Cisco Tech Day
Denver

Universal ZTNA in a SASE World

Rob Wiley
GES Solutions Engineer

Thank you to our sponsors!

World Wide Technology, Inc.

PRESIDIO®

robwiley@coyote:~$ whoami ; curl https://www.linkedin.com/in/robfwiley | qf -ri

NAME: Rob Wiley

TITLE: Global Enterprise Solutions Engineer @ Cisco

TENURE: 2006 – 2012 AS NCE (Best Buy, Target, Cargill, Accenture)

2012 – 2020,2025 – Present Solutions Engineer

RELEVANCE: Returned in August 2025 after 5 years as a SASE DC @ PAN

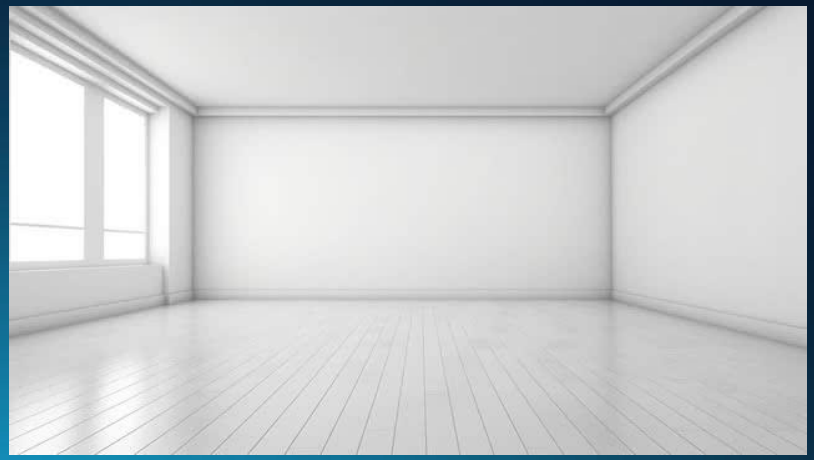
ACTIVE_PROCESSES:

> Jiu-Jitsu & Gym Rat

> Empty nester with zero boomerangs!

> Typical Cisco Nerd

robwiley@coyote:~$



cisco

Agenda

- Evolution of ZTNA
- UZTNA Architecture with Cisco Secure Access
- Flexible Zero Friction Access
- The Identity Layer: Cisco Identity Intelligence
- DEM: Actionable Experience Insights
- Integrations to the Wired World

A quick question…

Why we should care about ZTNA Strategies

91%

of employees are using multiple networks to connect to work

85%

of employees access company platforms from unmanaged devices

82%

of organizations cite remote logins as a heightened threat vector

60%

Talos IR incidents involved Identity

44%

Identity attacks specifically targeted Active Directory

cisco

The State of Zero Trust Maturity

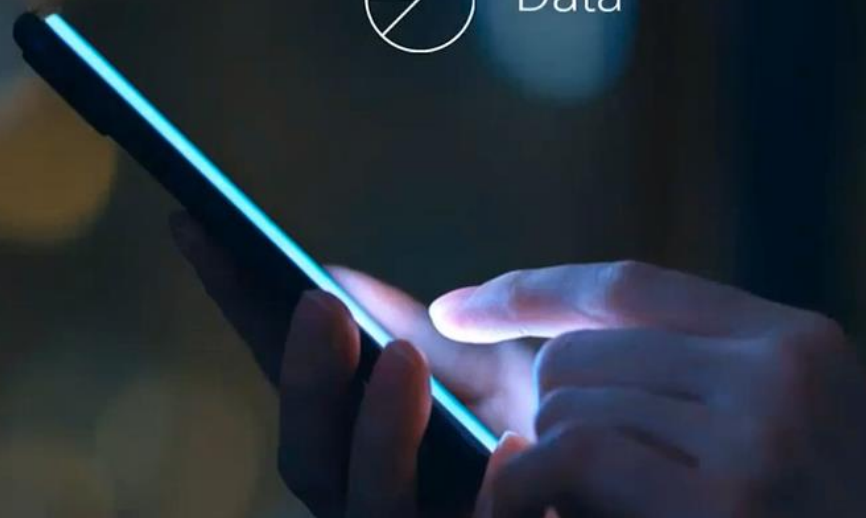
Identity

Network

Devices

Apps/Workload

Data



86%

Nearly all organizations have started on some aspect of zero trust (at least one pillar)

"We know we need to do it"

36%

Have reached maturity in at least one pillar

"Our focus is on XYZ pillar"

2%

Have reached maturity across all pillars which means that 98% have not.

"We've still got a long way to go"

