Is VPN Really Dead and Replaced by Zero Trust Network Access (ZTNA)?

Gustavo Medina
Security Solutions Engineer
https://www.linkedin.com/in/tavo-medina

Cisco Webex App

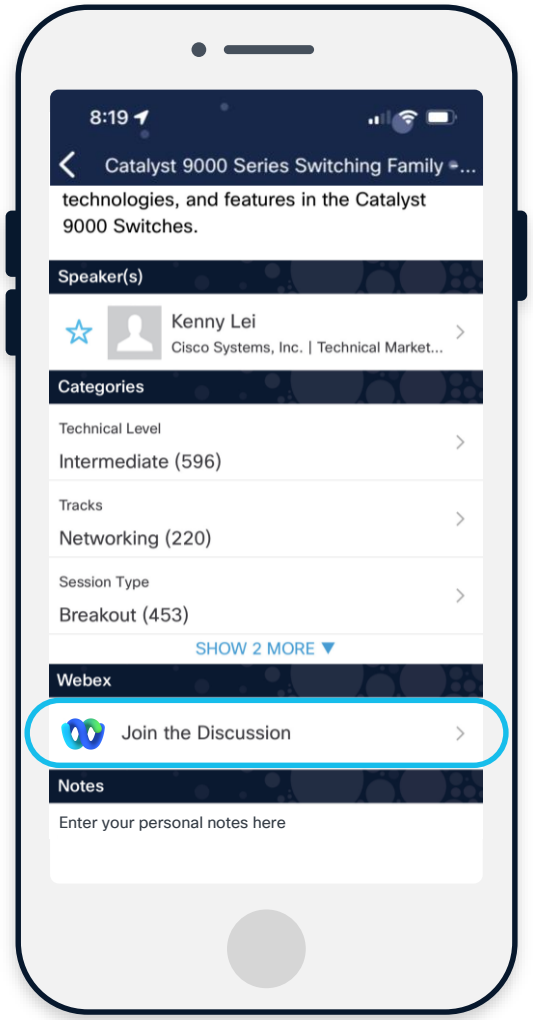
Questions?

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 June 13, 2025.



https://ciscolive.ciscoevents.com/
ciscolivebot/**#BRKSEC-1015**

Agenda

01 Introduction

02 What is ZTNA?

03 VPN vs ZTNA: Key Differences

04 VPN Common Objections

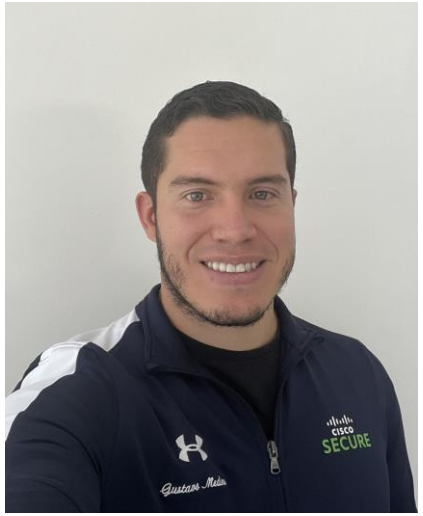
05 Why ZTNA?

06 Universal ZTNA (UZTNA)

07 Cisco Secure Access

08 Flexible Journey to ZTNA

$ whoami



- ~~Gus~~tavo Medina
- Technical Solutions Architect
- Costa Rican CR
  - Currently living in Mexico MX
- Joined Cisco (TAC) in 2009
- CCIE Security #51487
- Football Fan

Introduction

“ZTNA solutions are rapidly replacing remote access VPNs for application access.”

“Organizations identify VPN replacement as their primary motivation for evaluating ZTNA offerings, but find that justification comes from risk reduction, not from any cost savings.”

Gartner Market Guide for Zero Trust Network Access – August 2023

How many Cisco Lives have you attended?

Security

SASE / Security Service Edge (SSE)

Learn how Secure access service edge combines networking and security functions in the cloud to deliver seamless, secure access to applications, anywhere users work. Core functions include software-defined wide area network, secure web gateway, firewall as a service, cloud access security broker, and zero-trust network access.

START

Monday, June 9 | 8:00 a.m.
BRKSEC-1015
Is VPN really dead and replaced by Zero Trust Network Access (ZTNA)?

Monday, June 9 | 11:00 a.m.
IBOSEC-1103
Private Access Showdown: Traditional VPN vs. Zero Trust Access

Monday, June 9 | 11:00 a.m.
BRKSEC-2143
Do You Know Where Your Data Is? A Deep Dive on Cisco Secure Access CASB and DLP and How to Protect Your Locations, Data and Users

Monday, June 9 | 2:30 p.m.
BRKSEC-2285
The Latest in Cisco Secure Access (SSE) Innovation

Tuesday, June 10 | 11:00 a.m.
BRKSEC-2238
Getting SASE with Umbrella and Meraki - Understand best practices for simple and flexible integrations between Meraki and Umbrella

Tuesday, June 10 | 3:00 p.m.
BRKSEC-2882
Zero Trust Access: Enterprise Browsers and Secure Client

Tuesday, June 10 | 4:00 p.m.
BRKSEC-3027
Deep Dive into Cisco's Use of QUIC, MASQUE and OS Native Capabilities to Deliver Frictionless Zero Trust Access

Wednesday, June 11 | 10:30 a.m.
BRKSEC-2170
Evolving Perimeters and Universal(Hybrid) Zero Trust with Cisco Secure Firewall

Wednesday, June 11 | 1:00 p.m.
BRKSEC-2885
How It's Made: Cisco Secure Access

FINISH

Thursday, June 12 | 10:30 a.m.
BRKSEC-2857
Add Visibility to Your S(A)SE with ThousandEyes

What is ZTNA?

Gartner

Internal Workforce Remote Access

Privileged Remote Access

Extended Workforce & BYOD

On-prem Access

VPN vs ZTNA

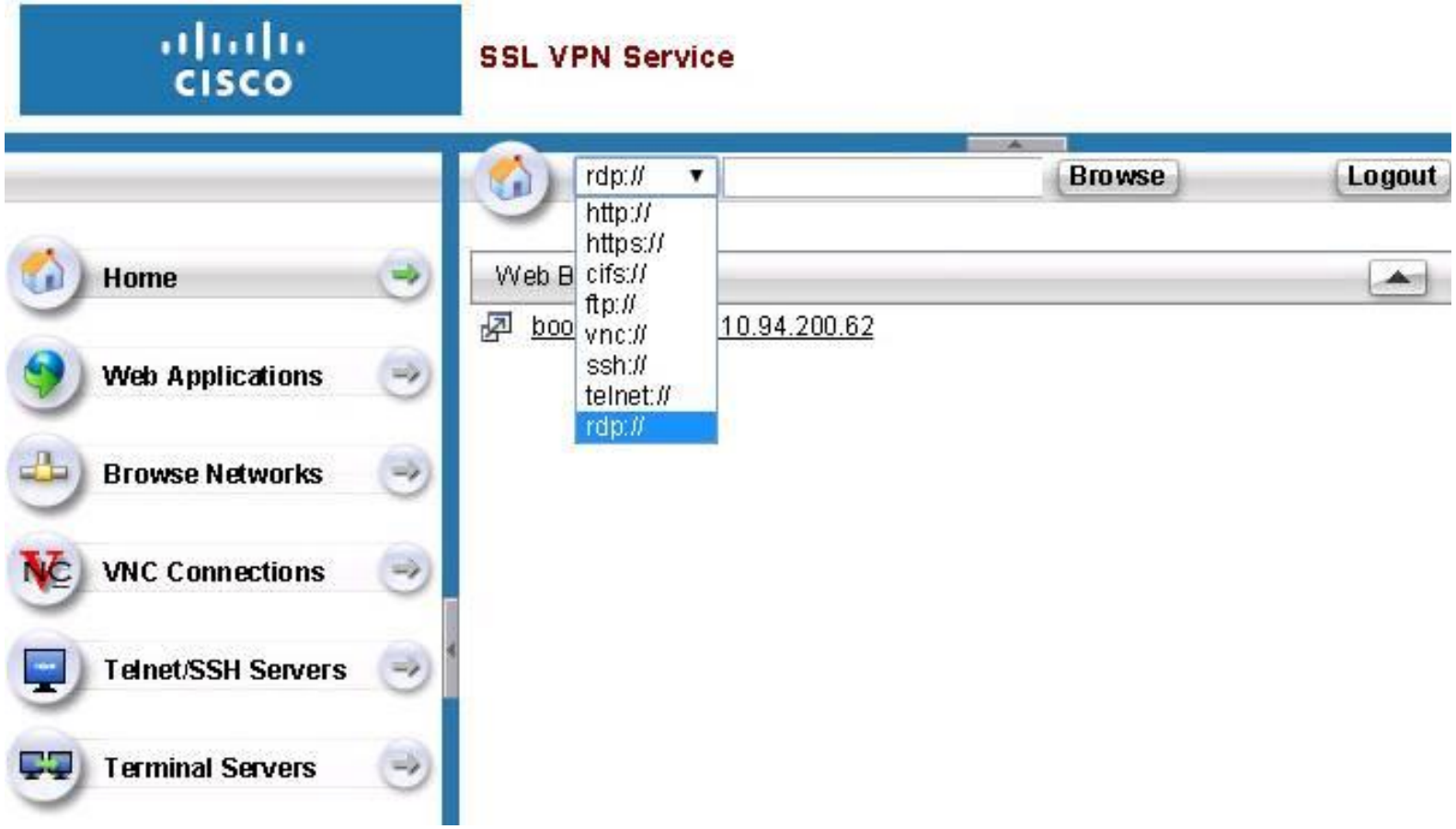
Key Differences

	VPN	ZTNA
User Experience	Requires VPN client software	No client software required *
Access Scope	Access to full network or network segment	Access to specific applications
Posture Checks	Posture assessed once at VPN authentication	Posture assessed at each application access
Connection Architecture	1:1. Client-to-Headend relationship	Client can connect to different headends per application
Trust Model	Implicit	Explicit

