cisco Live!

Let's go

The bridge to possible

Cisco Secure Access

Cisco's latest SSE innovation

Anders Piilmann, Solution Engineer
apiilman@cisco.com

A little about me

- I have **28 years** of experience in the network and security
- Covered operations, design, and architecture.
- I have experience with most of the vendors in IT infrastructure and security.
- Done architecture, design, and leading implementations of solutions ranging from 100k+ of users down to SMBs.

What is session about

- This session is a technical introduction to Cisco Secure Access
- Typical Use Cases
- Cisco Secure Access high level architecture
- Which components make up Cisco Secure Access

- So, if you are already familiar with Cisco Secure Access this session is probably not for you ☺

What is this session NOT about

How to configure Cisco Secure Access

Deep technical dive

How to sell Cisco Secure Access

Let’s dive in

Cisco Secure Access gives your users easy and consistent access from anywhere in world.

Agenda

- Introduction to CSA
- The Architecture of CSA
- SD-WAN Integration
- Resource Connector
- Private Application Access (ZTNA) and Remote Access VPN
- Use Cases
- Digital Experience Monitor

Introduction to CSA

Why Cisco Secure Access?

Operational and Security Challenges Remain for IT

Multi-vendor/tool approach is very common, and can be a challenge to manage

Multiple agents to install and manage

IT/Security Admin

SWG agent

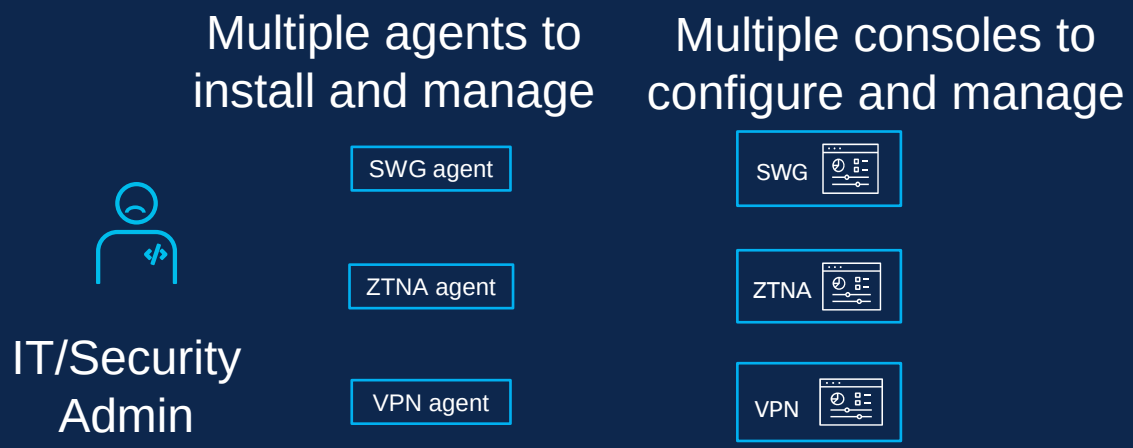
ZTNA agent

VPN agent

- Licenses/hardware
- Cumbersome deployments
- Increased attack surface

Operational and Security Challenges Remain for IT

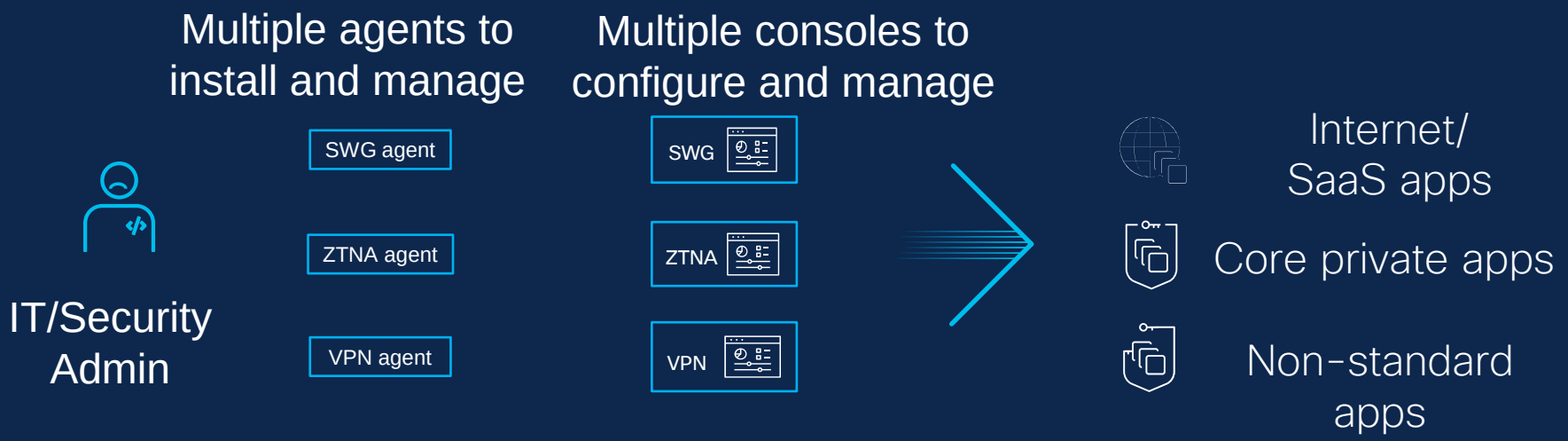
Multi-vendor/tool approach is very common, and can be a challenge to manage



- Licenses/hardware
- Cumbersome deployments
- Increased attack surface

Operational and Security Challenges Remain for IT

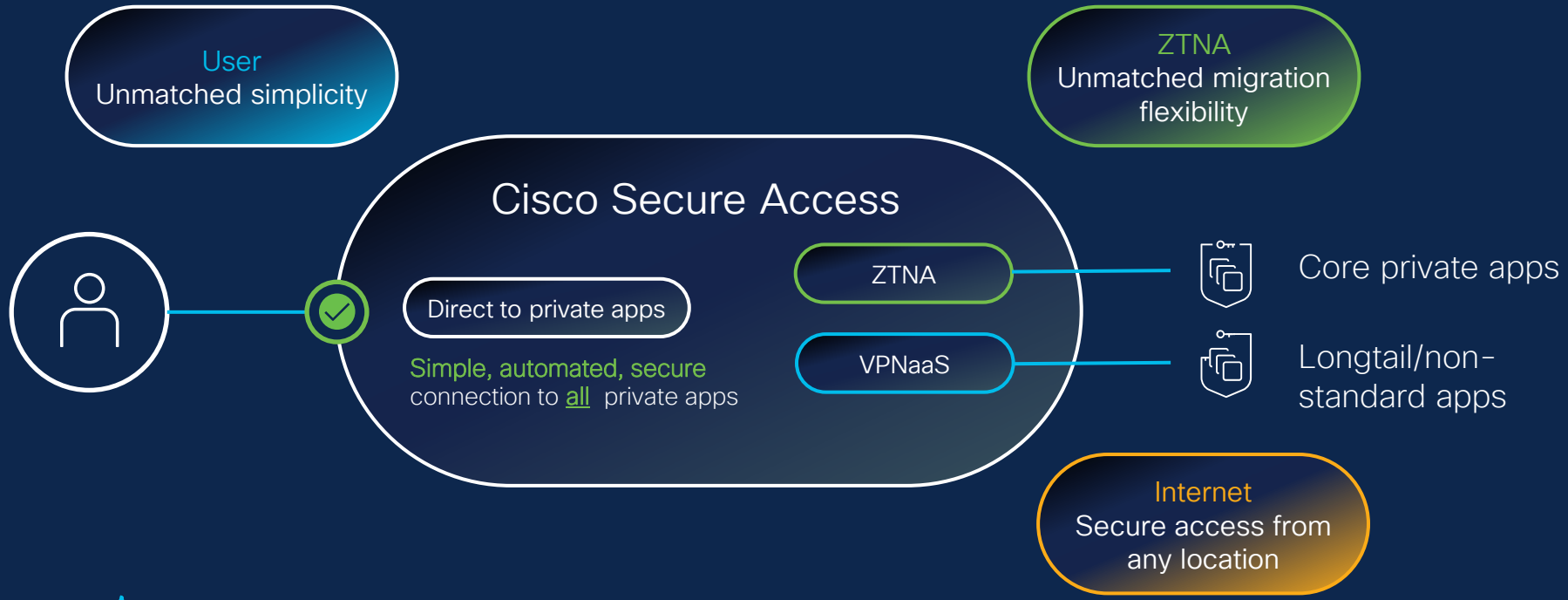
Multi-vendor/tool approach is very common, and can be a challenge to manage



- Licenses/hardware
- Cumbersome deployments
- Increased attack surface

- App support limitations
- Suboptimal performance
- Additional user training and support

Modernize remote access to all private apps, and the Internet. In one unified solution



What are the primary Use Cases for CSA

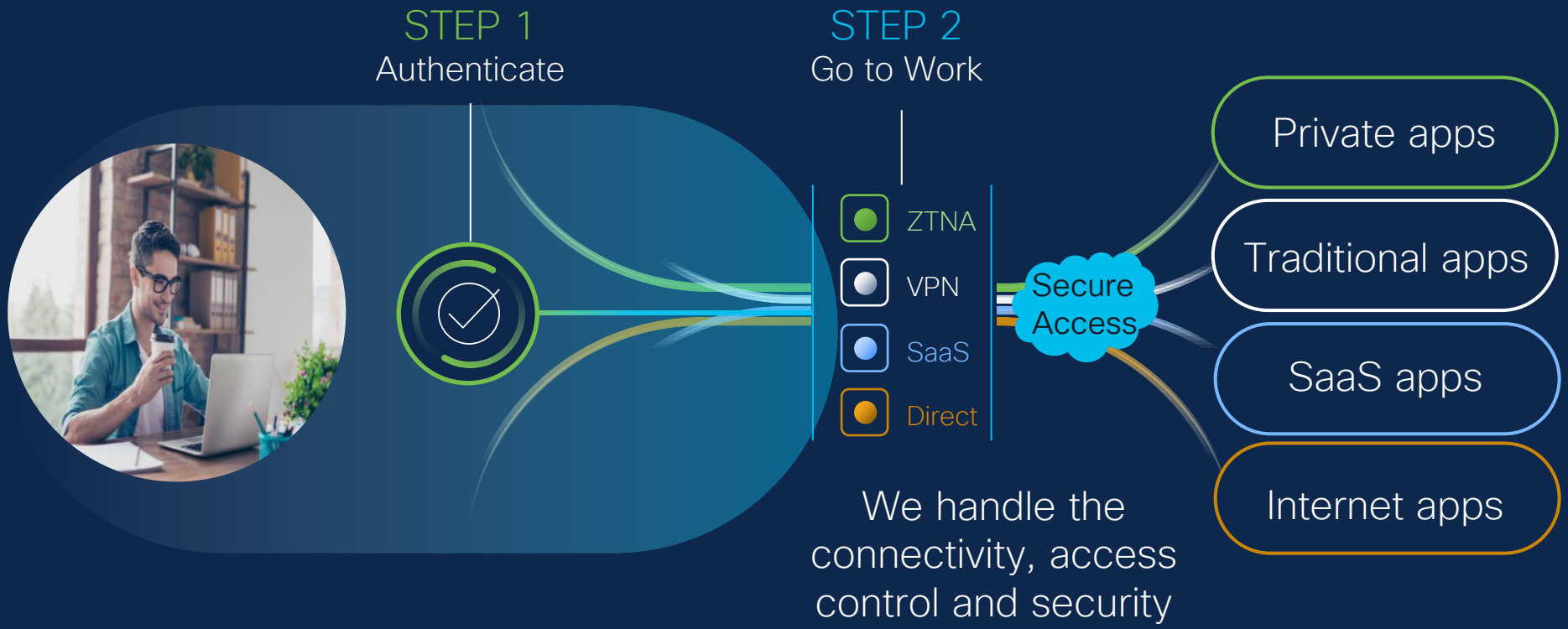
- VPNaaS (typically for legacy applications)
- Private Application Access (cloud/private cloud, on-prem)
- Secure Internet Access

Legacy access
Unmatched simplicity

ZTNA
Unmatched migration flexibility

Internet
Secure access from any location

Cisco Secure Access – User Anywhere



It just works. No drama, no fuss. Just pure convenience.