Traditional ZTNA: The OG Use Case, Work from home

Managed

Remote

STEP 2
Access

Policy A:
Strict access control

Blind Trust

Policy B:
Direct access

In office

Private apps

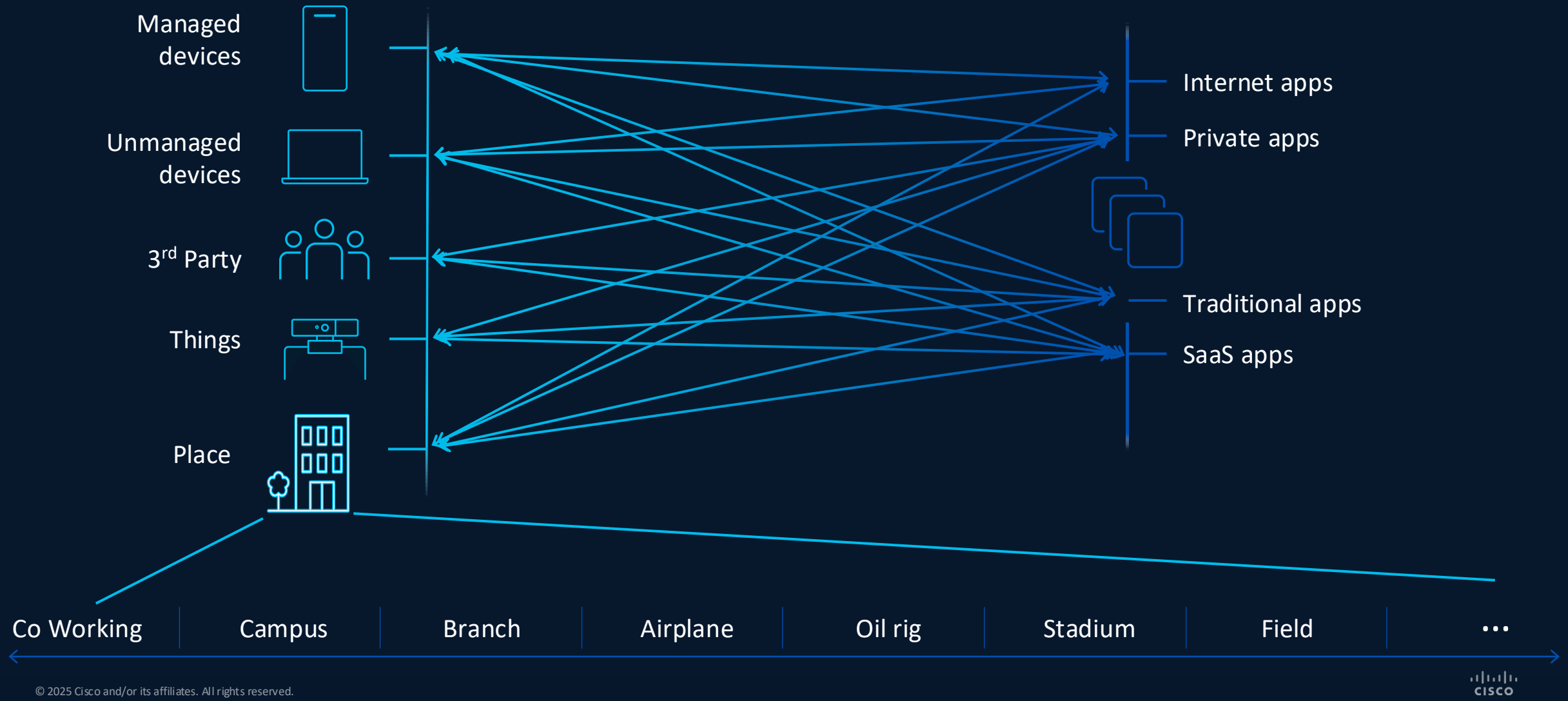
Traditional apps

Managed devices, private apps

Different policies for home versus office

Blind trust between authentication and access

Traditional ZTNA: Work from Anywhere to Any Location



SSE and zero trust initiatives

Current state

Frustrated Users

+

Overworked IT / Security

=

Successful attackers

There must be a better way.

cisco

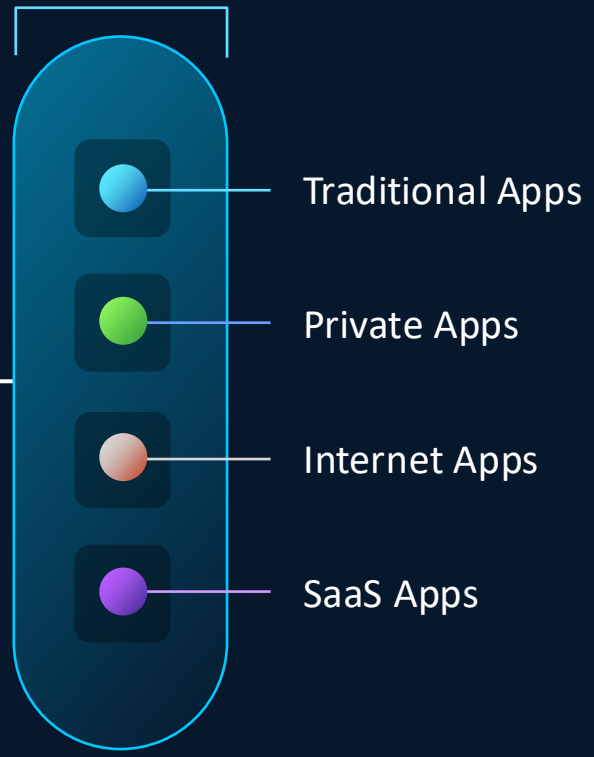
Cisco Universal ZTNA

Every device, person, thing, everywhere

Zero downtime:
Experience and Policy Assurance

Zero impostors:
Identity Trust

Zero friction:
We do the plumbing.



Consistent Security:
Security Service Edge

cisco

Cisco Secure Access

Cisco SSE – **Single Vendor** SASE

Core SSE

- Secure Web Gateway (SWG)
- Cloud Access Security Broker (CASB) and DLP
- Zero Trust Network Access (ZTA)
- Firewall as a Service (FWaaS) and IPS

Cisco delivers the core and more in a single subscription…

- DNS Security
- Multimode DLP
- Advanced Malware protection
- Sandbox
- Talos Threat Intelligence
- VPN as a Service
- Digital Experience Monitoring*
- Remote Browser Isolation*

Add-on solutions

- SD-WAN
- XDR
- DUO IAM
- CSPM

* Included in the unified experience / separate license (optional)