We had WebVPN Clientless before ZTNA was even a concept

Supported since ASA 7.1
*Deprecated on 9.17

VPN 3000
Series Concentrator
supported Clientless



VPN Common Objections

- VPNs provide a bad user experience.
- VPN assumes that anyone or anything passing network perimeter controls can be trusted.
- ZTNA (Zero Trust Network Access) takes the opposite approach by not trusting any user or device until proven otherwise.
- ZTNA extends the zero-trust model beyond the network.
- ZTNA reduces the attack surface by hiding applications from the internet

Although traditional VPNs have been a mainstay for decades, ZTNA is the natural evolution of VPN and offers better security, more granular control, and a better user experience in light of the complexity of today's networks, so it can be a smarter choice for securely connecting a remote workforce.

Zero Trust, ZTA, and ZTNA: What's the difference? - CSO
https://www.csoonline.com/article/570475/zero-trust-zta-and-ztna-what-s-the-difference.html

Cisco Secure Client VPN Demo (Formerly AnyConnect)


Cisco AnyConnect Secure Mobility Client
Edit
Sat 3 Jun 23:44
Macintosh HD

VPN Objections

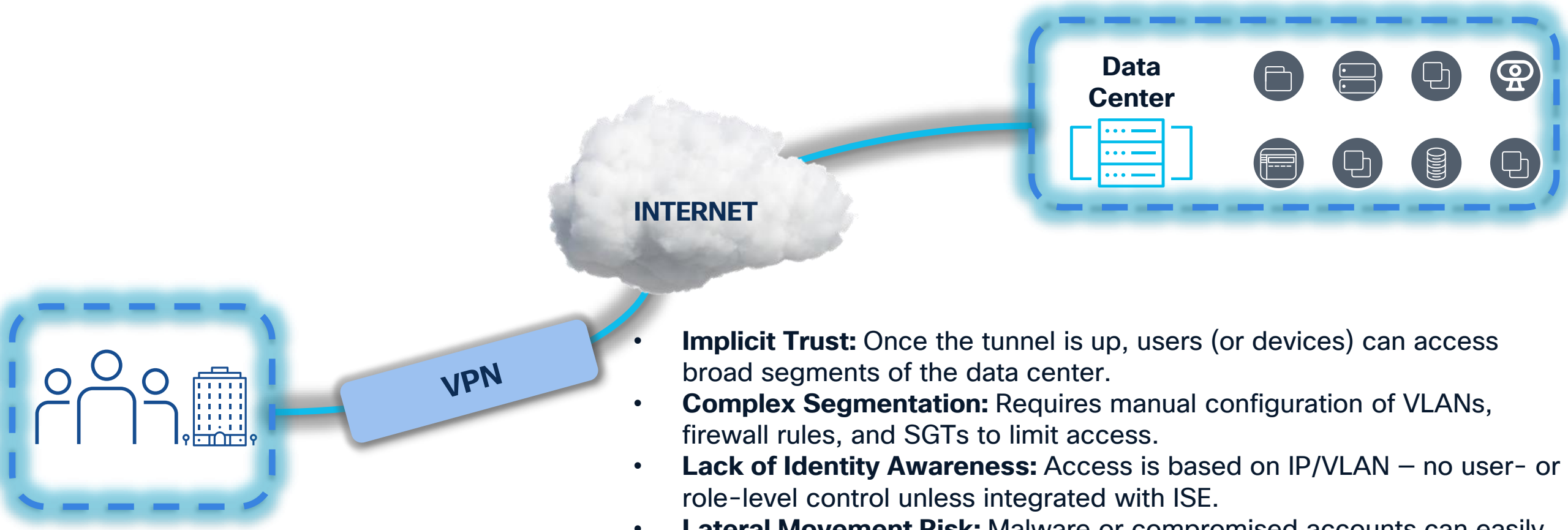
- VPNs provide a bad user experience.
- VPN assumes that anyone or anything passing network perimeter controls can be trusted.
- ZTNA (Zero Trust Network Access) takes the opposite approach by not trusting any user or device until proven otherwise.
- ZTNA extends the zero-trust model beyond the network.
- ZTNA reduces the attack surface by hiding applications from the internet

VPN Objections

- VPNs provide a bad user experience.
- VPN assumes that anyone or anything passing n[illegible]ork perimeter controls can be trusted.
- ZTNA (Zero Trust Network A[illegible]e approach by not trusting any user or device until pro[illegible]
- ZTNA extends the zero-[illegible]del beyond the network.
- ZTNA reduces the attack surface by hiding applications from the internet

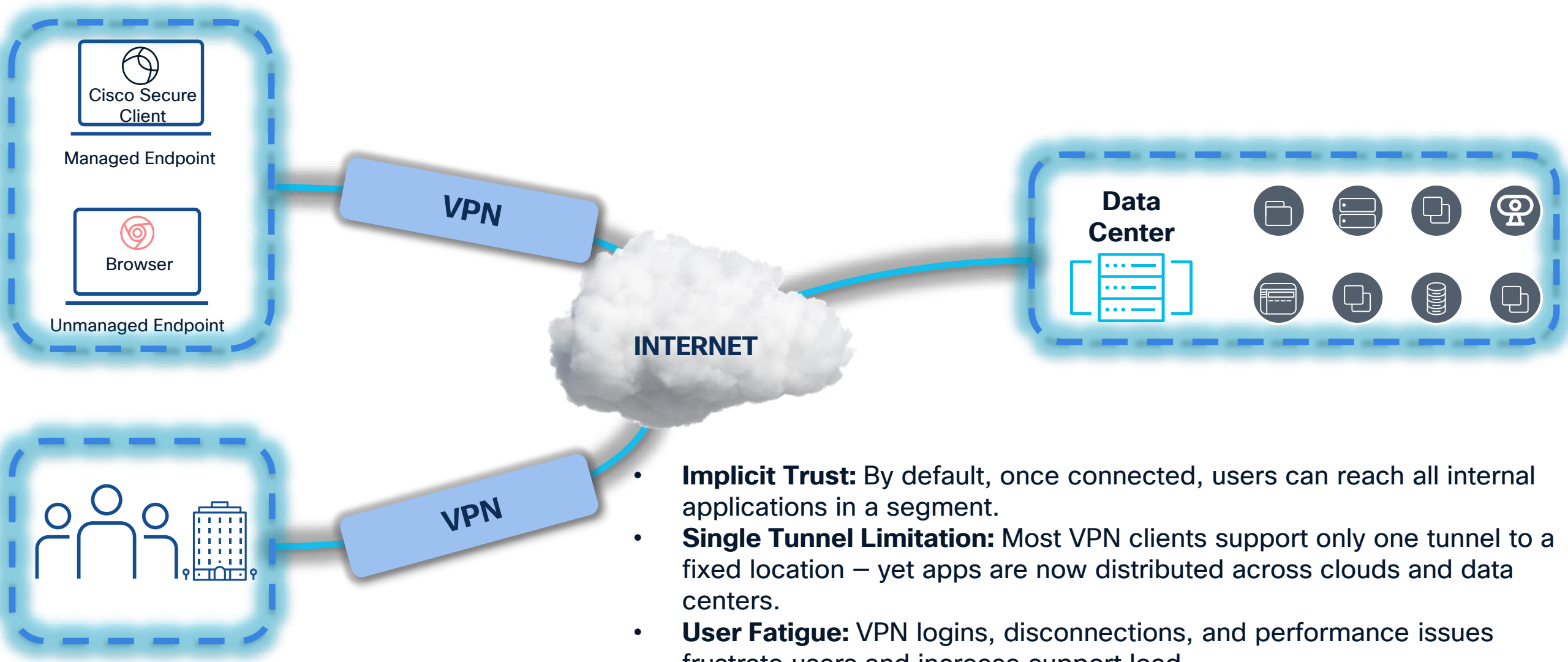
Why Zero Trust Network Access (ZTNA)?