Benefits

Faster time to productivity for users

Easy, frictionless user experience

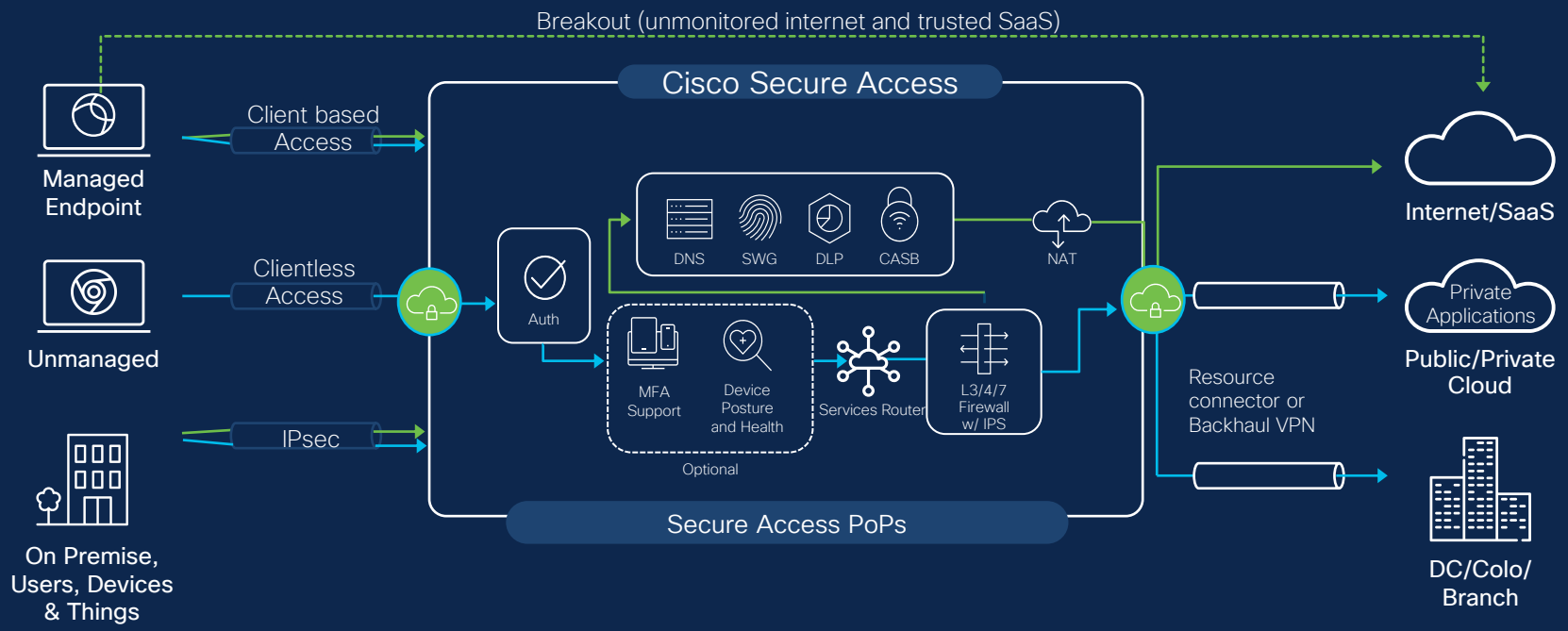
All in one solution

The Architecture of CSA

Architecture Overview

Reference Diagram

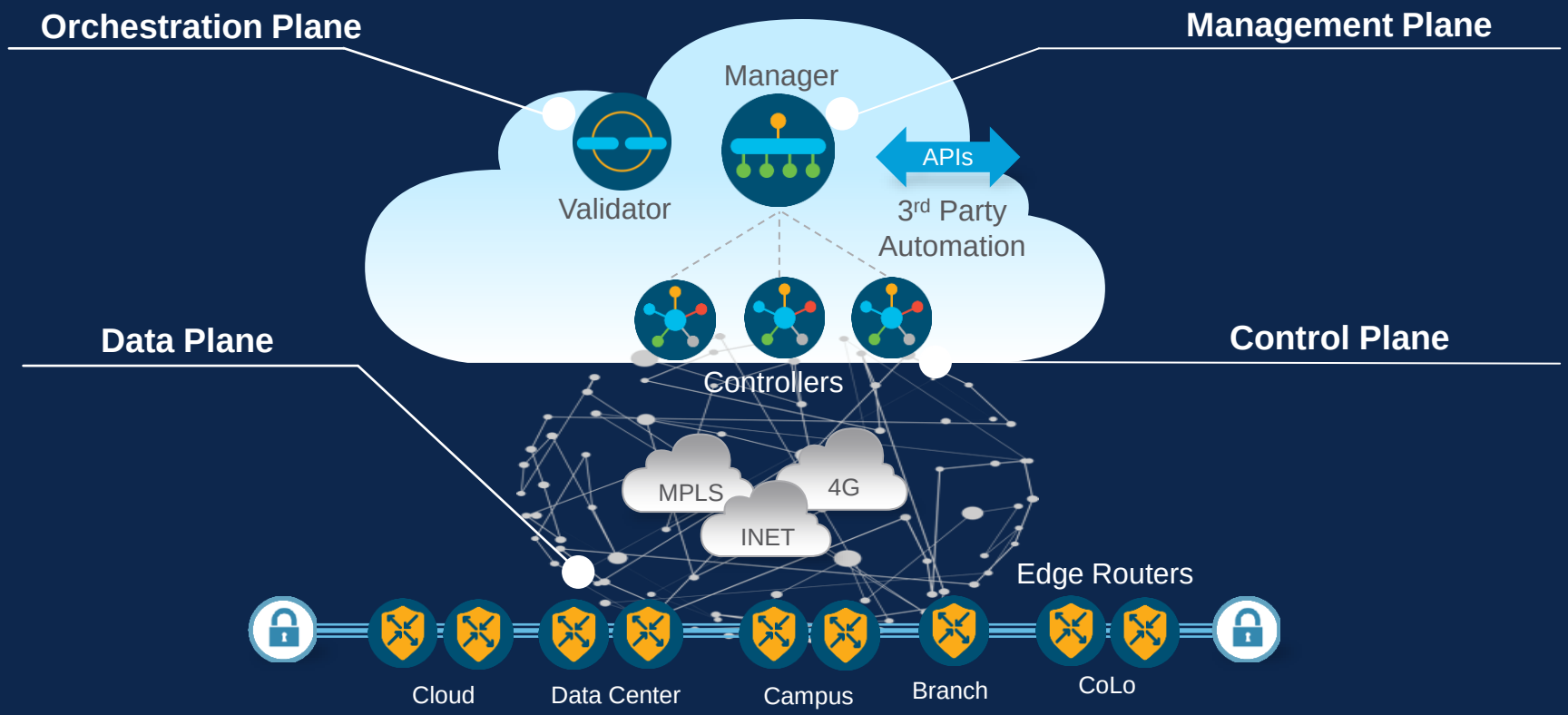
Internet Traffic
Private Traffic
Secure Tunnel