Safe Use of AI Apps & Agentic AI

Classification: **Safety Guardrail**

Toxicity

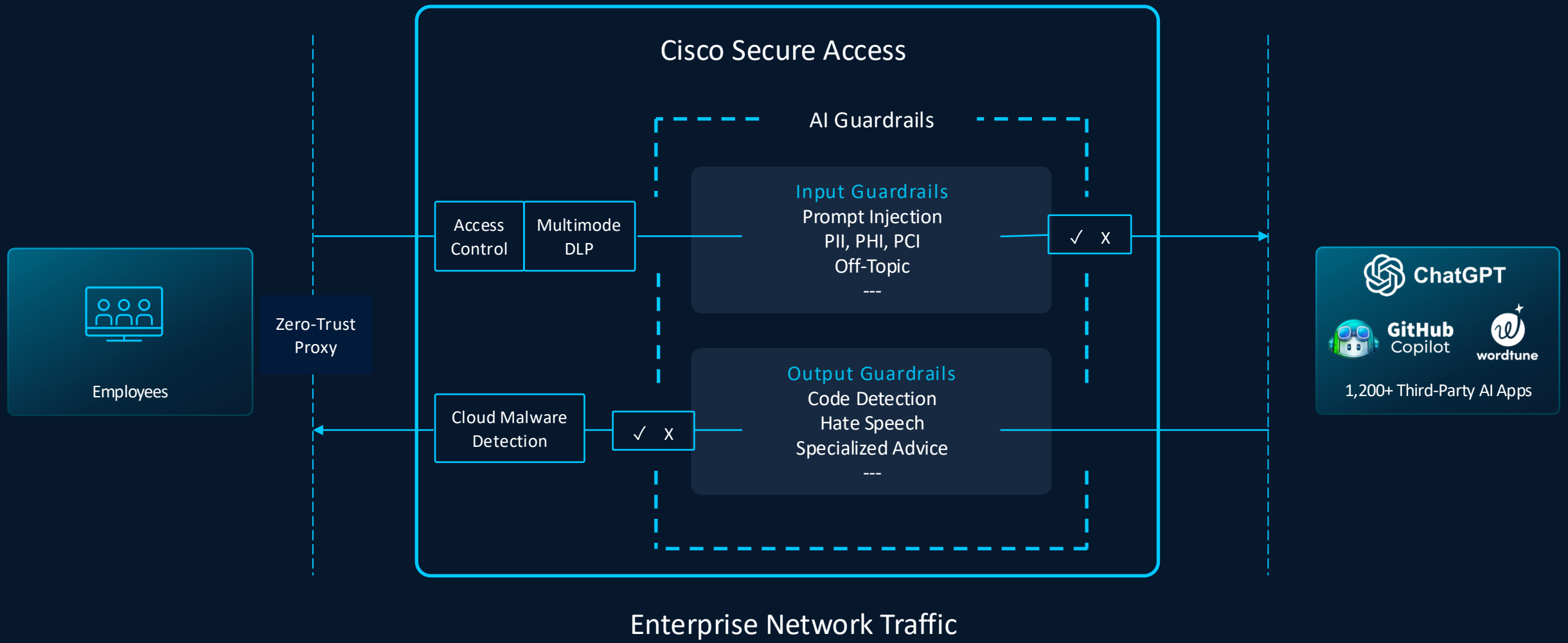
How to make a bomb

Classification: **Safety Guardrail**

Privacy

Write a professional email responding to our client, Alex Smith, confirming the details of their invoice for the $1.2M deal with ACME Company.