Users in Branch accessing Apps in DC



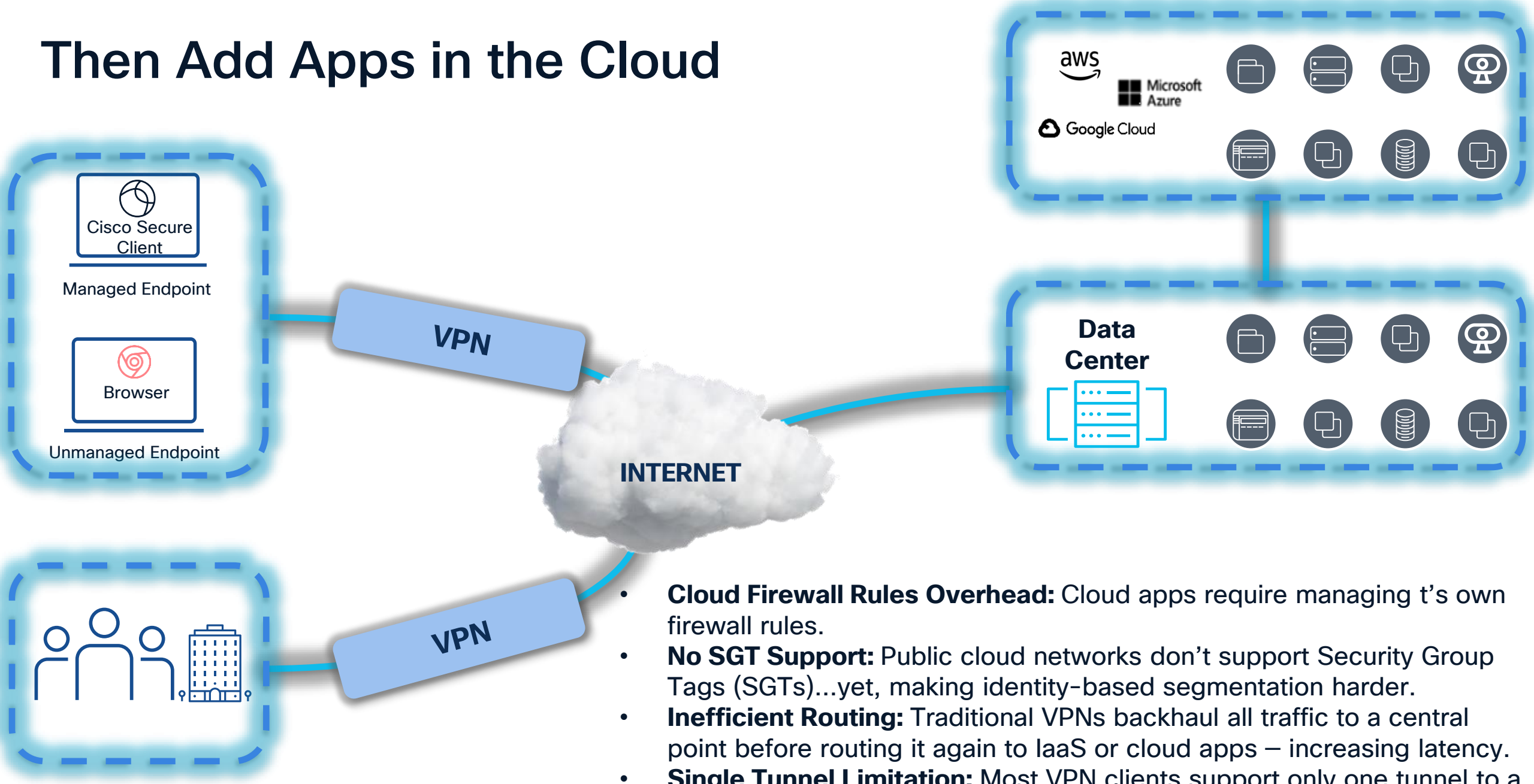
- **Implicit Trust:** Once the tunnel is up, users (or devices) can access broad segments of the data center.
- **Complex Segmentation:** Requires manual configuration of VLANs, firewall rules, and SGTs to limit access.
- **Lack of Identity Awareness:** Access is based on IP/VLAN – no user- or role-level control unless integrated with ISE.
- **Lateral Movement Risk:** Malware or compromised accounts can easily pivot within the network.

Now Add Remote Users



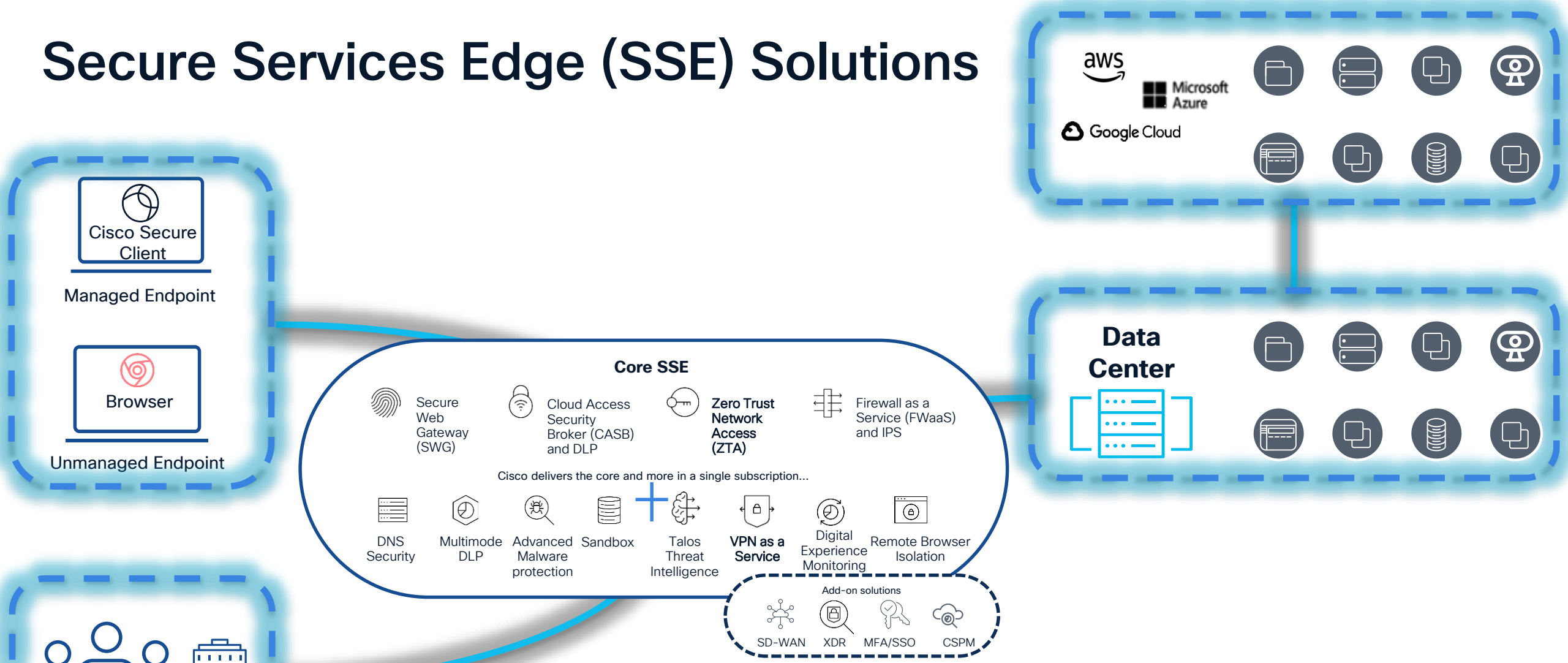
- **Implicit Trust:** By default, once connected, users can reach all internal applications in a segment.
- **Single Tunnel Limitation:** Most VPN clients support only one tunnel to a fixed location – yet apps are now distributed across clouds and data centers.
- **User Fatigue:** VPN logins, disconnections, and performance issues frustrate users and increase support load.
- **Complex Segmentation:** Granular access is only possible if the existing network supports SGT or similar tagging – not always feasible.

