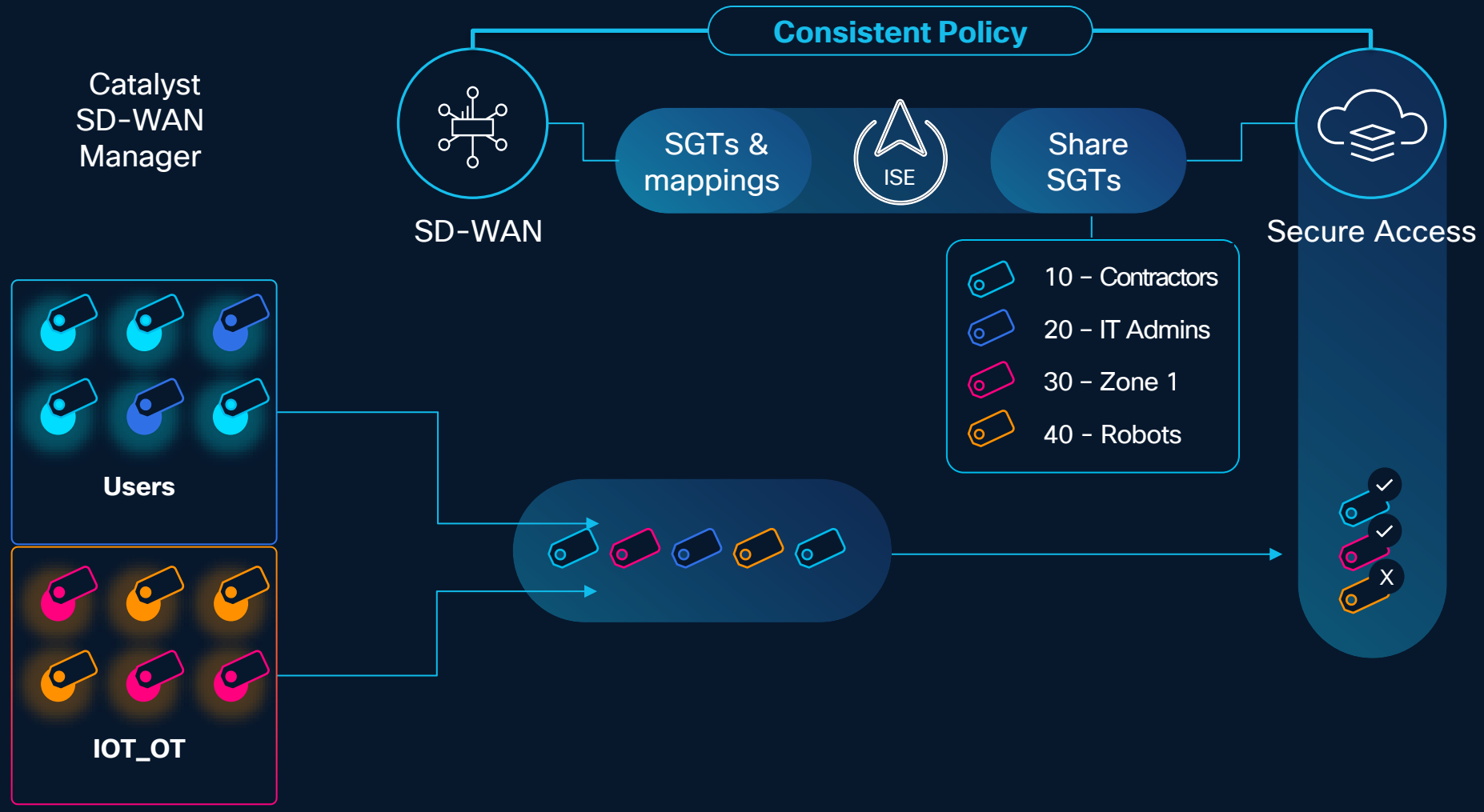
- Session-based security
- No VPN tunnels
- User and group-packet steering
- User and group-based policy

cisco

Identity Services Engine (ISE)