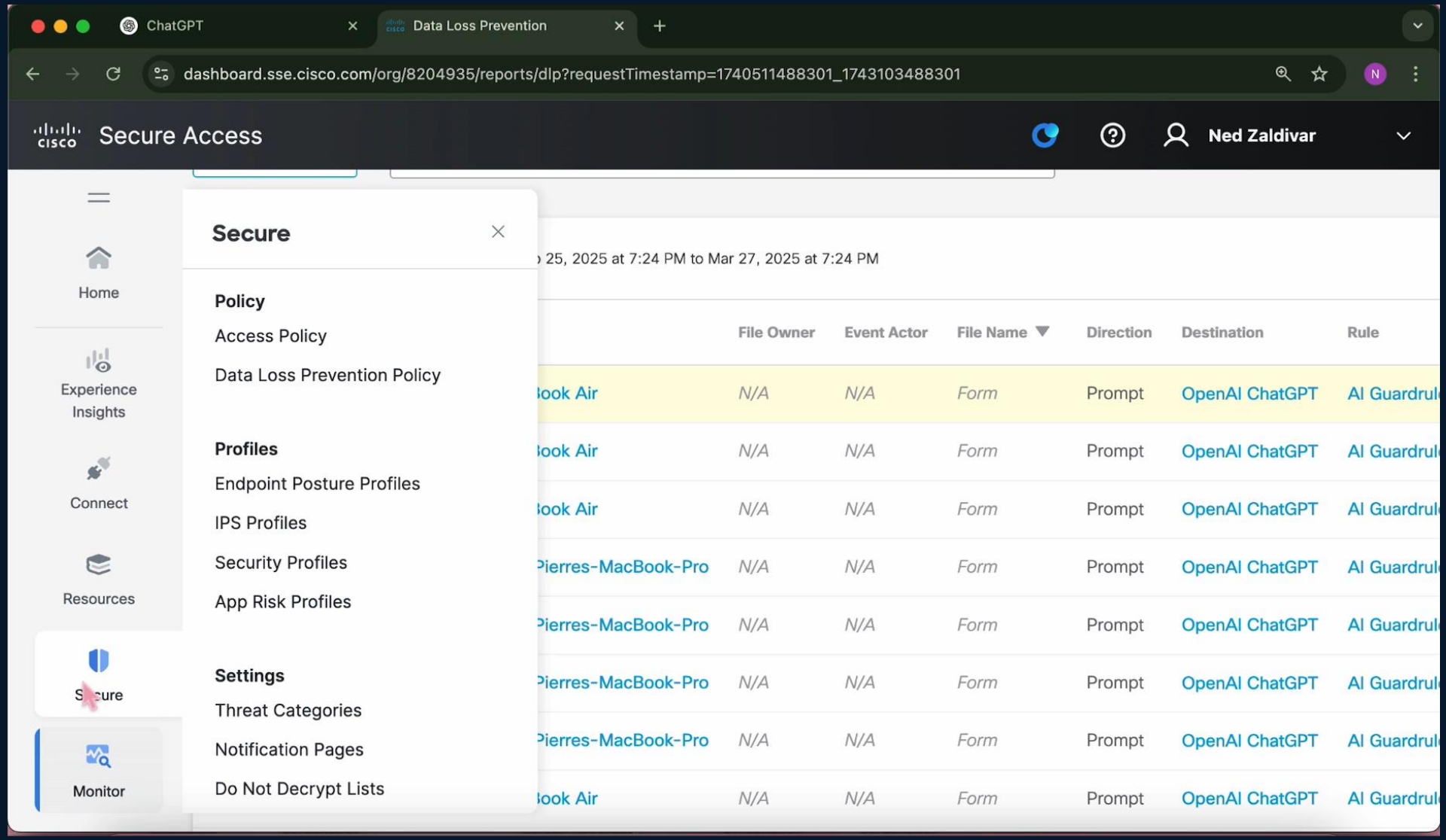
Protecting Usage of Third-Party AI Apps



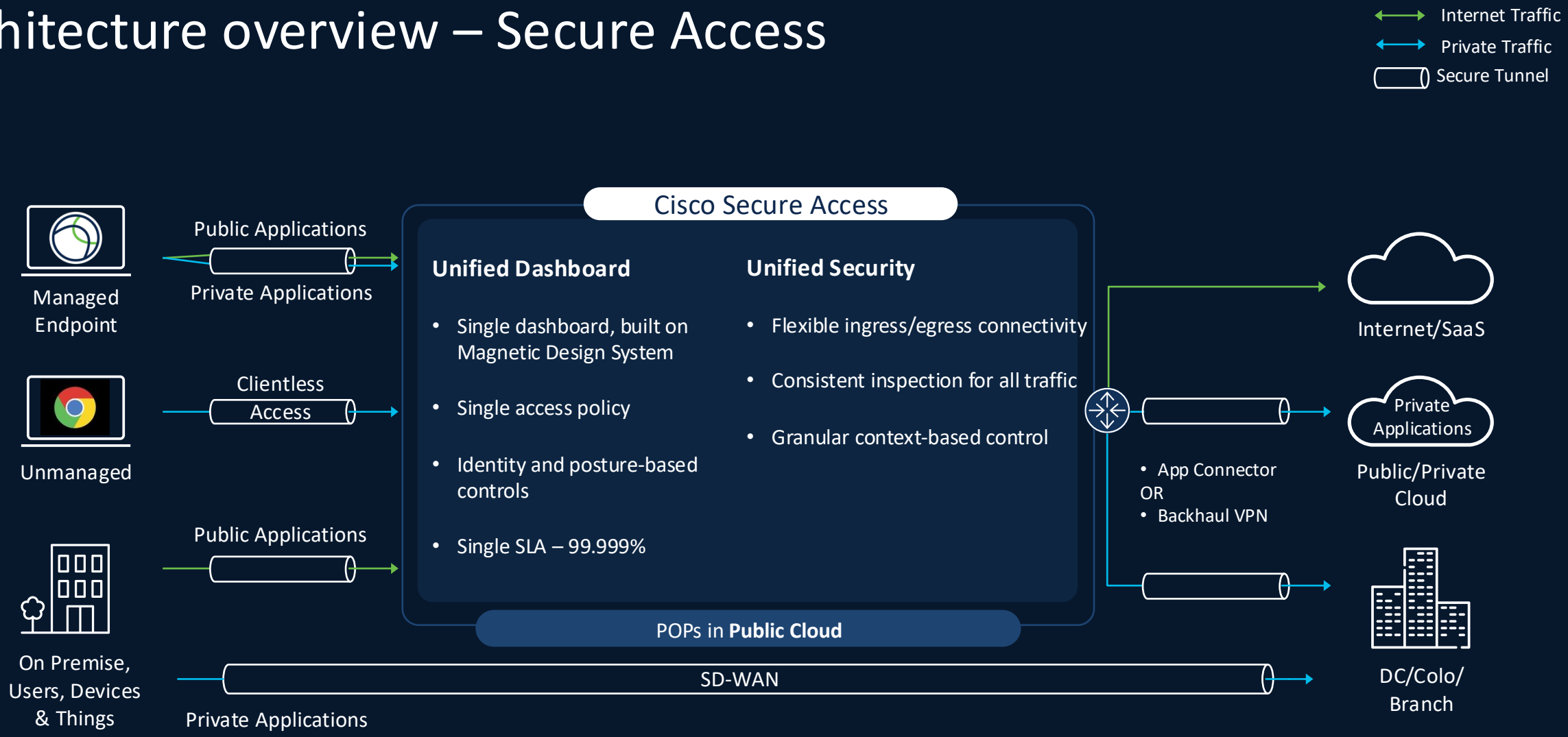
AI Access Demo

Shadow AI Security with Cisco Secure Access Demo

Shadow AI Security with Cisco Secure Access Demo



Architecture overview – Secure Access



Users & Devices — **How** — **Apps**

Cisco Secure Access

Proven cloud-native security converged into one service

Umbrella DNS
>12 years