Then Add Apps in the Cloud



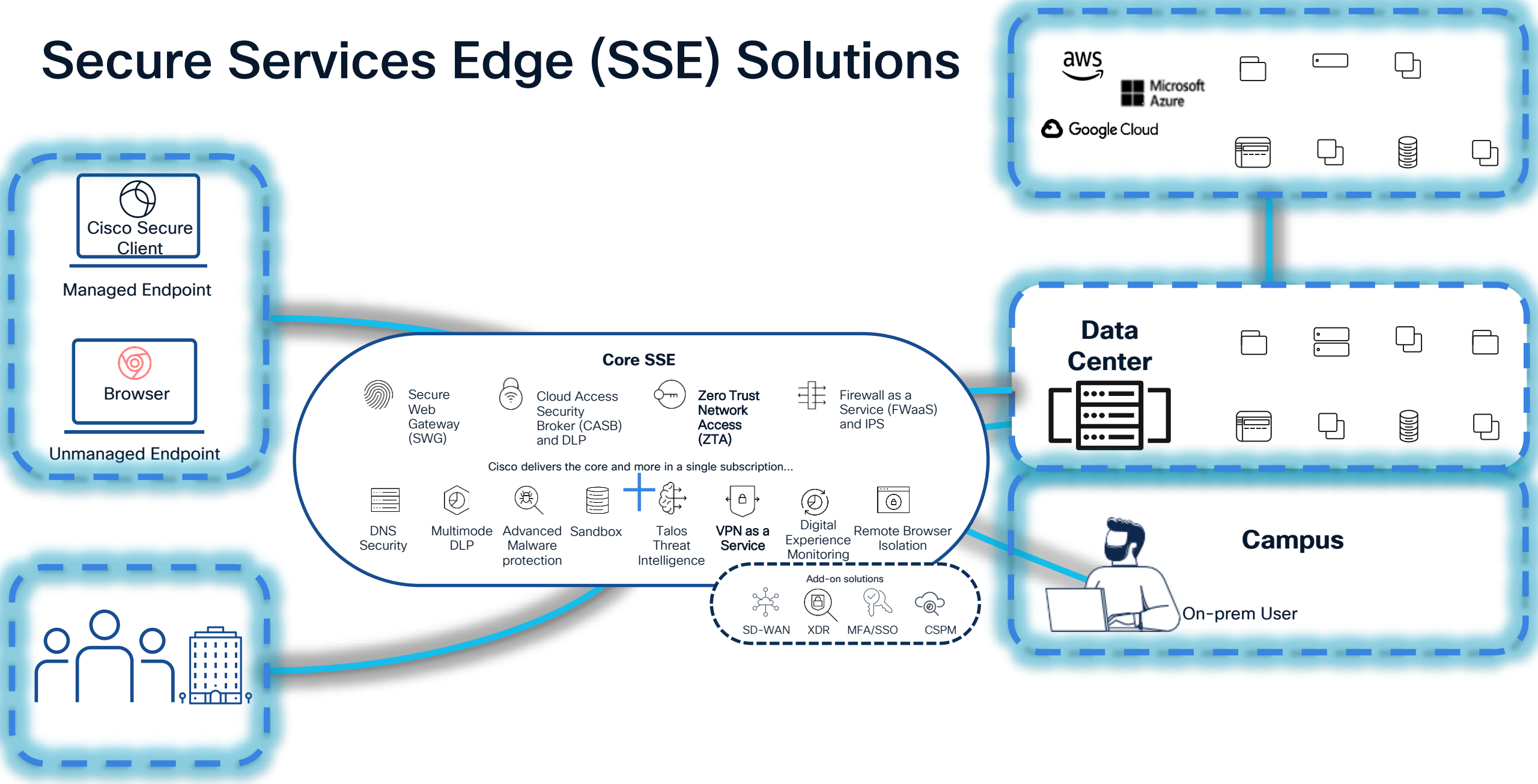
- **Cloud Firewall Rules Overhead:** Cloud apps require managing t's own firewall rules.
- **No SGT Support:** Public cloud networks don't support Security Group Tags (SGTs)...yet, making identity-based segmentation harder.
- **Inefficient Routing:** Traditional VPNs backhaul all traffic to a central point before routing it again to IaaS or cloud apps – increasing latency.
- **Single Tunnel Limitation:** Most VPN clients support only one tunnel to a fixed location, This limits routing flexibility across cloud providers.

Secure Services Edge (SSE) Solutions



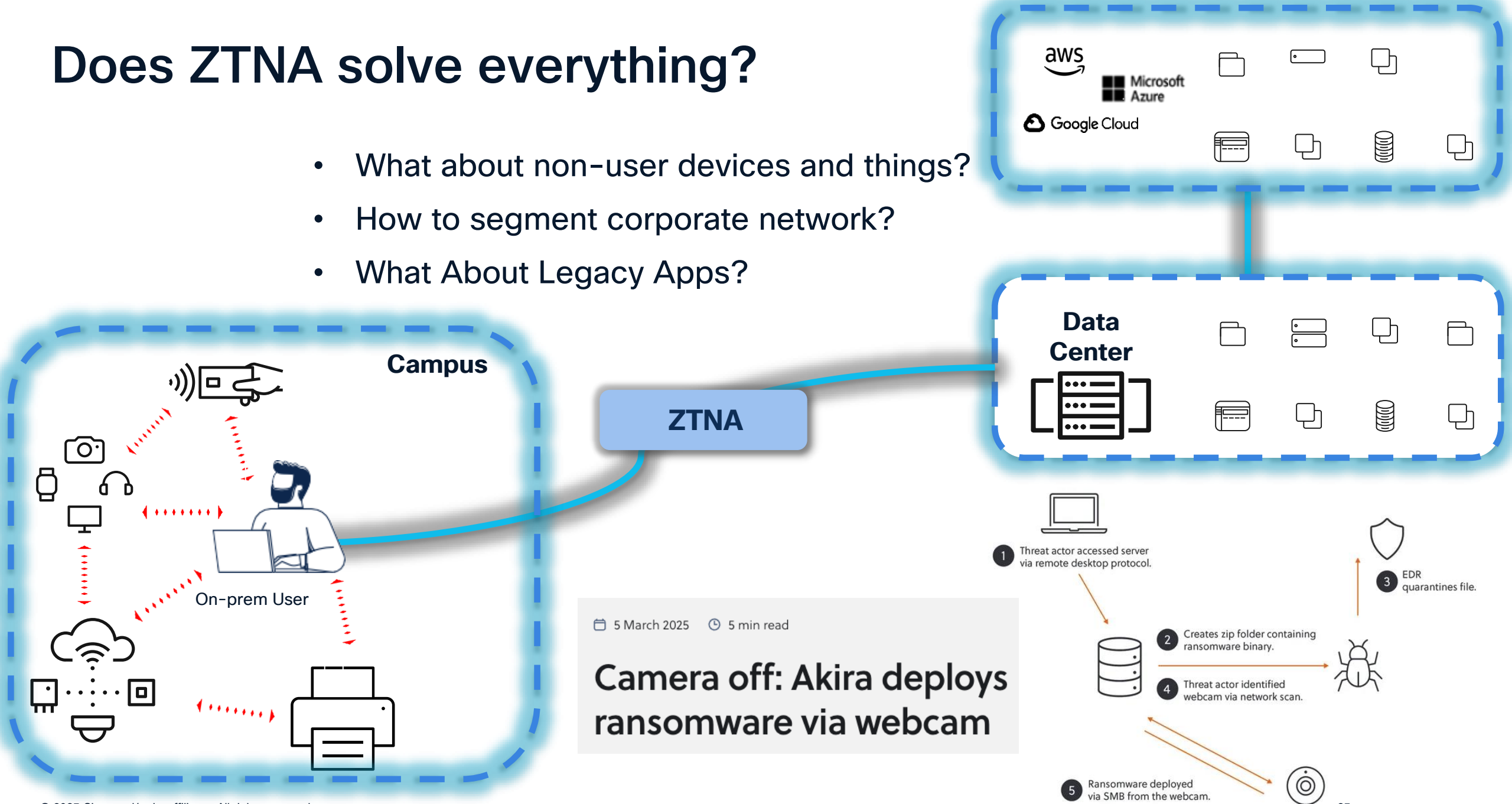
- **Network Re-Architecture Required:** Implementing SSE often involves redesigning routing to steer all user traffic through cloud-based enforcement points.
- **Potential Latency Impact:** Backhauling traffic to SSE PoPs can introduce performance issues, especially for latency-sensitive apps.
- **Application Compatibility Gaps:** Some legacy applications may not be fully compatible with your chosen ZTNA solution.
- **Operational Complexity:** Troubleshooting user issues can be more complex than with legacy VPNs.

Secure Services Edge (SSE) Solutions



Does ZTNA solve everything?

- What about non-user devices and things?
- How to segment corporate network?
- What About Legacy Apps?