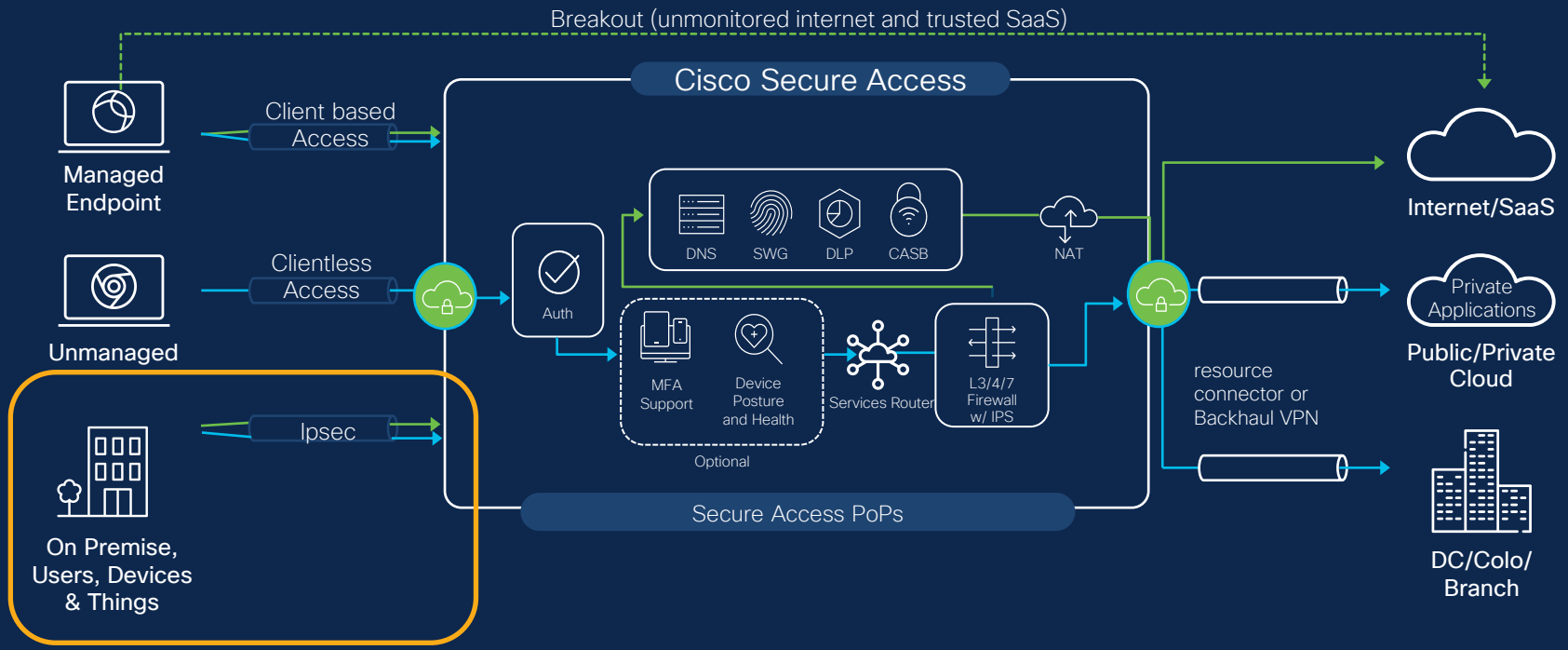
Users — **How** — **Apps**

SD-WAN Integration

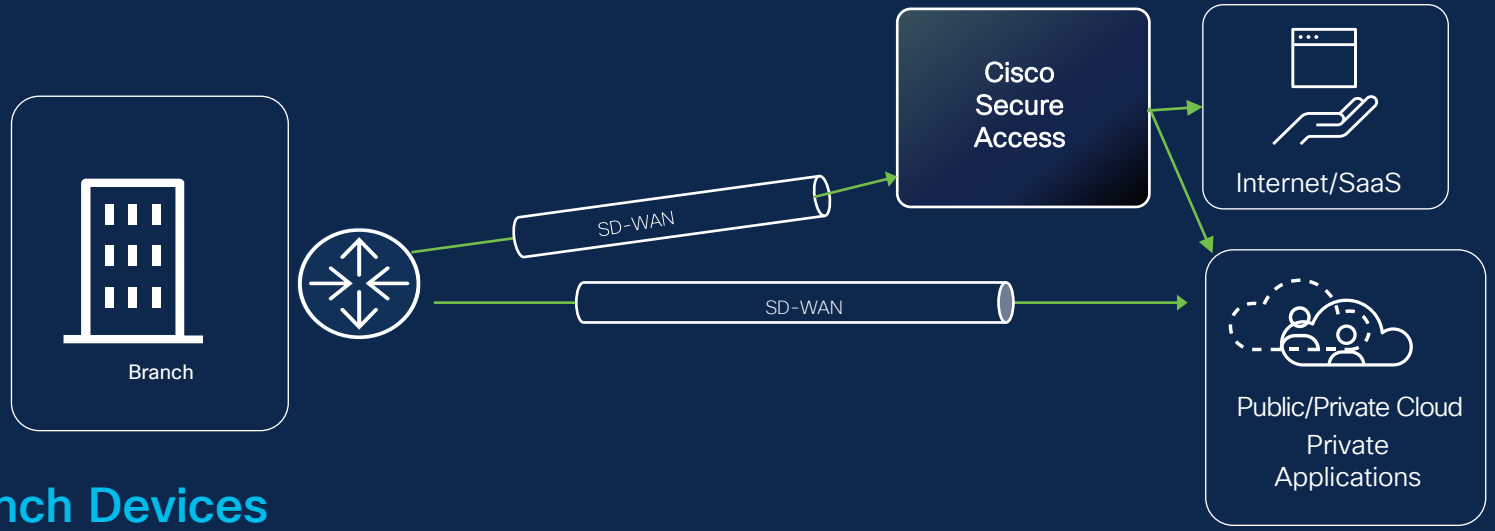
What is Software Defined WAN (SDWAN)?



Architecture Overview



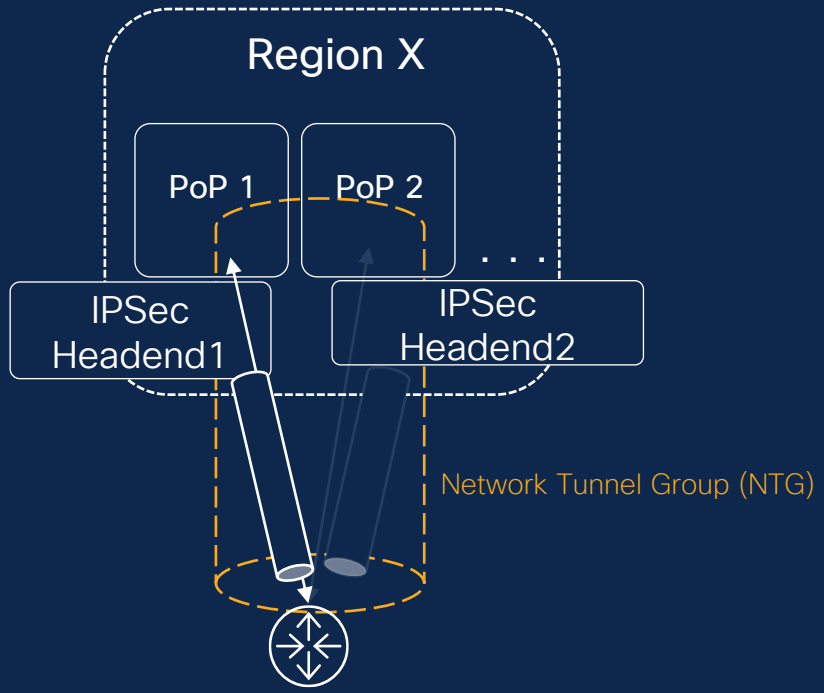
SDWAN Integration



Branch Devices

→ Edge Device Tunnel to Secure Access
→ All internet traffic is routed to Secure Access
→ **Auto Tunnels with Catalyst SD-WAN for Secure Internet Access**

High Availability (SDWAN)



Customer on-prem equipment

When do we switch from Primary to Secondary?

- DC out of rotation
- DC outage

How do we switch from Primary to Secondary?

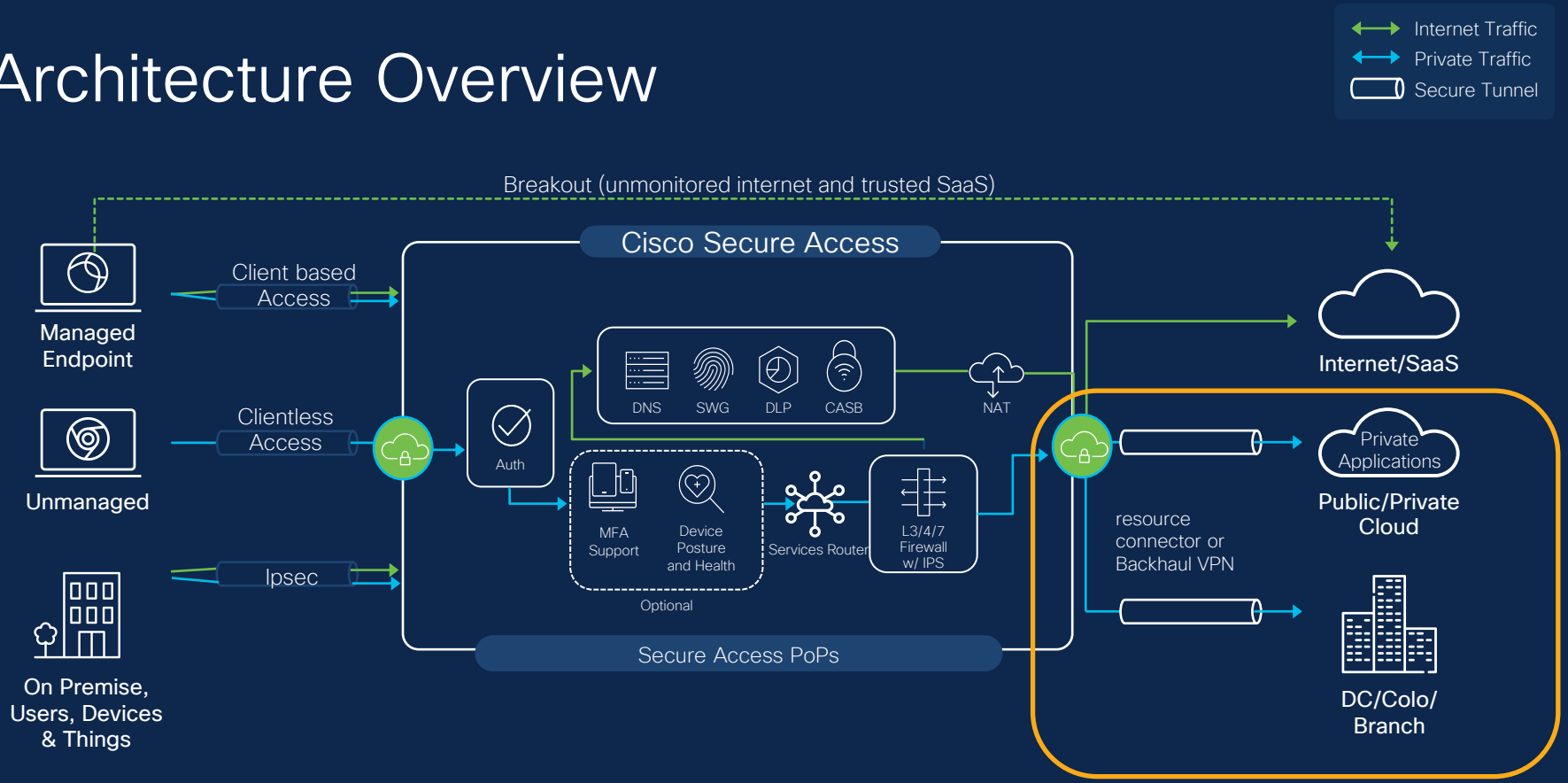
- API endpoint when static routing is enabled
- BGP

Key highlights

- Redundancy is based on BGP or API
- Fully integrated into Catalyst SD-WAN (Auto tunnel config)
- Two types of redundancy:
  - Secure Access side: 1 primary DC and 1 secondary DC.
  - Client side:
    - Active/Active: both devices send traffic to IPSec headend. IPSec headend ECMP on the return path. No flow stickiness
    - Active/Standby: Active device must advertise routes to IPSec headend with higher priority

Resource Connector

Architecture Overview



Differentiate with QUIC and MASQUE

QUIC:

A fast, secure web transport protocol over UDP

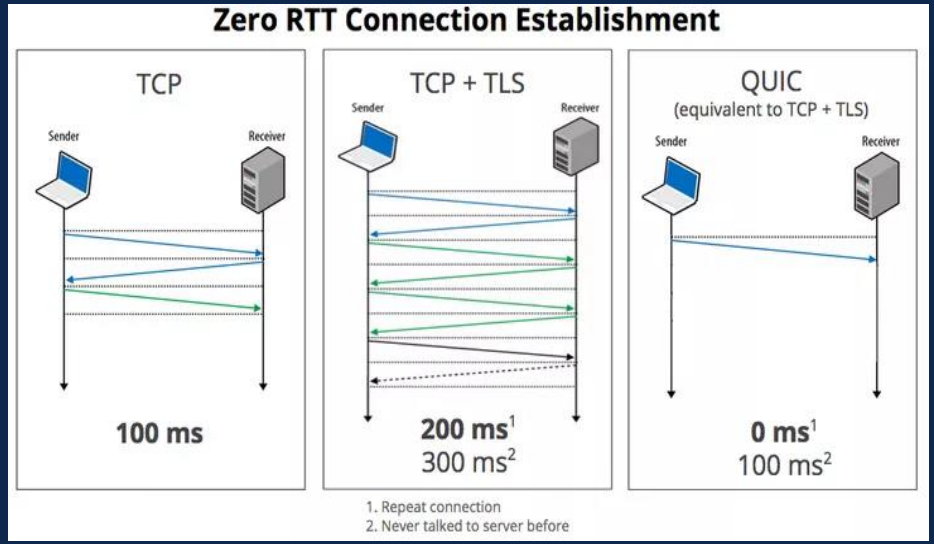
Provides its own layer of security, packet loss detection, data recovery, and congestion control.