Umbrella SWG
>5 years

DUO Posture
>4 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

Cisco Secure Access

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

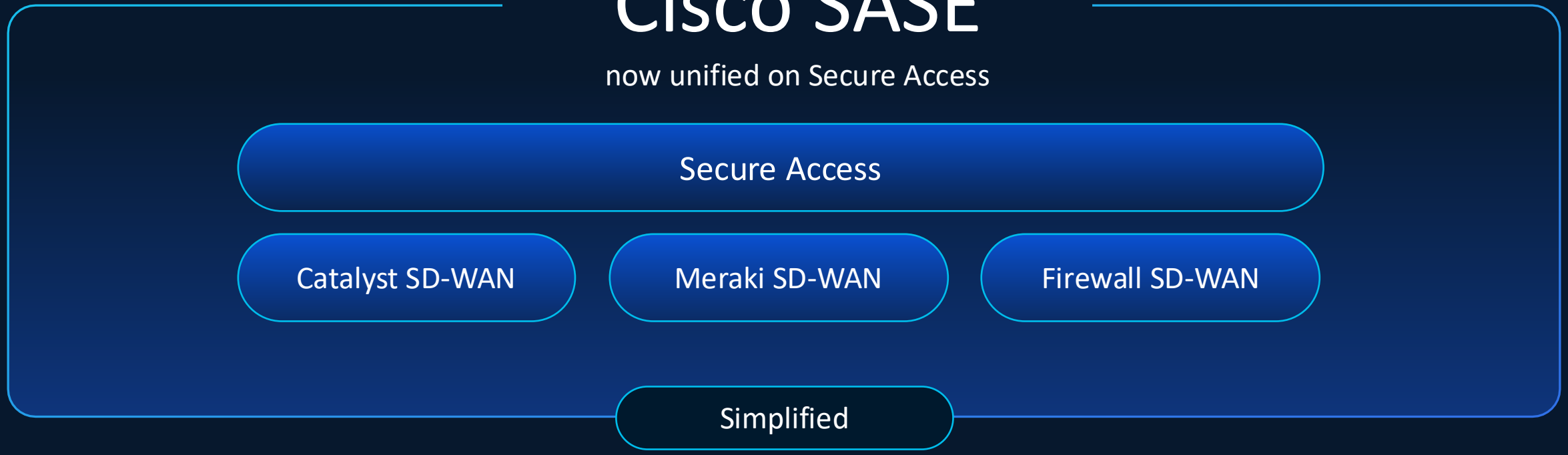
Single EXPERIENCE

Cisco Universal ZTNA

Takes ZTNA to users and **devices**

Cisco SASE

now unified on Secure Access



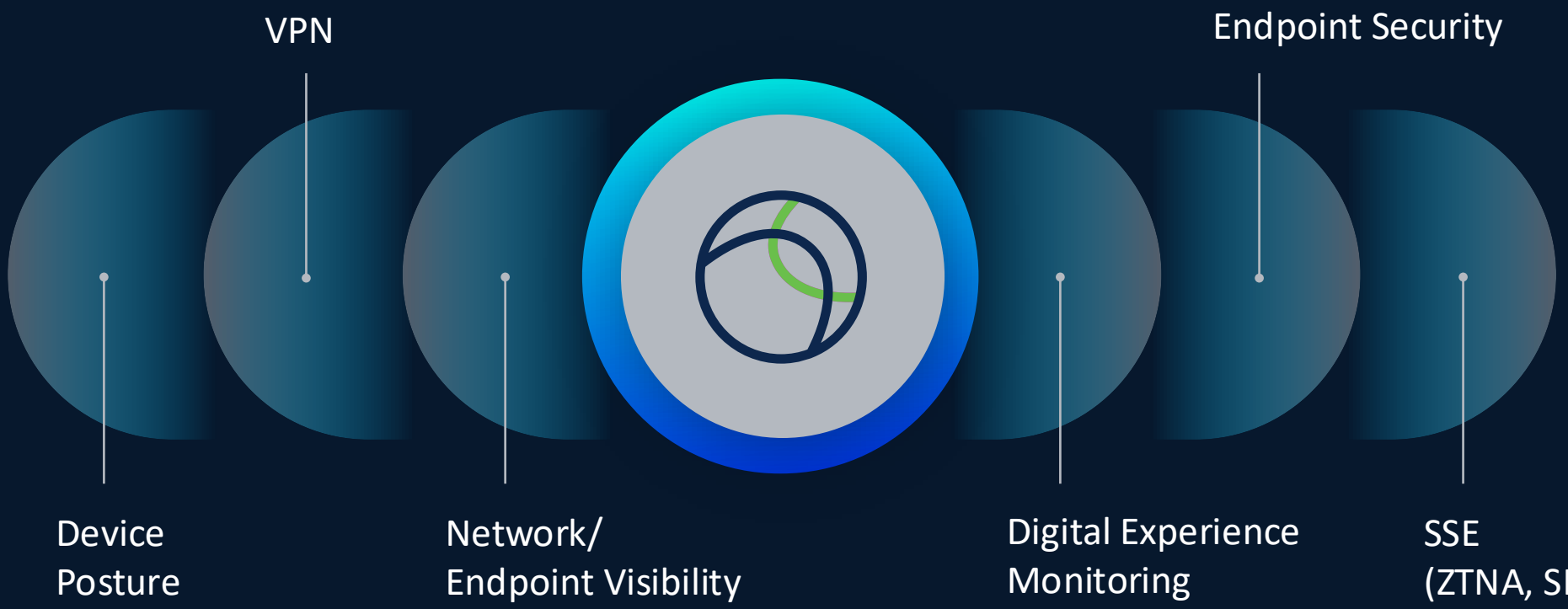
Flexibility to choose optimal connectivity