5 March 2025 5 min read

Camera off: Akira deploys ransomware via webcam

https://www.s-rminform.com/latest-thinking/camera-off-akira-deploys-ransomware-via-webcam

Universal ZTNA

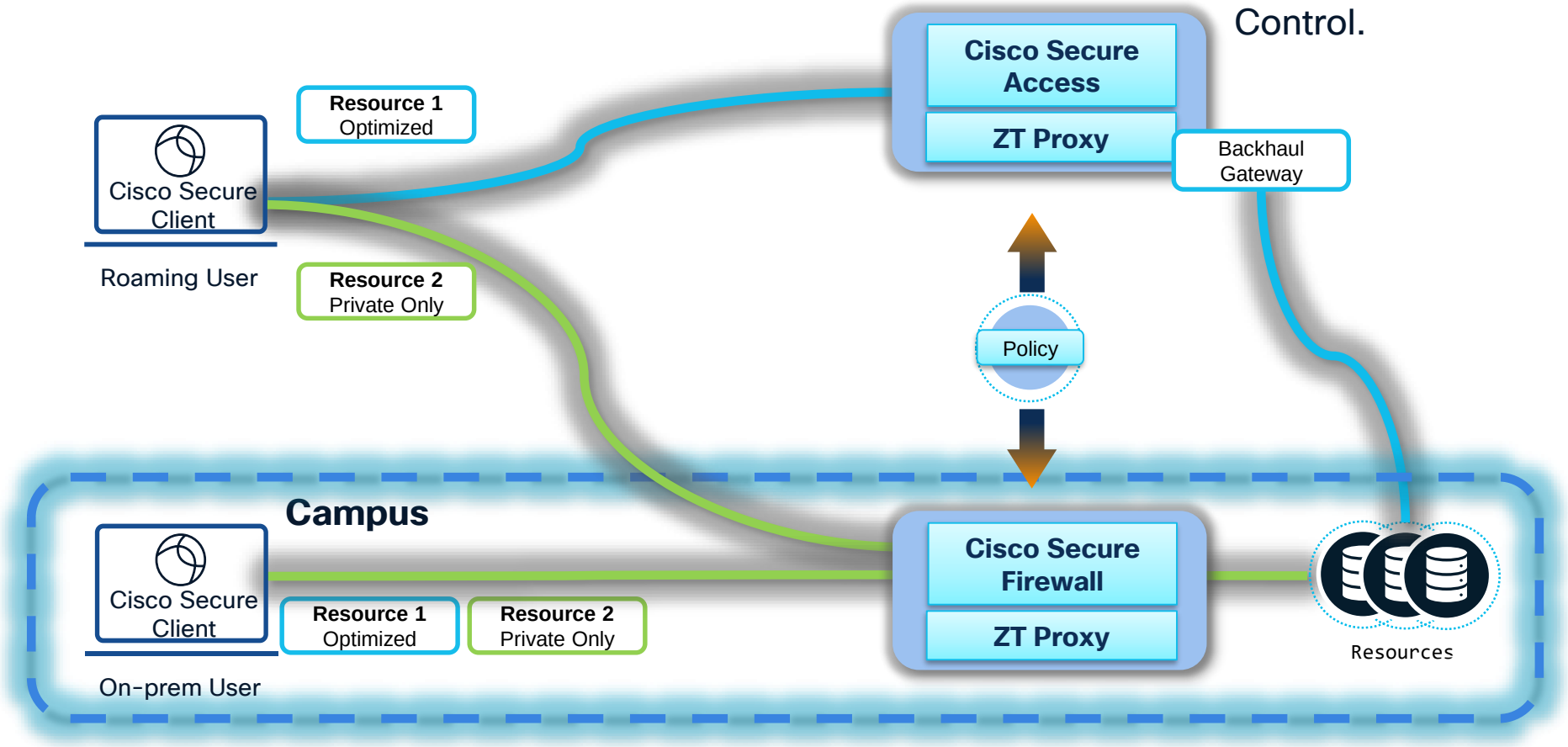
“Having partly started as a “next generation” replacement for VPN connectivity for remote secure access with ZTNA, uZTNA has shifted the value proposition to support local enforcement in on campus and branch “on-premises” locations.”

Gartner Emerging Tech Horizon for Communications – April 2025

Cisco Universal ZTNA

- Single Policy, Distributed Enforcement

- Optimal connectivity based on user location.
- Enterprise privacy for sensitive resources.
- Resiliency in case of catastrophic Cloud Outage.
- Centrally managed through Security Cloud Control.



Universal ZTNA Admin Experience

https://control.v3.int.security.cisco.com/dashboard?en

Security Cloud Control

2 4 Sujith RS

Enterprise
UZTNA-TEST - United States

Home

Products

Firewall

Secure Access

Platform services

Favorites

Security Devices

Shared Objects

Platform Administration

Assign roles

Create organization users and assign roles to control access.

Assign

Other tasks

CLAIM SUBSCRIPTION

Claim subscriptions to activate instances in your organization.

Claim

SET YOUR DEFAULT LANDING PAGE

Select a product page to view first when you enter the organization.

Select

ONBOARD FIREWALL DEVICES

Manage your firewall in Security Cloud Control.

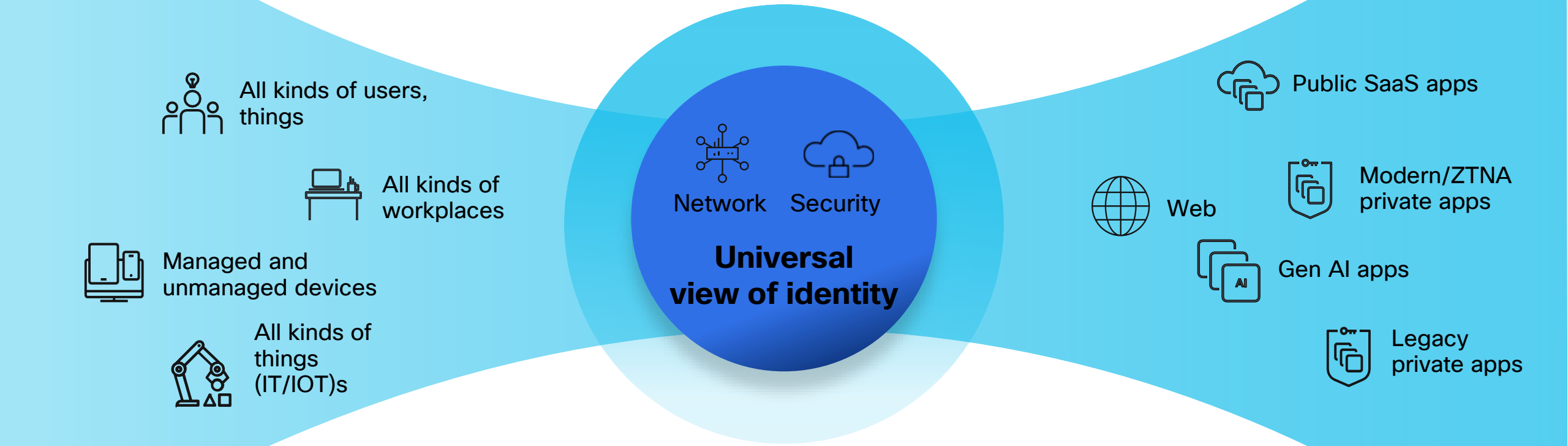
Onboard

INTEGRATE IDENTITY PROVIDER (IDP)

Provide single sign-on (SSO) to your organization's users.