HTTP/3 is based on QUIC

MASQUE:

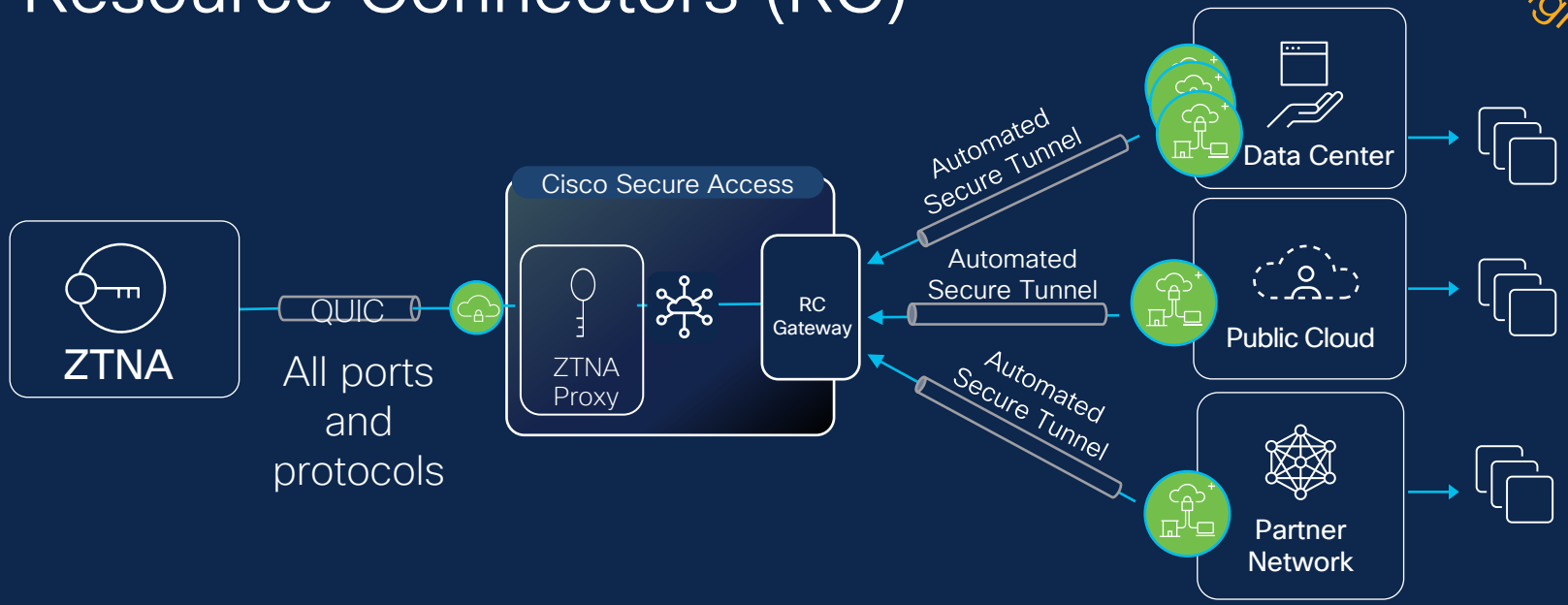
A proxy that routes multiple apps over one QUIC connection.

Efficient without little overhead.



Resource Connectors (RC)

Reference Diagram



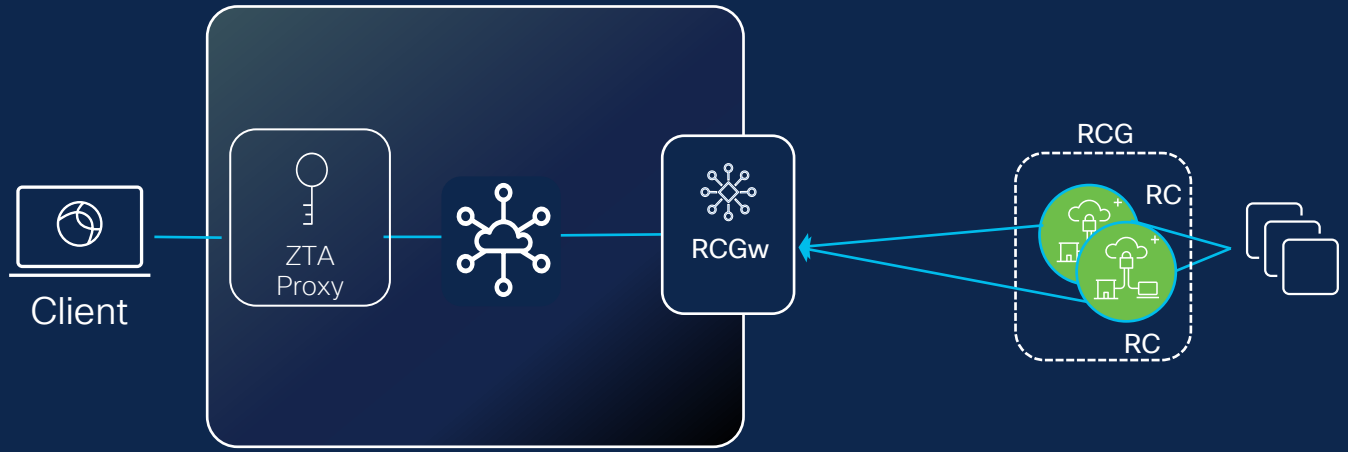
Benefits

- Overlapping IPs support
- Intelligent connectivity
- Latency aware (future)
- Load aware (future)
- On demand authorization
- Cloud managed connectors

Select Cisco Innovations

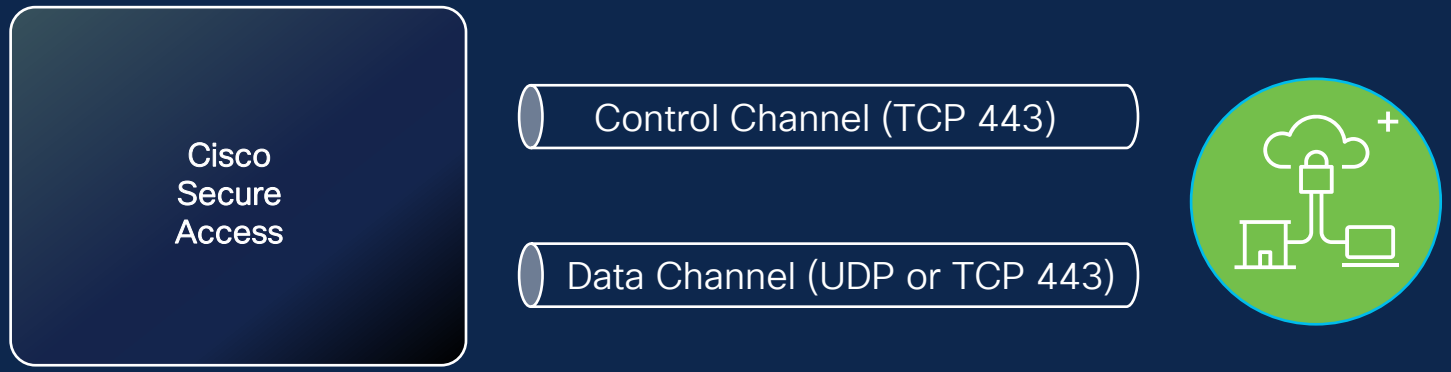
- Network isolation
- Invisible operations- no exposed IP, no over-the-internet DNS queries, no breadcrumbs or system leaks
- Standards-based, compatible with forthcoming mobile ZTNA clients

Resource Connector Components



- Resource connector Gateway (RCGw) – Secure Access Edge for private app connectivity
- Resource connectors (RC) – Hosted on customer's Premises (On-Prem/Cloud)
- Resource connector Group (RCG) – Logical grouping of resource connectors for Scaling and Redundancy, All resource connectors within a group will connect to the same RCGw

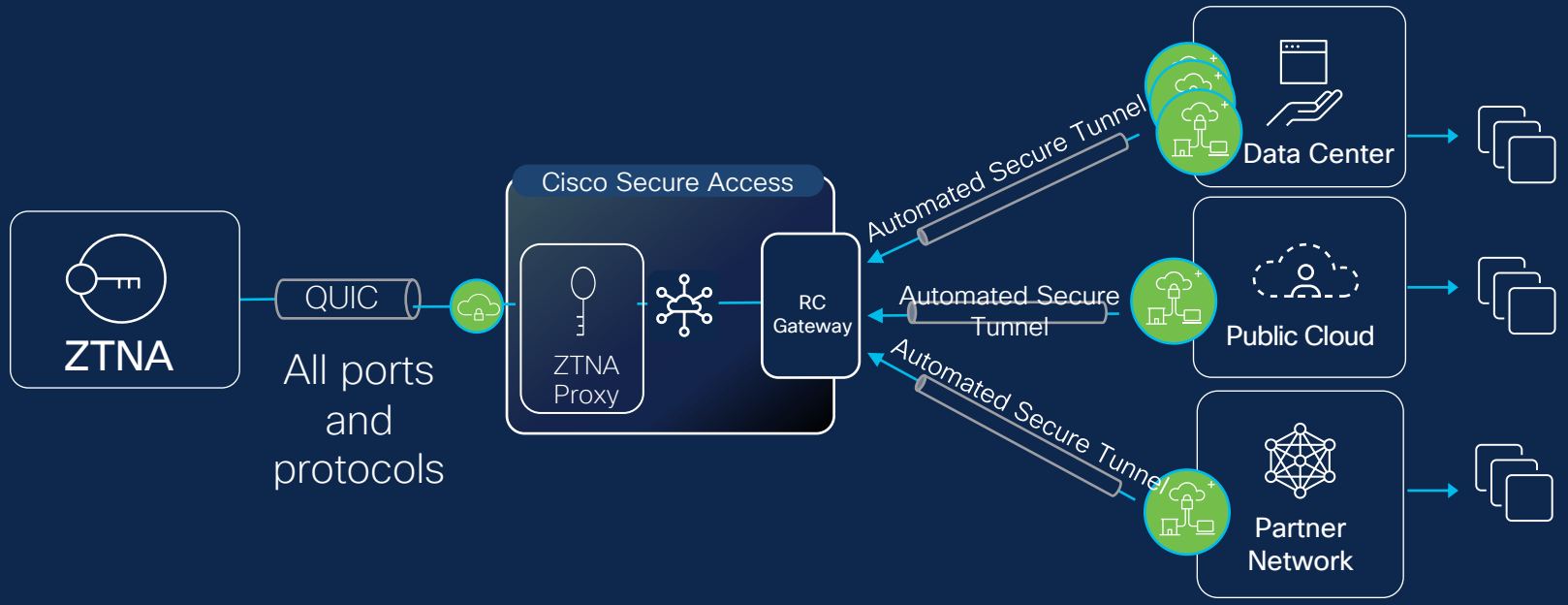
Resource Connector Communication Channels