Unified security policy managed by Security Cloud Control

Consistent cloud enforcement

Flexible Zero Friction Access

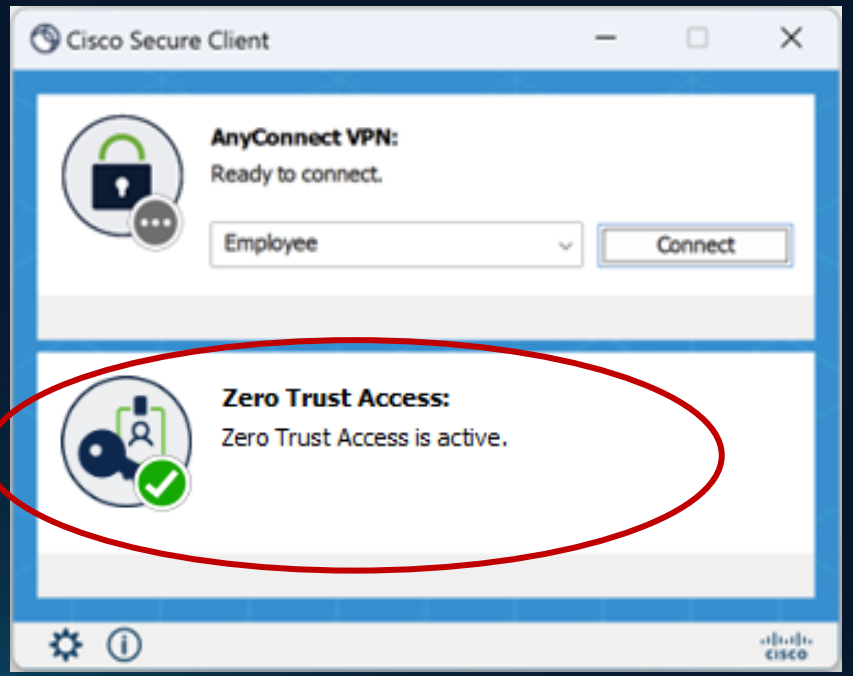
One client, multiple functions



Zero Trust access module

New in Cisco Secure Client for Cisco Secure Access

- 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
- **Delivered over Next Gen protocol (QUIC Tunnel & MASQUE Proxy)**



MASQUE and QUIC

Built-in security and performance

RDP

Chrome

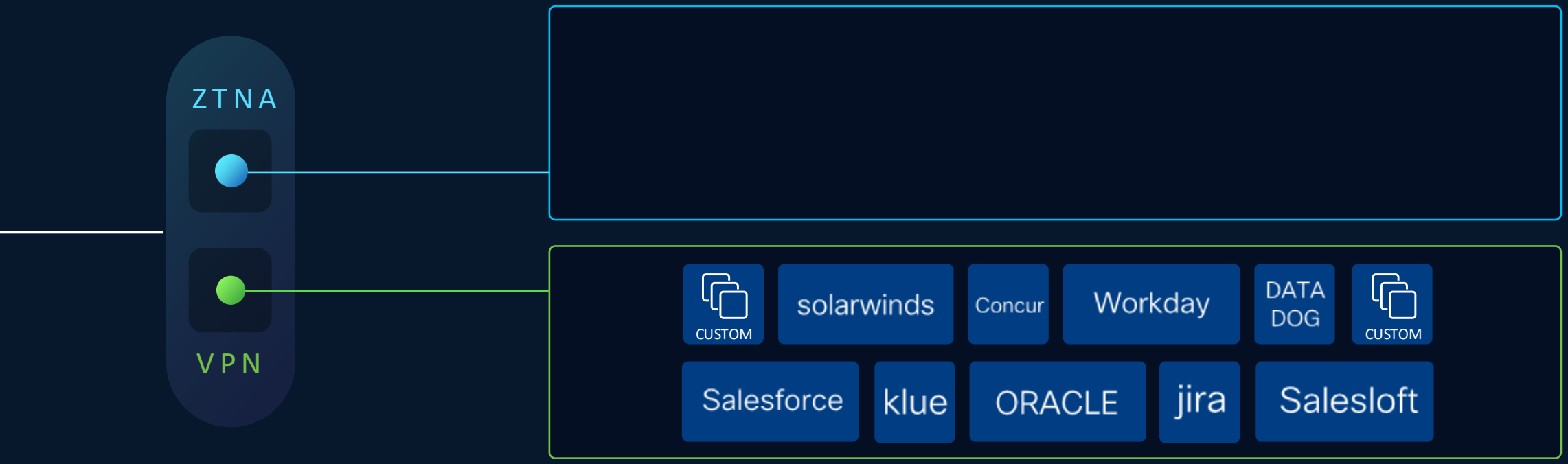
QUIC: Transport protocol improving Performance and Security

MASQUE: Framework for tunneling protocols over QUIC.

- ✓ Seamless connection migration
  Better throughput and latency
- ✓ Integrated into mobile OS
  (iOS and Android)
- ✓ Secure-by-default
  Users and Applications are fully isolated.