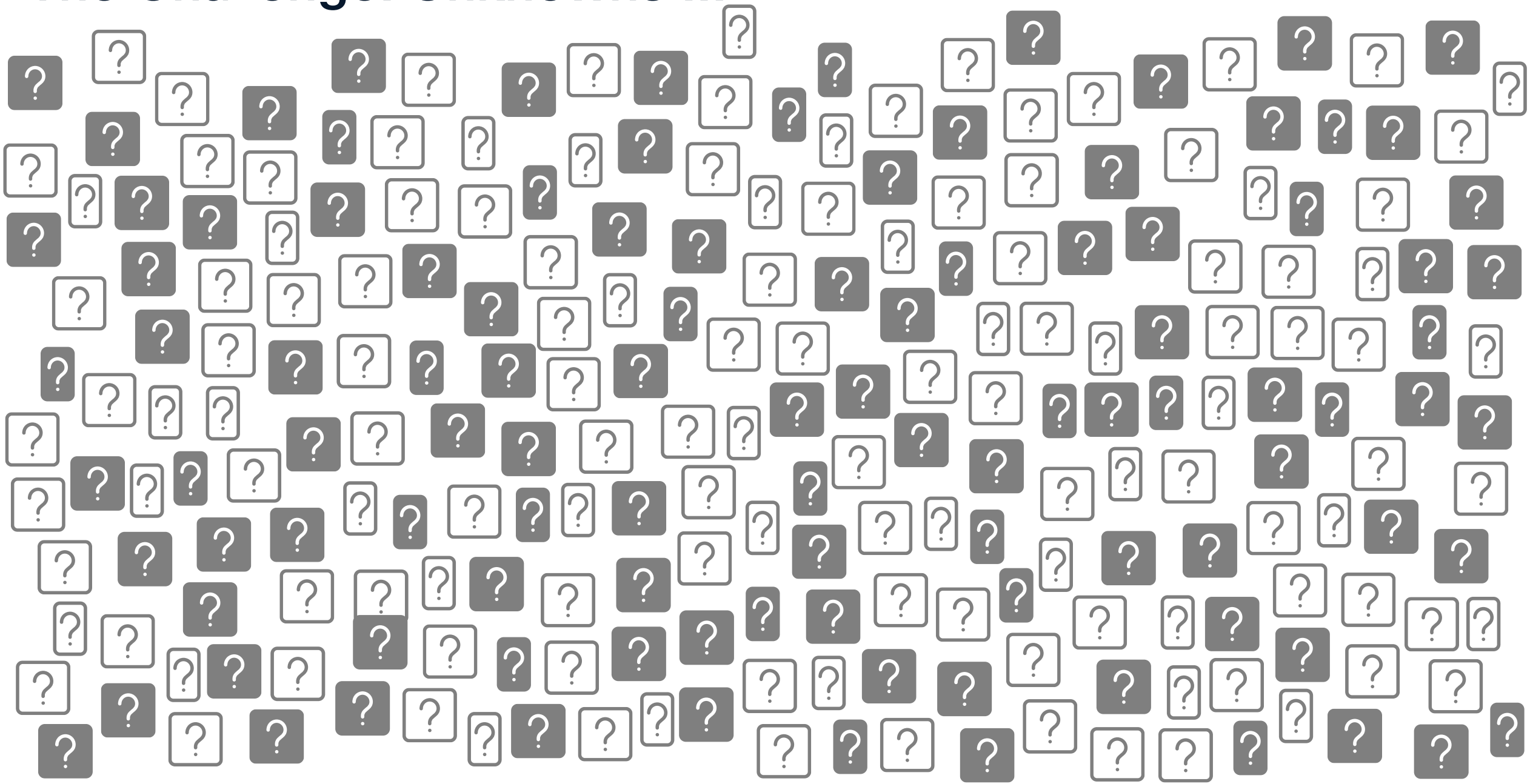
Configure

Universal Identity makes UZTNA Possible



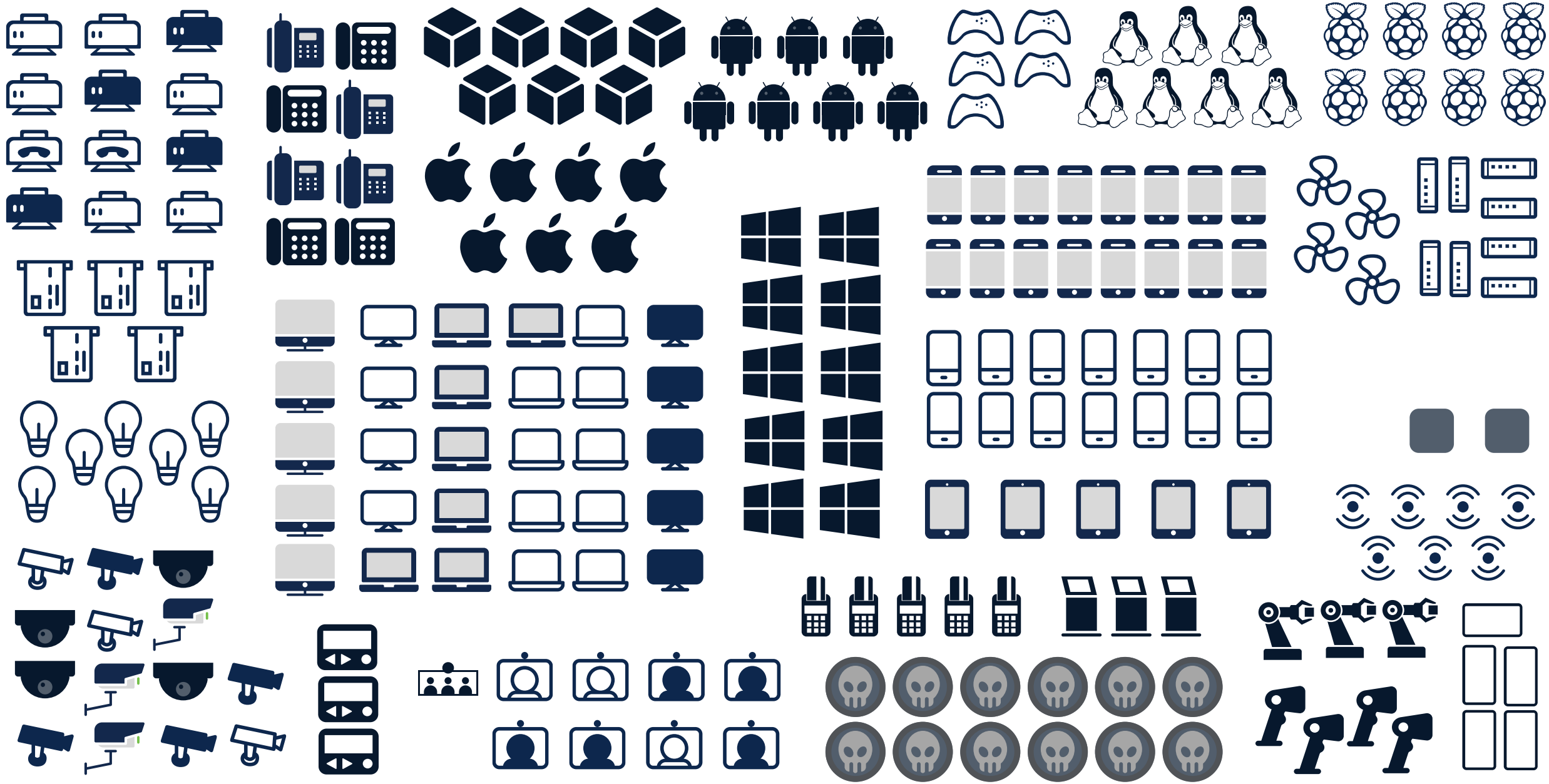
There is no universal zero trust without ubiquitous, shared identity across the enterprise

The Challenge: Unknowns ...

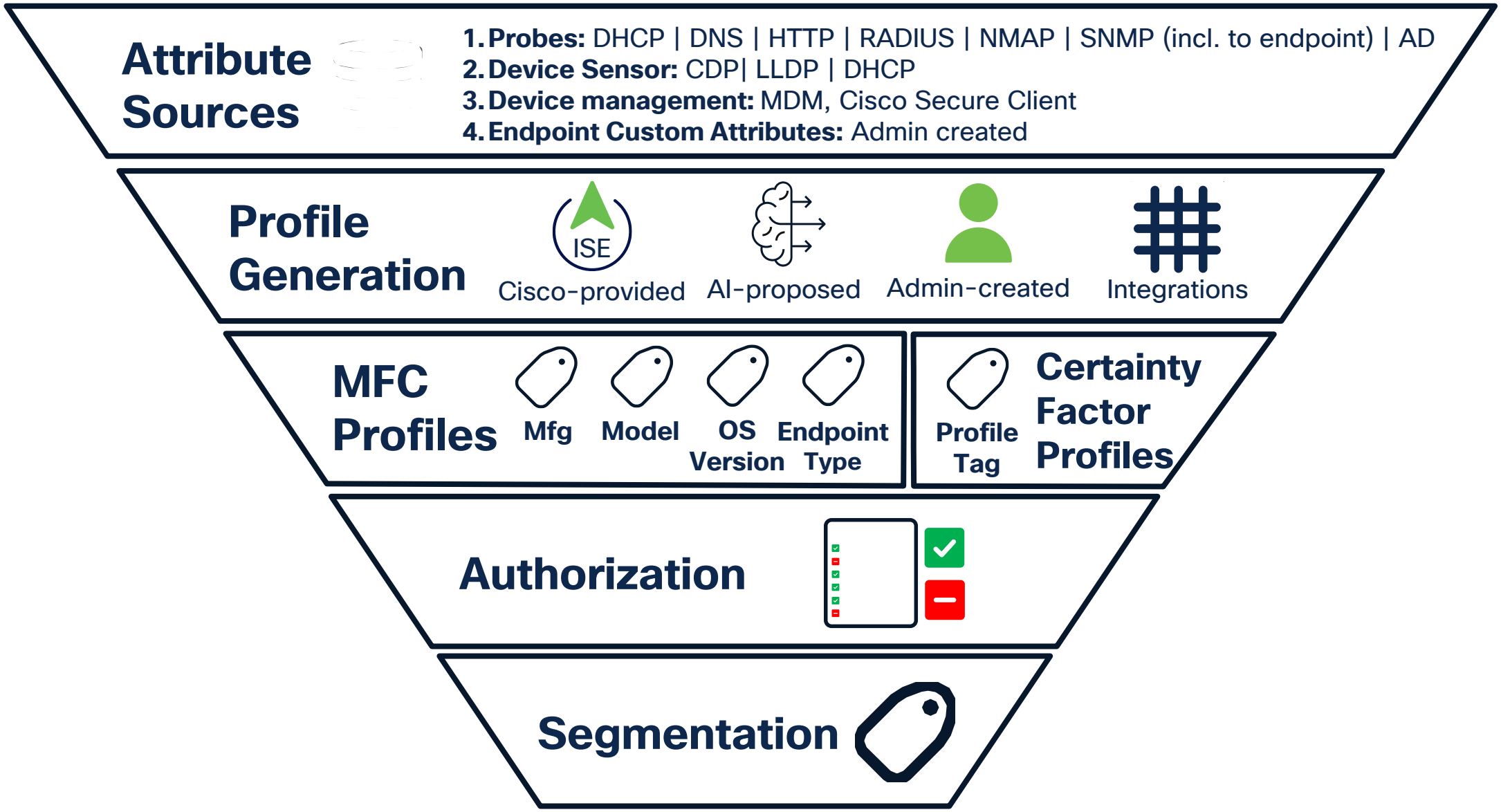


The Challenge: Unknowns to Known ...