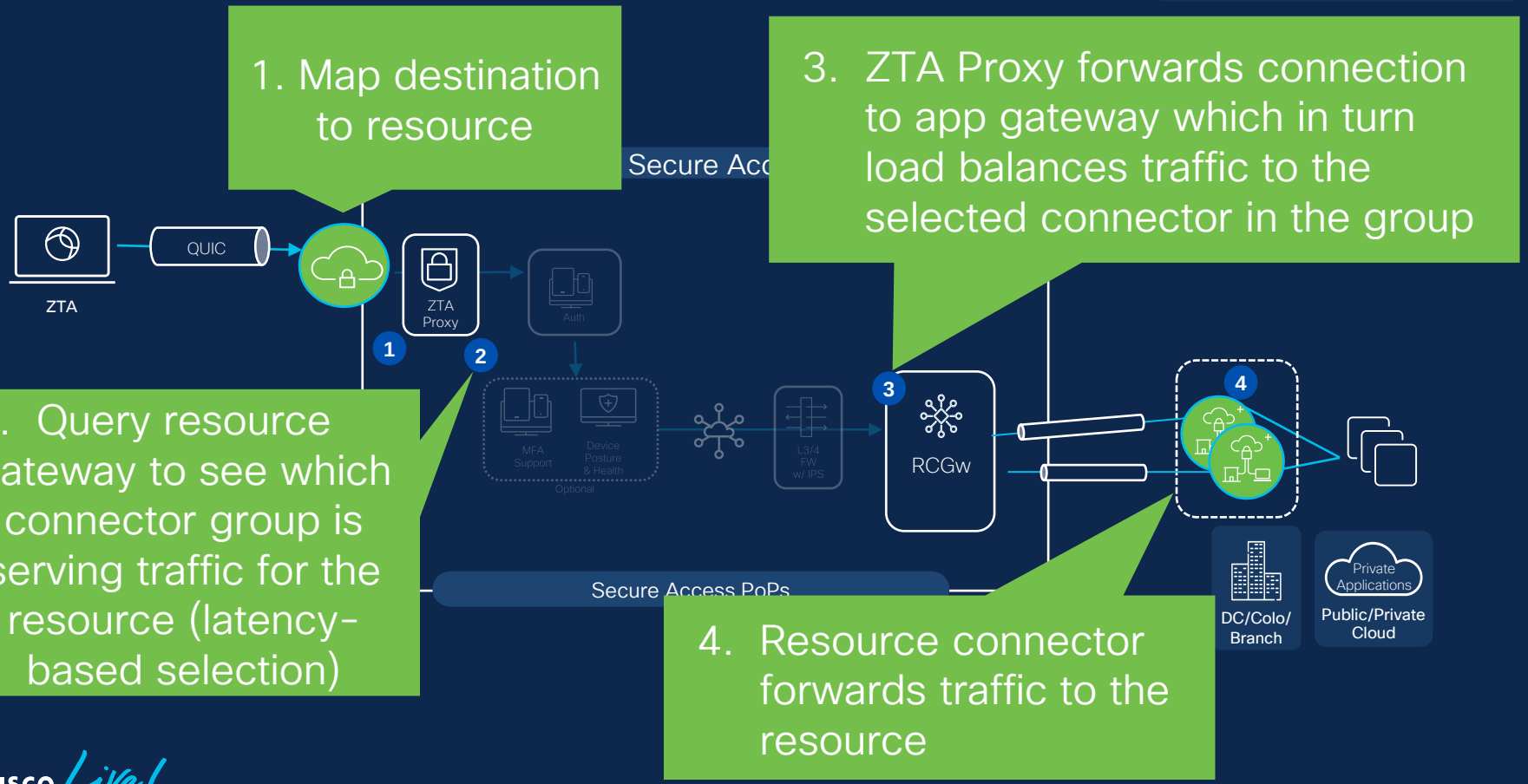
Inside-out, Always On

- Data: D(TLS) tunnels for application traffic
- Control: MQTT over TLS
  - on-demand messages from controller to agent: upgrade, revoke, troubleshooting
  - Metrics: basic system and networks statistics, monitor status

Resource Connectors (RC)



End to End Workflow

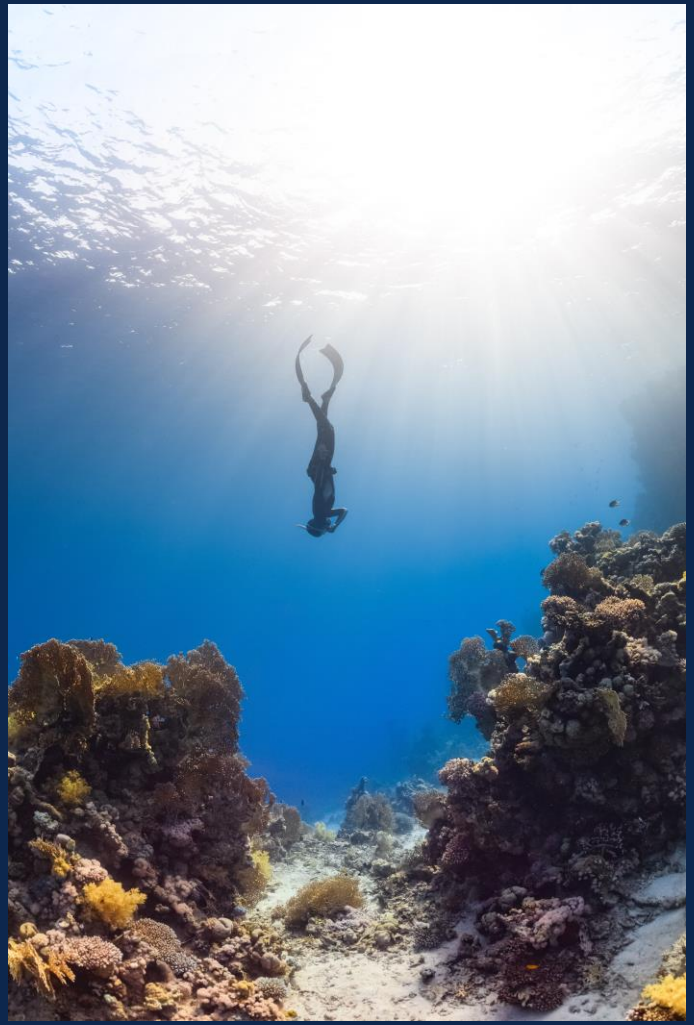


Benefits

- Virtual appliance connector, deployed in front of private applications
- Simplified deployment vs IPSEC VPN
- All ports and protocols supported
- Automatic tunnel establishment using OUTBOUND connections only
- Minimize routing complexities
  - No setting up dynamic routing
  - Supports Overlapping subnets
  - Easy to Scale with high availability

Cisco Secure Access gives your users easy and consistent access from anywhere in world.

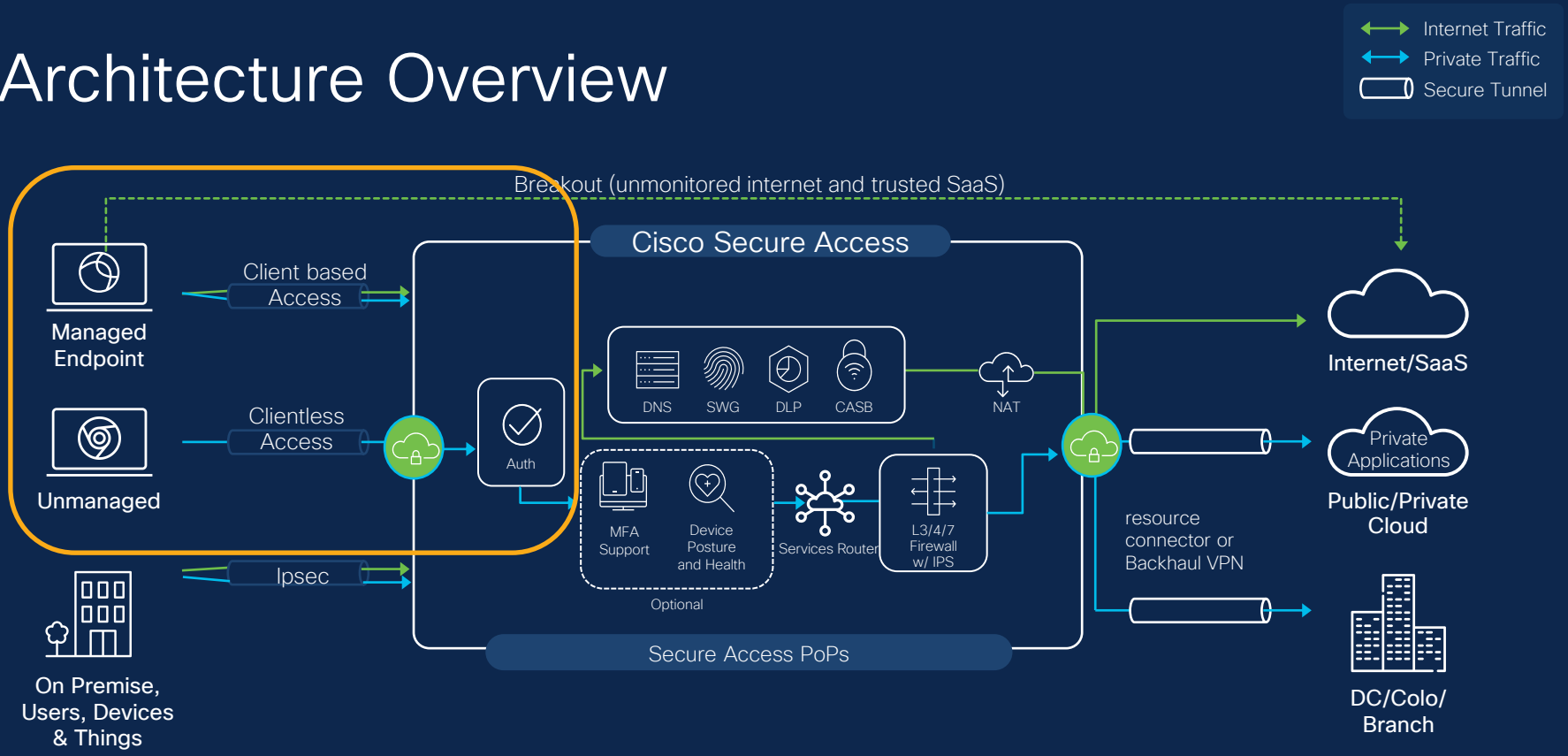
Let’s go a bit deeper….



Private Application Access (ZTNA)

And Remote VPN

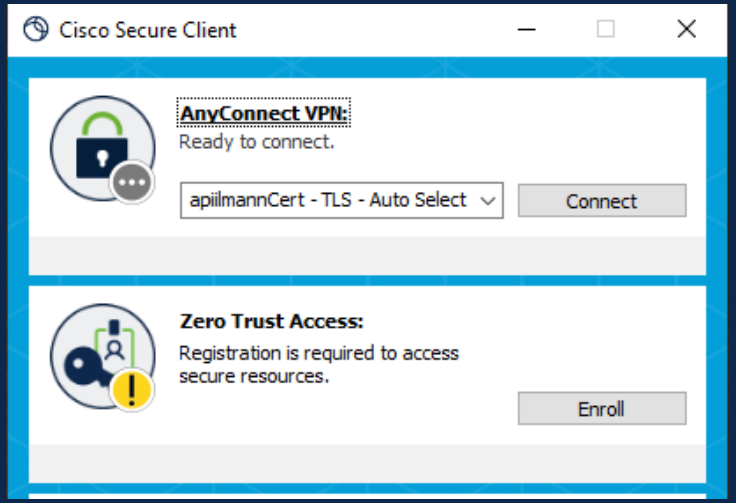
Architecture Overview



Cisco Secure Access: Simple, frictionless user experience

Note: Supports both client and clientless ZTNA connectivity

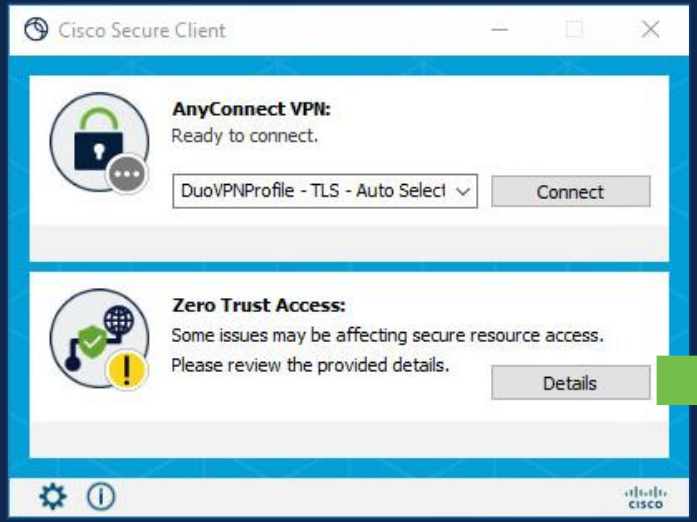
Cisco Secure Client Zero Trust Access Module