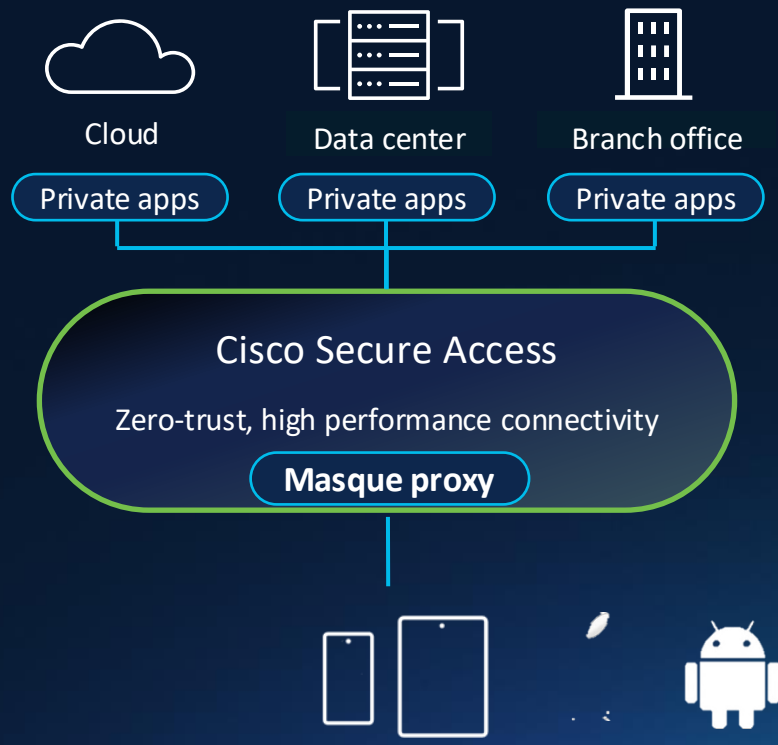
Seamless transition to ZTNA

VPN-as-a-Service simplifies ZTNA roll-out



Zero Trust secure access from mobile devices

Apple iOS and Android



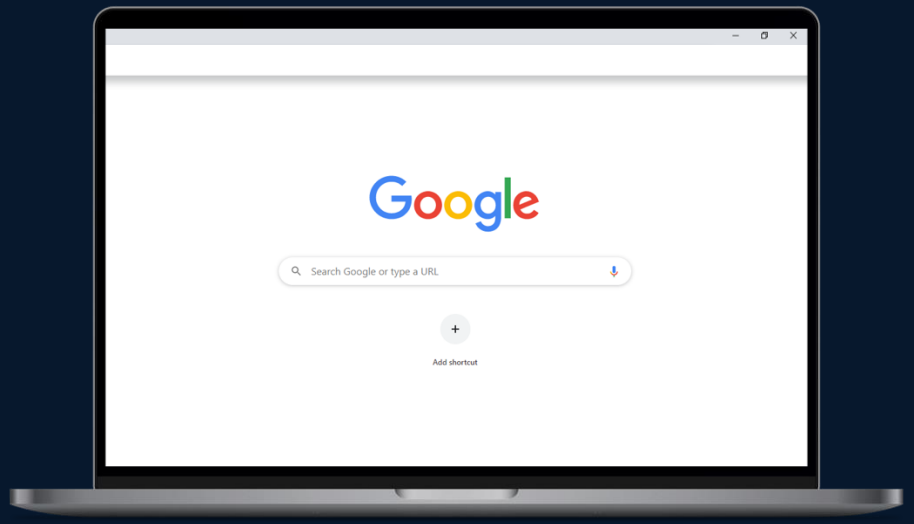
Cisco and major mobile providers collaborated to develop the industry's first zero-trust architecture for mobile devices

- Apple iOS 17+
- Generic Android 14+
- Android on Samsung Knox 3.10+

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

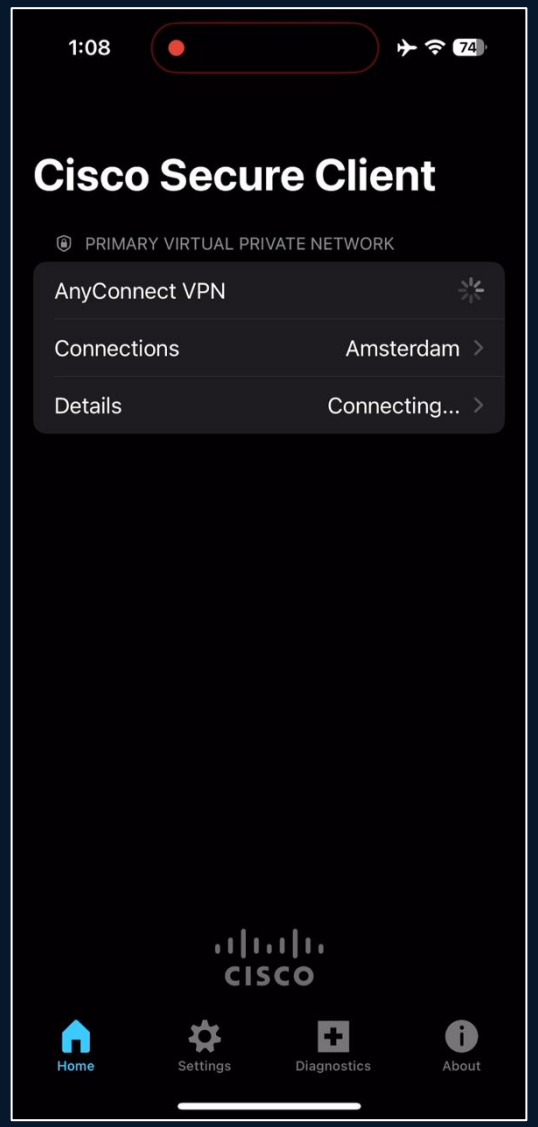
Native Device Support

BYOD via enterprise managed Google Chrome
Advanced protocol support for Apple, Samsung