The Challenge: Unknowns to Known to Classified

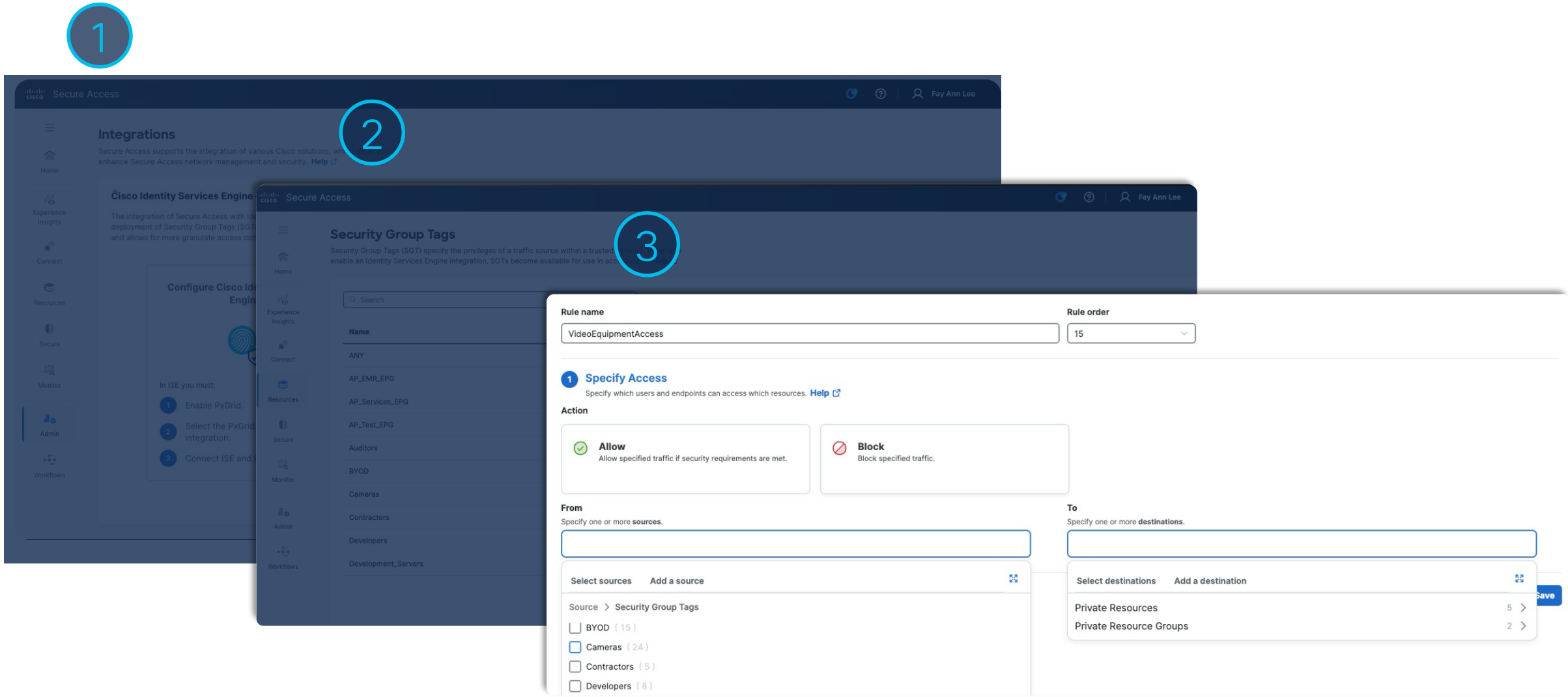


Turning Attributes Into Profiles, Profiles Into Protection



Security Group Tags (SGTs) based policy

Provides SGT attributes from ISE as a source in policy in Secure Access



Cisco ZTNA Options

Cisco ZTNA Options

Duo Network Gateway (DNG)

Secure Firewall

Since 7.4

Secure Access

Cisco Secure Access

Proven cloud-native security converged into one service

Umbrella DNS >12 years

DUO Posture >4 years

Umbrella SWG >5 years

Umbrella CASB >5 years

RBI >5 years

ZTNA >4 years

Secure Client >3 years

VPN Termination >10 years

Cloud Firewall >5 years

Experience Insights/DEM (ThousandEyes) >3 years

Umbrella DLP >5 years

Umbrella Advanced Malware Protection >7 years

Protecting 70,000+ customers | More than 220M endpoints

Validated by Miercom in their 2024 SSE Benchmark Report

Cisco Secure Access

Single EXPERIENCE

- Single Console
- Single Policy
- Single Client
- Single License

Single Client: All-inclusive modules and licensing

AnyConnect VPN (Core)

ZTA Module (new!)

ISE Posture

Secure Endpoint (AMP)

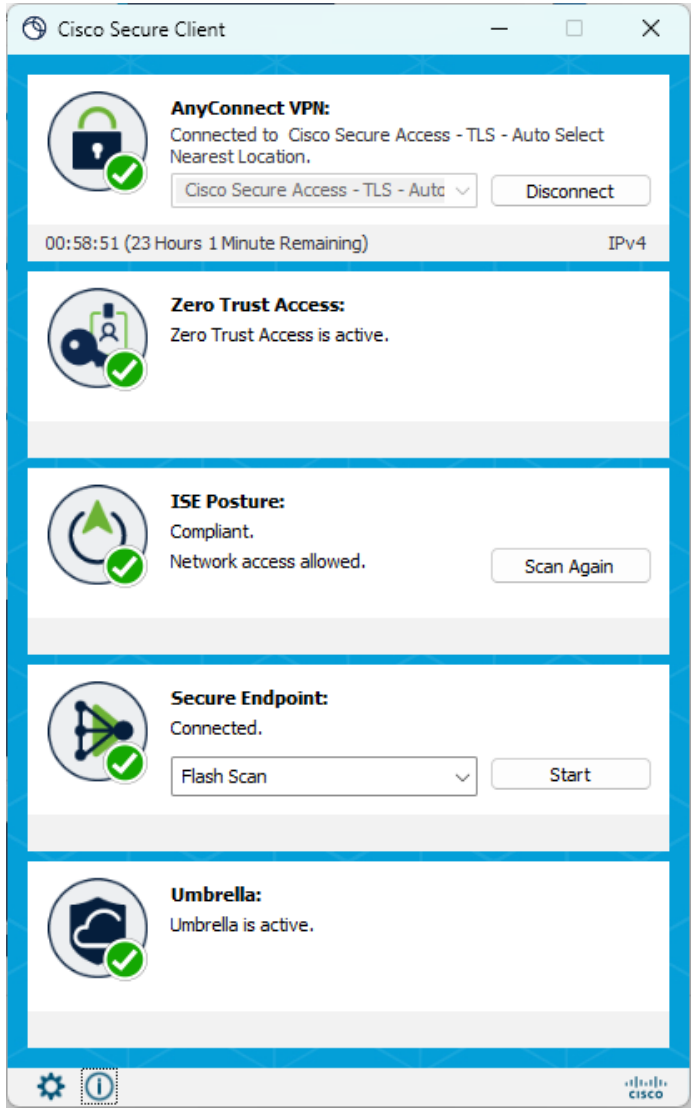
Roaming Module

Thousand Eyes (No UI)

Duo Health (Posture)

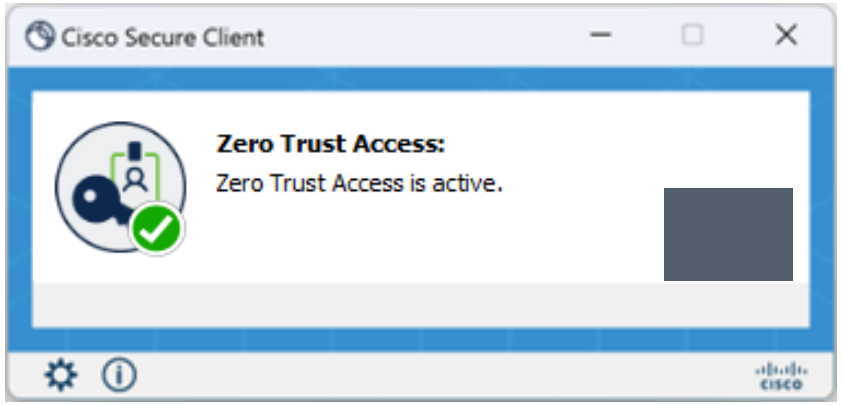
Diagnostic and Reporting (DART)