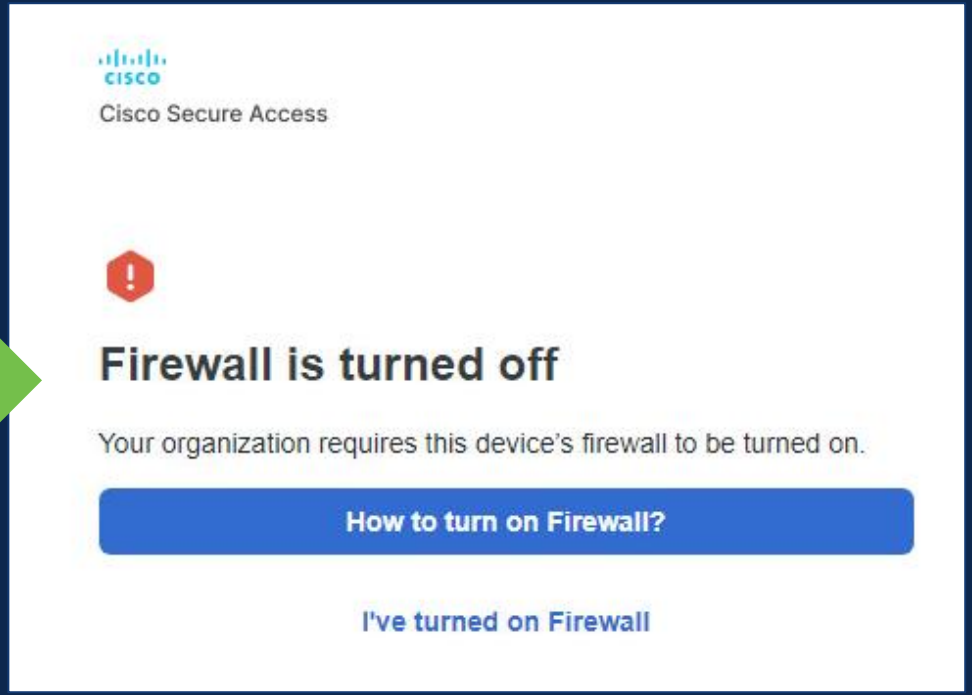


- Transparent user experience (When enrolled)
- Service managed client certificates with TPM/hardware enclave key storage

- Support for both TCP and UDP applications
- Cisco and third-party VPN client interop
- Next-generation protocol (MASQUE + QUIC)

Client based Posture





Posture

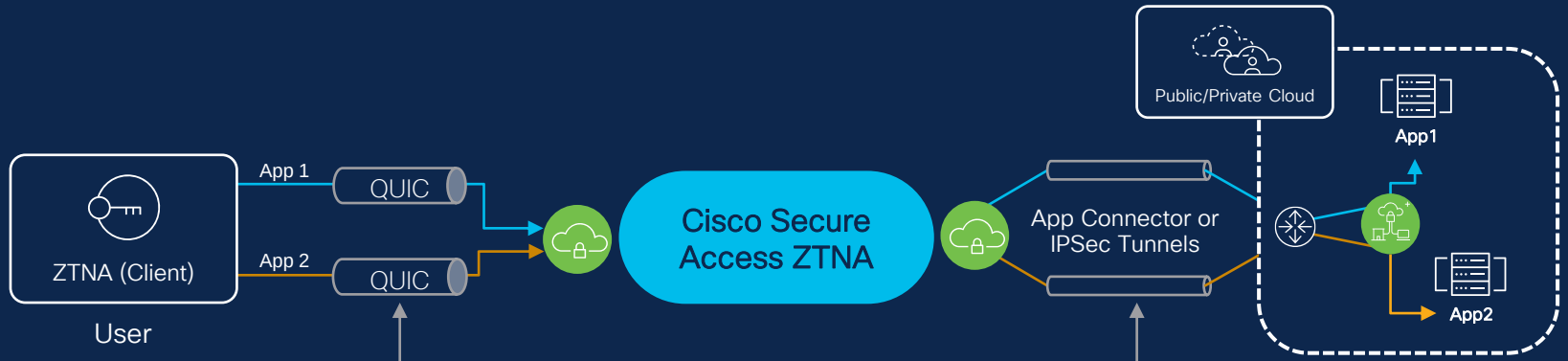
Authorization check prior to application access

Authorization and access check per session

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

Secure Private Access with Cisco

Industry-first HTTP3-based proxy for secure, segmented zero trust access control



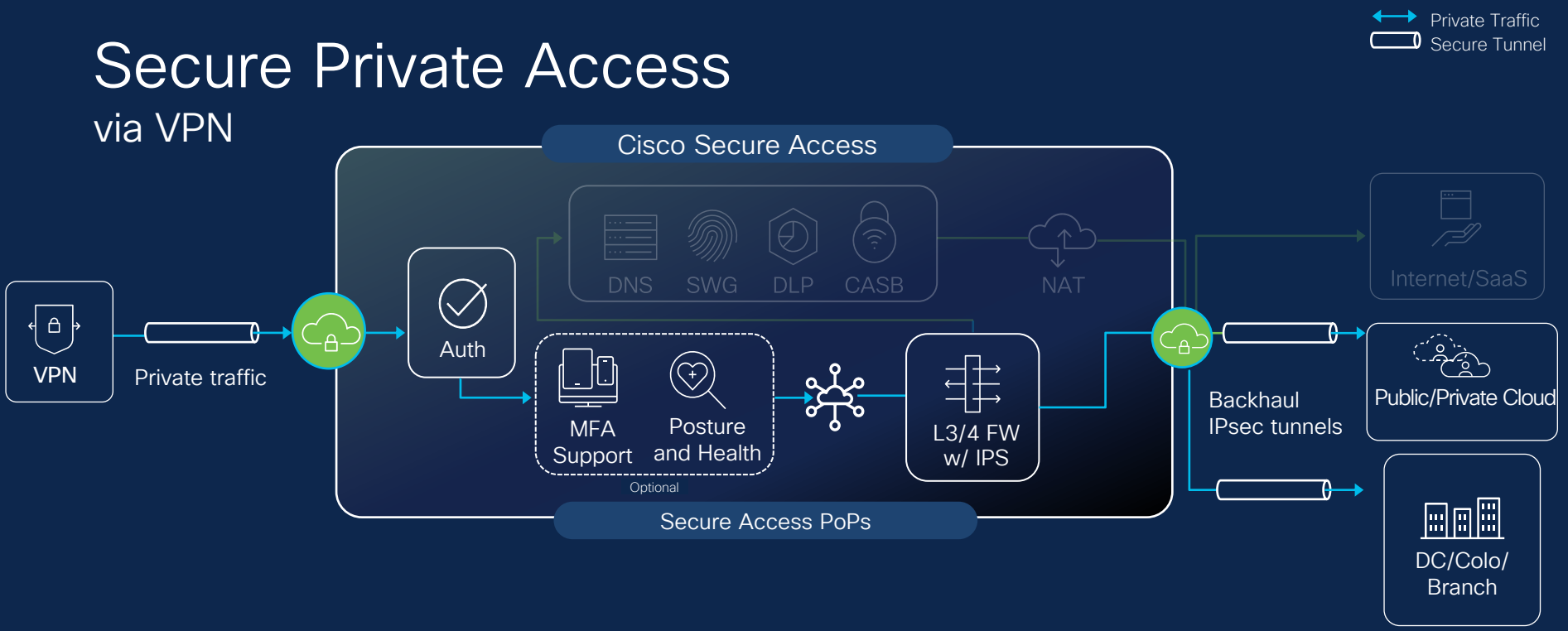
- Dedicated user to app micro-tunnels
- ‘One click’ seamless access
- Advanced protocols speed content delivery

- Optimized L4-7 user to app connectivity
- Fully isolated network-resources are hidden
- Fast deployment with no firewall setting changes

Use Cases

Secure Private Access

via VPN

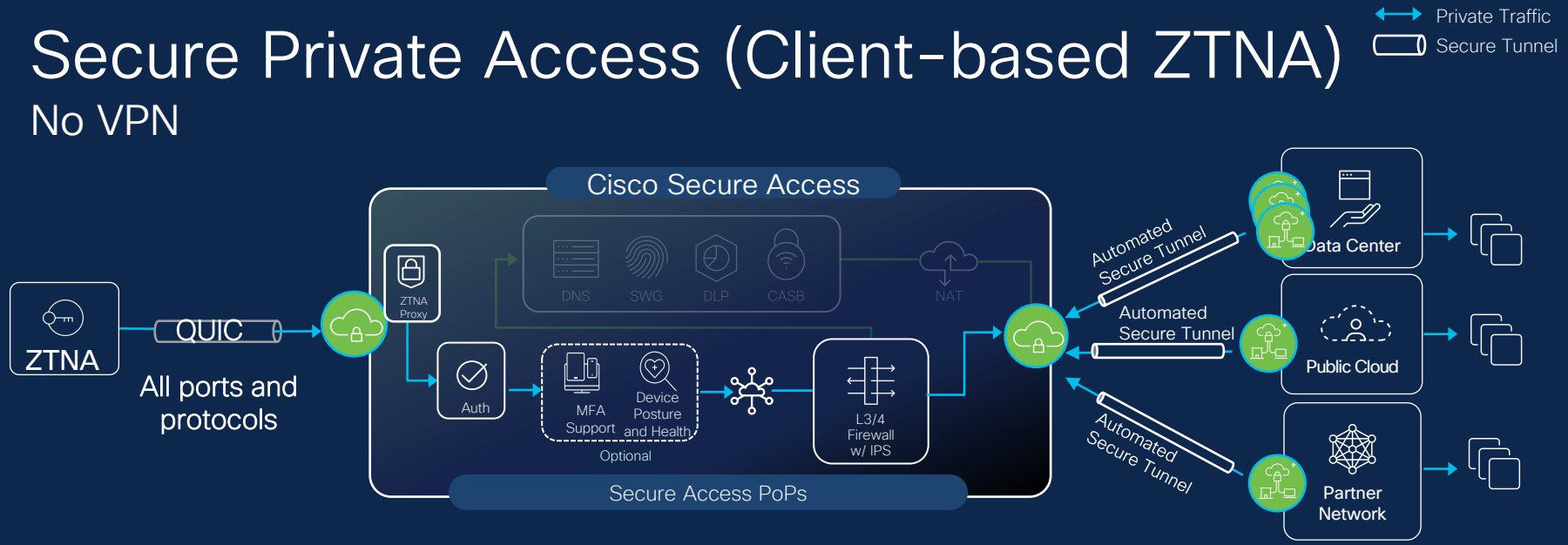


Benefits

- SAML 2.0 + cert-based authentication
- Posture verification (optional)
- Trusted Network Detection
- Start before logon
- IPS
- Granular context-based control

Secure Private Access (Client-based ZTNA)