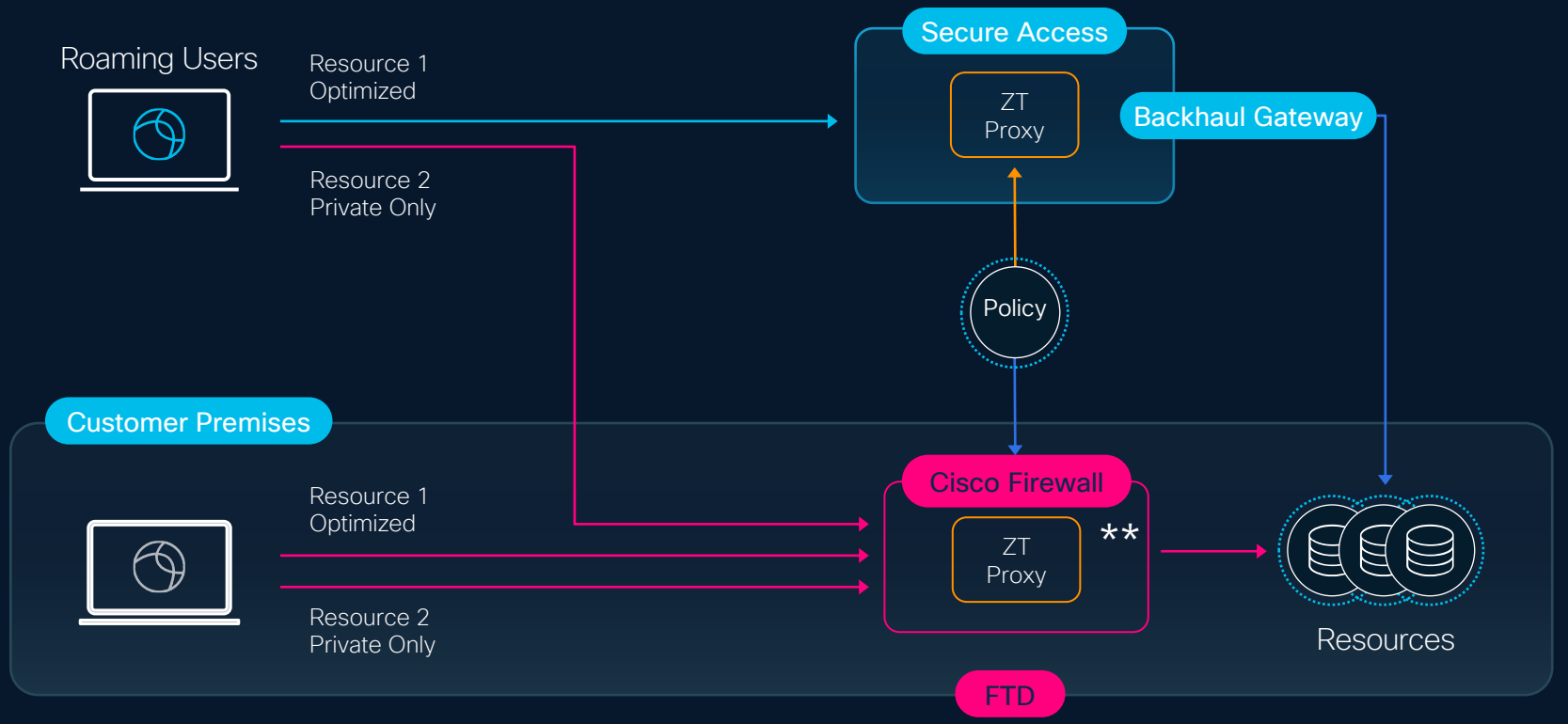
Leverage SGTs for granular access control

- 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



Hybrid Private Access for Flexible Enforcement

Single set of ZTNA policies used in cloud and on-premise



Complete your session evaluations

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

Earn up to 800 points by completing all surveys and climb the Cisco Live Challenge leaderboard.

Level up and earn exclusive prizes!

Complete your surveys in the Cisco Live Events app.

Continue your education

Visit the Cisco Stand for related demos

Book your one-on-one Meet the Expert meeting

Attend the interactive education with Capture the Flag, and Walk-in Labs

Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

Thank you


CISCO