Cloud Management Module (No UI)



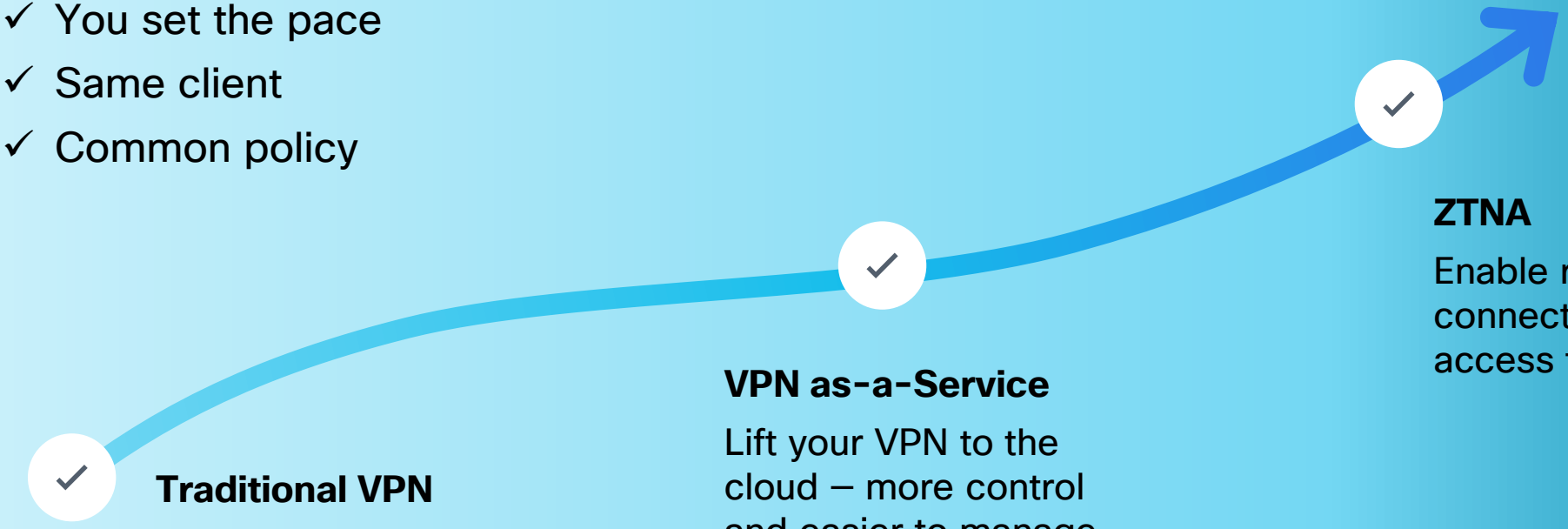
Zero Trust Access Module

- 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.
- Cisco and third-party VPN client interop.
- Next-generation protocol (QUIC & MASQUE).



Flexible Journey to ZTNA

- ✓ You set the pace
- ✓ Same client
- ✓ Common policy



Traditional VPN

Network level access – cannot control at app level

VPN as-a-Service

Lift your VPN to the cloud – more control and easier to manage

ZTNA

Enable remote users to securely connect with least privilege access to private applications

Cisco Secure Client VPNaaS and Zero Trust Access User Experience Demo

Cisco IT’s Journey to SSE

FULL CONFERENCE | IT LEADERSHIP

Cisco IT's Journey to SSE - Enabling Hybrid Work with Cisco Secure Access - BRKCOC-2040

Mike Cifelli, Network Systems Engineer, Cisco
Joe DeSanto, IT Technical Leader, Cisco - **Distinguished Speaker**

Schedule **Tuesday, Jun 10 | 4:30 PM - 5:30 PM PDT**

Cisco IT's journey to Security Service Edge (SSE) highlights prevailing success in our strategic expansion ensuring consistent, reliable, and secure hybrid worker connectivity worldwide.

Through the integration of VPNaaS, Zero Trust Network Access (ZTNA), and Generative AI protection with Secure Web Gateway (SWG), all managed by the Cisco Secure Access cloud service, customers will learn how our adoption is achieving robust and secure access without the need for hardware.

You will also gain insights into our journey on how we are transforming user experience and security while overcoming IT business challenges and ultimately paving the way for enterprise scale and stability.

Session Type: Breakout

Technical Level: Intermediate

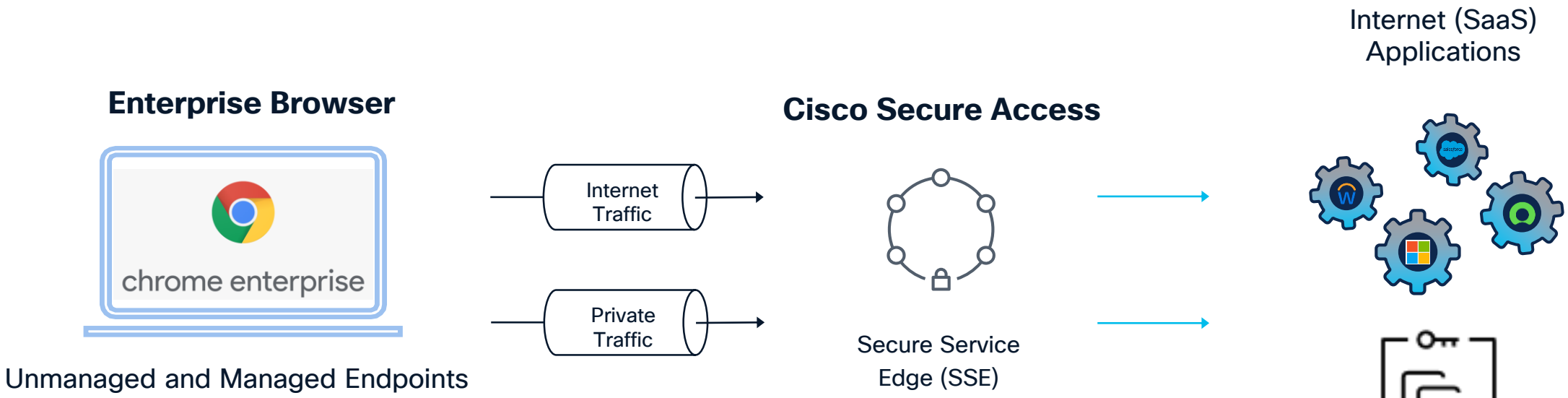
Technology: SASE, Hybrid Work, Security

Track: Security

Wipro's Secure Access and Chrome Enterprise Browser Integration

Secure Access with Enterprise Browser

Zero Trust Access to Private Apps and Internet Apps



- Device Trust
- Posture management
- Data Loss Prevention
- Copy-paste controls, Block Screenshots
- Block file upload/download
- Isolation of Web processes, Site isolation
- Management via Secure Access Console

- Seamless access to private apps
- Secure access to SaaS apps
- Content Inspection
- Access Control
- File type control
- Malware protection

Key takeaways

Key Takeaways

- **VPNs aren’t dead – but they’re no longer enough**. While VPNs still serve remote access use cases, they fall short in today’s hybrid, cloud-first environments.
- **ZTNA advances the model – but doesn’t solve everything**. It brings identity-based access and reduced attack surface, yet struggles with on-prem segmentation, non-user-based devices and legacy aplications.
- **UZTNA takes it further – but isn’t a silver bullet.** It extends ZTNA to support broader use cases, including on-prem users, but it doesn’t replace the advanced visibility and containment features that Cisco ISE provides – the two work best together.
- **Zero Trust isn’t a product – it’s a strategy.** Choose and combine technologies based on your specific environment, risk tolerance, and operational goals.

Which protocol is used by Cisco Secure Access for Client Based Zero Trust Network Access (ZTNA)?

Which of the following is a core advantage of Universal ZTNA (UZTNA) over traditional ZTNA?

Which feature is a key characteristic of ZTNA but not typically found in VPNs?

What is a significant challenge faced in the use case of a local user accessing an application within the same location in a Zero Trust Network Access (ZTNA) environment?

Which connectivity options are available in Cisco Secure Access for accessing private applications?

Who is the legendary Costa Rican goalkeeper known for starring in multiple World Cups and playing for clubs like Real Madrid and PSG?

Complete your session evaluations

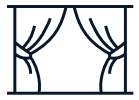
Complete a minimum of 4 session surveys and the Overall Event Survey to be entered in a drawing to win 1 of 5 full conference passes to Cisco Live 2026.

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



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

Contact me at: josemed@cisco.com

Thank you

cisco Live !


CISCO