No VPN

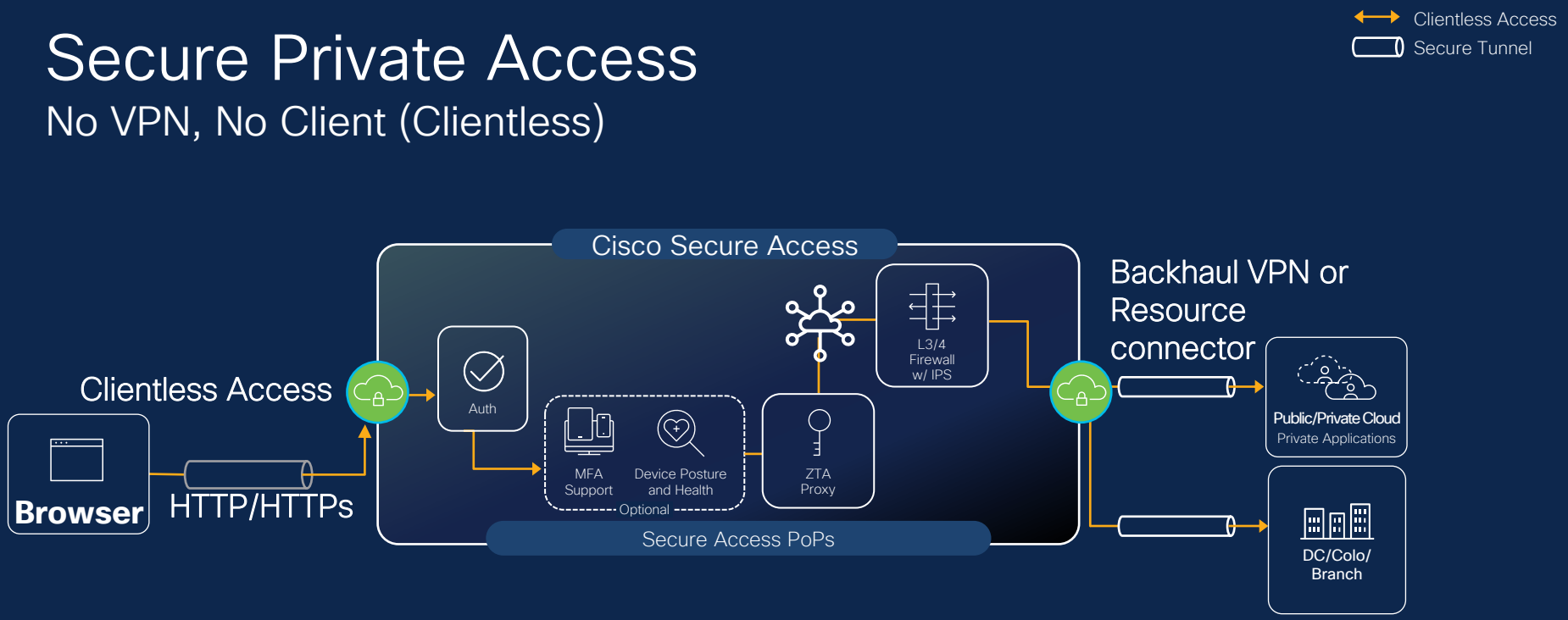


Benefits

- Inline security capabilities
- «Just works» user experience
- Performance benefits QUIC & MASQUE
- Per App tunnel
- App is behind proxy, not visible to client
- No routing/IP/network connectivity
- Zero trust per application policy

Secure Private Access

No VPN, No Client (Clientless)

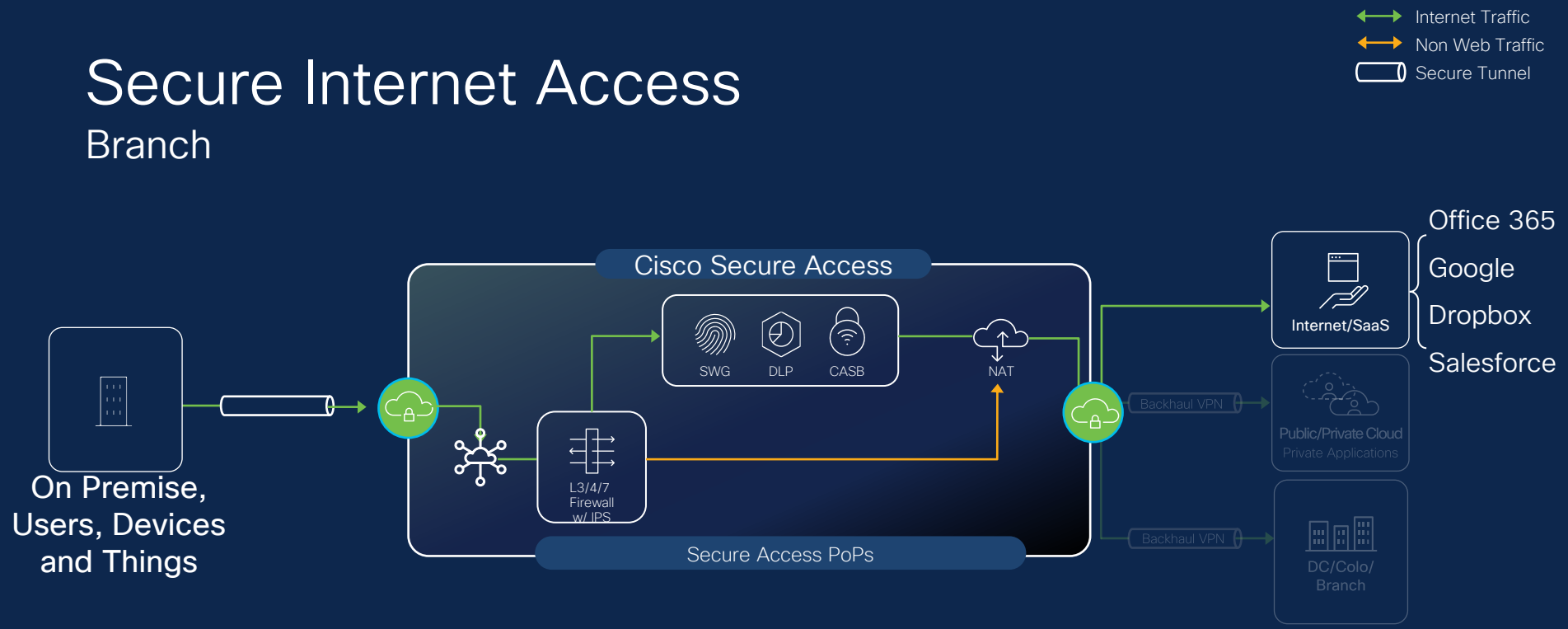


Capabilities

- Clientless
- App-specific access
- Undiscoverable IP address
- Least privileged user access
- Reduced threat surface

Secure Internet Access

Branch



Capabilities

- Auto tunnels with Catalyst SD-WAN
- 1 GBps per tunnel
- BGP
- ECMP support
- Active/Standby
- Overlapping subnets/Outbound NAT

Benefits

- Same client for VPN and ZTNA (Cisco Secure Client)
- No need for on-prem concentrators
- All configuration done in the same dashboard
- Clientless support
- Built-in posturing
- Transparent for the end users

Cisco Secure Access gives your users easy and consistent access from anywhere in world.

Digital Experience Monitor

Digital Experience Monitoring

Monitor the health and performance of users, applications, and network connectivity.

Optimize user productivity by automatically mining details on the user's end-to-end experience, enabling the IT/security staff to rapidly resolve the issue.

DEM* monitoring examples:

- Endpoint performance – CPU, memory, Wifi
- Network performance –endpoint to Secure Access
- Top 20 SaaS applications performance
- User specific events

*Global general availability coming soon

Experience Insight Overview Page

Secure Access

Help | Alerts | Alexander Business Corp, Inc

- Overview
- Connect
- Resources
- Secure
- Monitor
- Insights
- Admin
- Workflows

Digital Experience Management

By integrating with Thousand Eyes technology, you can have a clear view of how well your users, applications, and networks are performing.
Want to know more? Launch ThousandEyes to access detailed information, including a look back at historical data for various time periods. Help.

Refreshed 1 minute ago

Endpoint Performance Overview

Healthy status indicates both latency under 40 ms and loss at 1% or lower, ensuring optimal performance. At Risk status warns of either latency exceeding 40 ms or loss above 1%, while Unhealthy status signals that both metrics are outside the acceptable range, requiring immediate attention.

Performance Health Summary 96 total

Unhealthy	At risk	Healthy
3	4	89

Endpoints 120 total

96 Connected to the Cisco Secure Access cloud

Performance Health Events

	Unhealthy	At risk	Healthy	
London 8 total	2	2	4	5 min ago
New York 50 total	1	0	50	5 min ago
Bucharest 6 total	0	2	4	5 min ago

1 2 3

Endpoints

Search | Devices | Primary Location | Filters | 17 devices

User Name	Health Status	Connectivity to Cisco Secure Cloud	Device Name	Latency (ms)	Jitter (ms)	Loss (%)	WiFi (%)	CPU (%)	Memory (%)	Primary Location
Lee	Unhealthy	Disconnected	Android 13.1	3.0	3.0	3.0	23	33	36	London
Anna	Unhealthy	Connected	PC Windows 10.X.X	3.0	3.0	3.0	22	32	35	London
Jiny	Unhealthy	Connected	PC Windows 10.X.X	1.0	1.0	1.0	21	31	34	New York
Adam	At risk	Connected	PC Windows 10.X.X	1.0	1.0	1.0	21	31	34	Bucharest
Ben	At risk	Connected	PC Windows 10.X.X	1.0	1.0	1.0	21	31	34	Bucharest

Digital Experience Monitoring

Performance Insights

MacBook Pro 16" (M1 Pro) | iPhone 12

Device Details		VPN Access	Disconnect VPN	Zero Trust Access	Unenroll device
Device name	Lee's Laptop	Connection status	Connected	Enrollment status	Enrolled
Public IP address	1.156.487.548	Last connected	4.10.0761	Certificate status	Enrolled
Client version	4.10.0761	Last connected	Mar 14 2023 09:14:35	Client module version	5.5.01023
OS Version	macOS Ventura 13.4.1 (c)	Last location	San Jose, CA	Last connected	Mar 14 2023 09:14:35

Wifi Signal Quality
70dBm ↘ 20% mean
Wireless – Signal Quality

Memory Usage
56% ↘ 1% mean
System – Memory

CPU Usage
43% ↘ 1% mean
System – CPU Load

Endpoint Agent to Cisco Secure Access Cloud

Device (LEE-M-WJ12) — Poor — Local Network (WiFi Blizzard) — Good — Destination (Secure Access Cloud)

IP Address	Avg Latency (ms)	Maximum Latency (ms)	Minimum Latency (ms)	Jitter (ms)	Loss (%)
192.168.1.1	10.0	13.0	7.0	1.0	0.0

Recent Incident Log

Showing recent activity including recorded event, the Secure Access Self Remediation service actions, the action the user took and any resulting performance change.

Date and Time	Event	Suggested Remediation	Reading
Jul, 24, 2023 10:09 AM PST	Poor WiFi Signal Quality	• **Move closer to your router:** Or switch to another Wifi with a stronger signal to improve your network and application experience. • **Reboot the PC; Reboot your router**: Allows different system components to be flushed and for the clearing up of temporary files and processes. • **Close background applications**: Even if you are not using them, applications on your device are using precious resources. Before your meeting, close any applications and browser sessions that you are not using for a better experience.	70dBm - 80dBM

Dashboard visual is for illustrative purposes only

End User Monitoring and Troubleshooting

Secure Access

Help | Alerts | Alexander Business Corp, Inc

- Overview
- Connect
- Resources
- Secure
- Monitor
- Insights
- Admin
- Workflows

← Digital Experience Management

Lee | Contractors | Eng & DevEng & Dev | QA Group 1 | Last hour

Refreshed 1 minute ago

Wifi signal quality is low and is affecting their network and application experience.
Recommend they move closer to their router or switch to another Wifi with a stronger signal to improve their network and application experience.

Name	Lee
Email	Lee@corp.com
Primary location	New York
Internal IP address	1.156.487.548

Connection	ZTNA
IP address	1.156.487.548
OS Version	Windows 11 22H2 (10.0.19044)
Hostname	hostname.eng.sun.com

Endpoint Performance

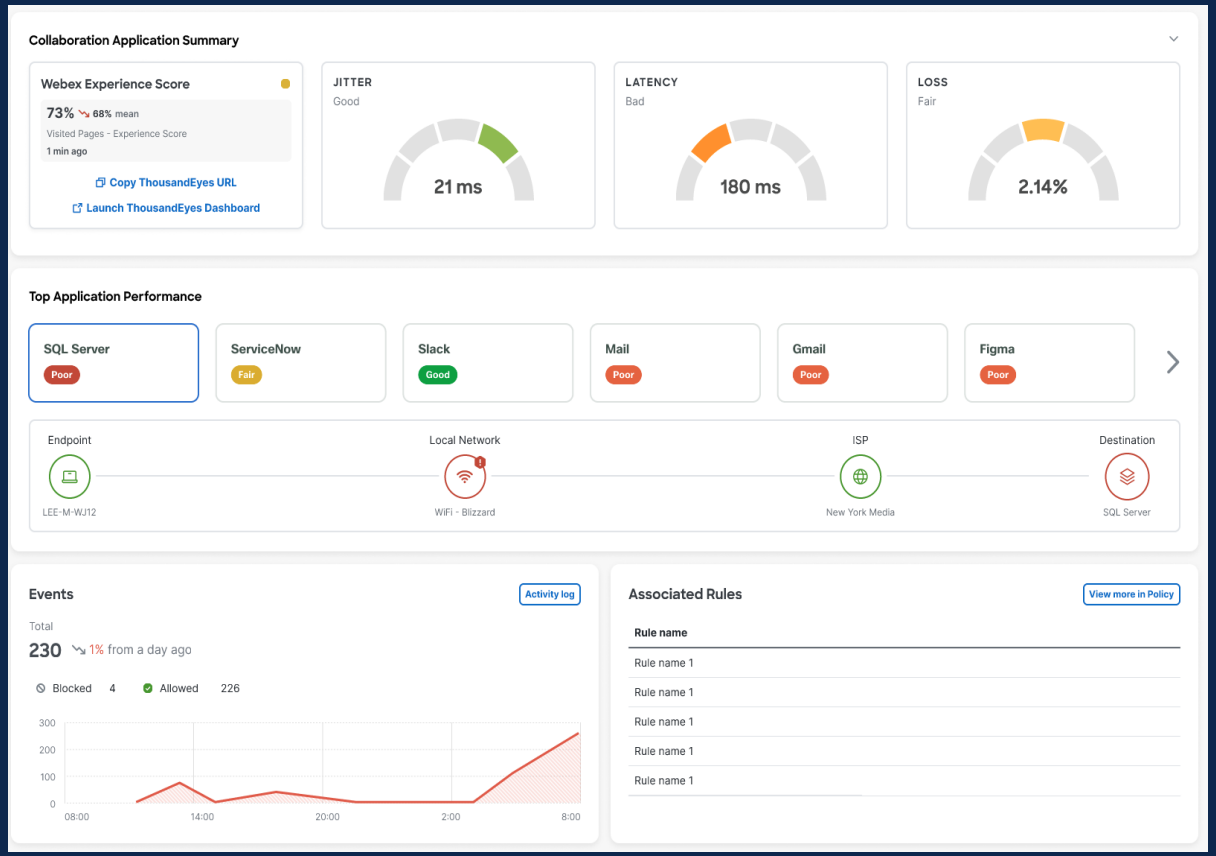
Launch ThousandEyes | Copy ThousandEyes URL

CPU Usage	Memory Usage	Wifi Signal Quality
43% ↘ 1% mean	56% ↘ 1% mean	13% ↘ 77% mean
System – CPU Load	System – Memory	Wireless – Signal Quality
5 minutes	5 minutes	5 minutes

Endpoint	Local Network	ISP	Destination
LEE-M-WJ12	WiFi - Blizzard	New York Media	Secure Access

IP Address	Avg Latency (ms)	Maximum Latency (ms)	Minimum Latency (ms)	Jitter (ms)	Loss (%)
192.168.1.1	10.0	13.0	7.0	1.0	0.0

End User Monitoring and Troubleshooting



Top 20 SaaS Applications Health

Top 20 SaaS applications performance

1 London

You can see top 20 SaaS applications performance per region.

Search

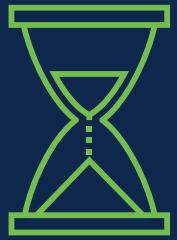
Application	Reachable	URL (Domain)	Loss (%)	Avg Latency (ms)	Jitter (ms)	Type	Region	Time
Mail	✓	mail.ru	0,0	1.0	0.0	ping	London	2023-07-13 12:14:15
Outlook	✓	outlook.com	0.0	1.0	0.0	ping	London	2023-07-13 12:14:15
Miro	✓	miro.com	0.0	1.0	0.0	ping	London	2023-07-13 12:14:15
Slack	✓	slack.com	0.0	1.0	0.0	ping	London	2023-07-13 12:14:15
Gmail	✓	slack.com	0.0	1.0	0.0	ping	London	2023-07-13 12:14:15
Salesforce	✓	salesforce.com	0.0	1.0	0.0	ping	London	2023-07-13 12:14:15
Box	✓	box.com	0.0	1.0	0.0	ping	London	2023-07-13 12:14:15
Figma	✓	figma.com	0.0	1.0	0.0	ping	London	2023-07-13 12:14:15
Notion	✓	notion.com	0.0	1.0	0.0	ping	London	2023-07-13 12:14:15

Rows per page 10 < 1 2 ... 10 >

Benefits

Built-in self remediation for end users

Cut down on time for troubleshooting



Visualize application health, both for SaaS and Private Apps

Fresh out of the oven

Secure Access Regions	
Africa (South Africa)	Europe (Milan)
Asia Pacific (Hong Kong)	Europe (Spain)
Asia Pacific (Jakarta)	Europe (Stockholm)
Asia Pacific (Osaka)	India (South)
Asia Pacific (Seoul)	India (West)
Asia Pacific (Singapore)	Israel (Tel Aviv)
Asia Pacific (Tokyo)	Middle East (Bahrain)
Australia (Melbourne)	Middle East (UAE)
Australia (Sydney)	Switzerland (Zurich)
Brazil	United Kingdom
Canada (Central)	US (Midwest)
Europe (France)	US (Northern California)
Europe (Germany)	US (Pacific Northwest)
Europe (Ireland)	US (Virginia)

- Green are online
- New regions can be stood up in as few as a couple of weeks

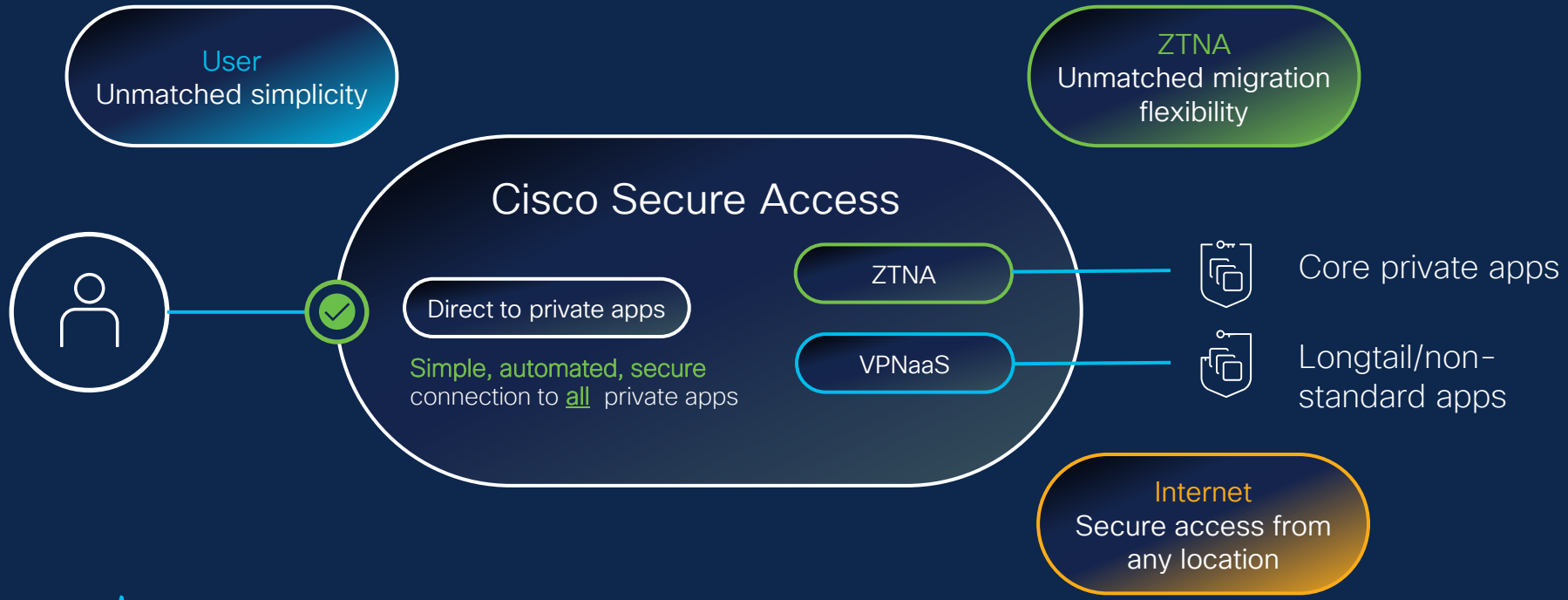
Cisco Secure Access traffic optimization with Apple iCloud Private Relay

Enterprise Relay with Apple iCloud Private Relay On

Single layer of encryption for lightning-fast, secure access

Cisco Secure Access gives your users easy and consistent access from anywhere in world.

Modernize remote access to all private apps, and the Internet. In one unified solution



Thank you for your time. If you would like to know more about CSA

Then this sessions will go into more detail:

- BRKSEC-2438 - Cisco Secure Access: stepping behind the curtain...
  Wednesday, Feb 7, 4:00 PM - 5:00 PM CET
  Hosted by Jonny Noble, Director, Technical Marketing

- BRKSEC-2079 - Zero Trust Network Access (ZTNA) Demystified - What It Is, Why You Need It and the New Cisco Technologies That Make Frictionless Security Possible
  Friday 11 AM – 12:30 PM CET
  Hosted by Steven Chimes, Platform Security Architect

The bridge to possible

Thank you

cisco Live!

cisco Live!

Let's go