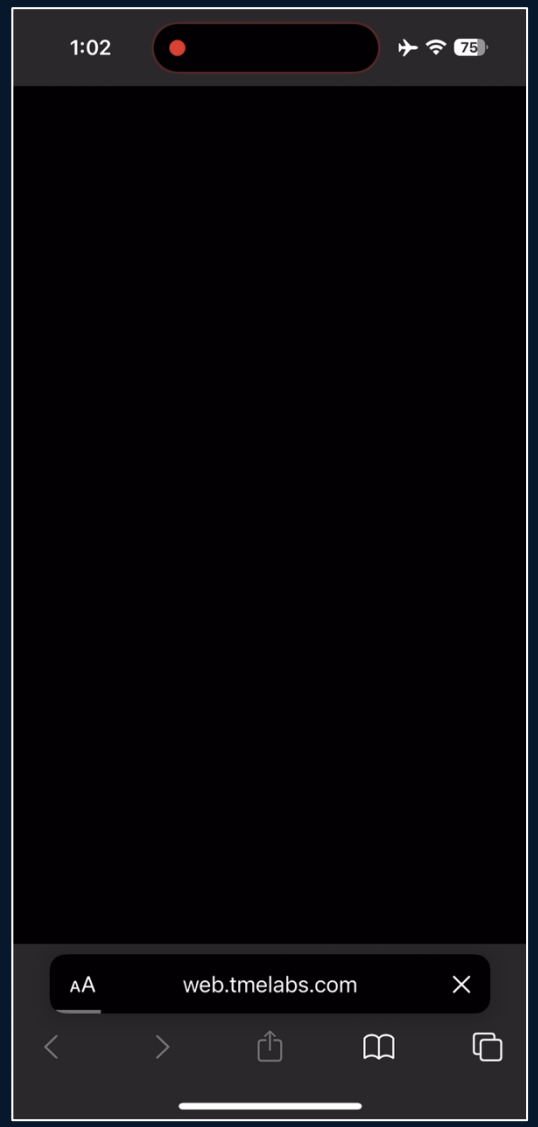


Chrome Enterprise Browser

Native OS Integration

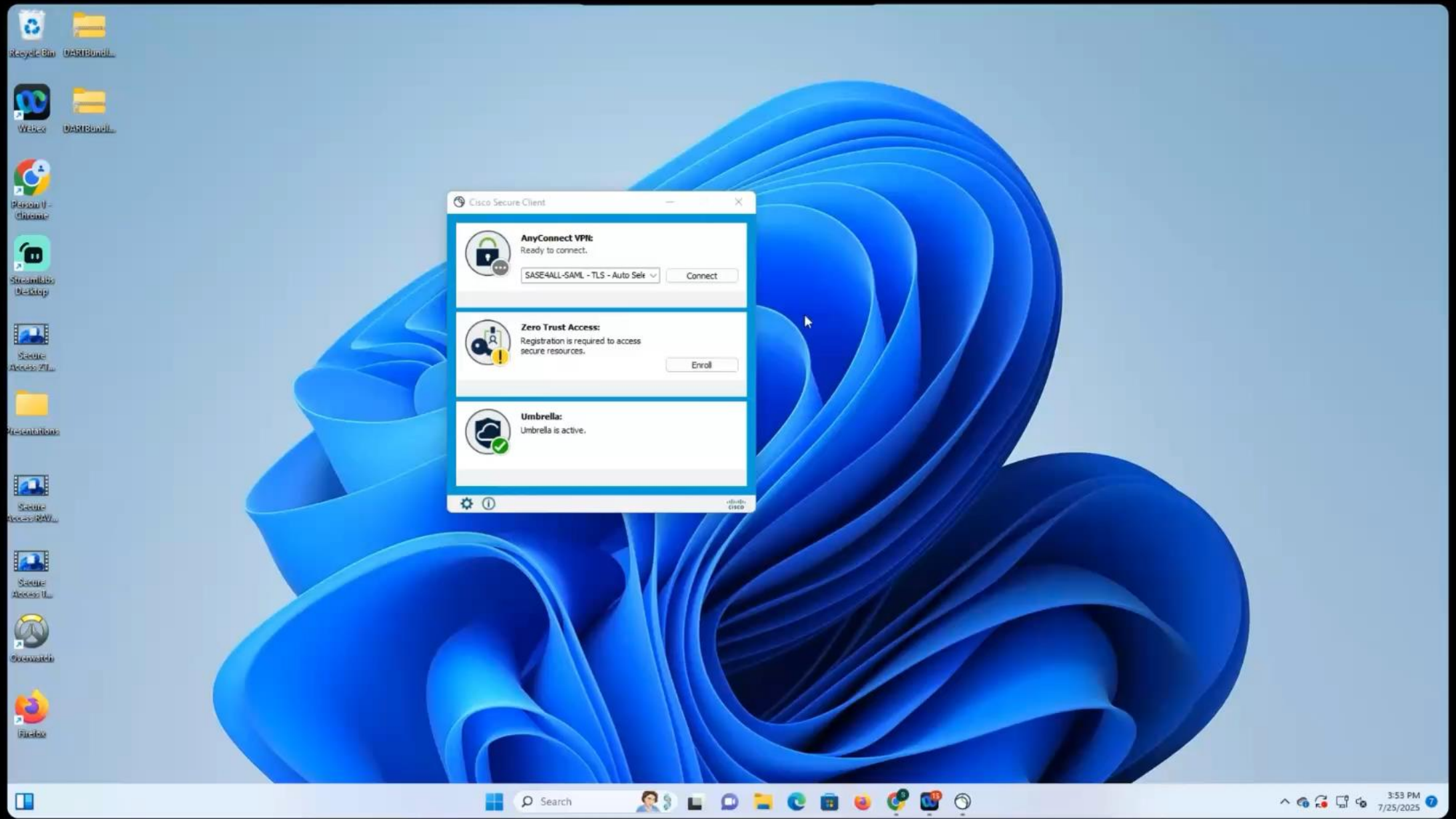


VPN



OS Native ZTA on iOS 17

ZTA connects + loads a site faster than VPN can even connect


Recycle Bin
DARTBundl...
Webex
DARTBundl...
Person 1 - Chrome
Streamlabs Desktop
Secure Access ZT...
Presentations
Secure Access ReV...
Secure Access T...
Overwatch
Firefox
Cisco Secure Client
AnyConnect VPN:
Ready to connect.
SASE4ALL-SAML - TLS - Auto Sele
Connect
Zero Trust Access:
Registration is required to access secure resources.
Enroll
Umbrella:
Umbrella is active.
Search
3:53 PM
7/25/2025

Organization
SGTDemos
Platform menu
Secure Access
Home
Experience Insights
Connect
Resources
Secure
Monitor
Admin
Platform services
Favorites
Security Devices
Shared Objects
Platform Management

End User Connectivity

End user connectivity lets you define how your organization's traffic is steered from endpoints to Secure Access or to the internet. Help

Cisco Secure Client | Manage servers

Zero Trust Access | Virtual Private Network | Internet Security

Enrollment methods

Manage

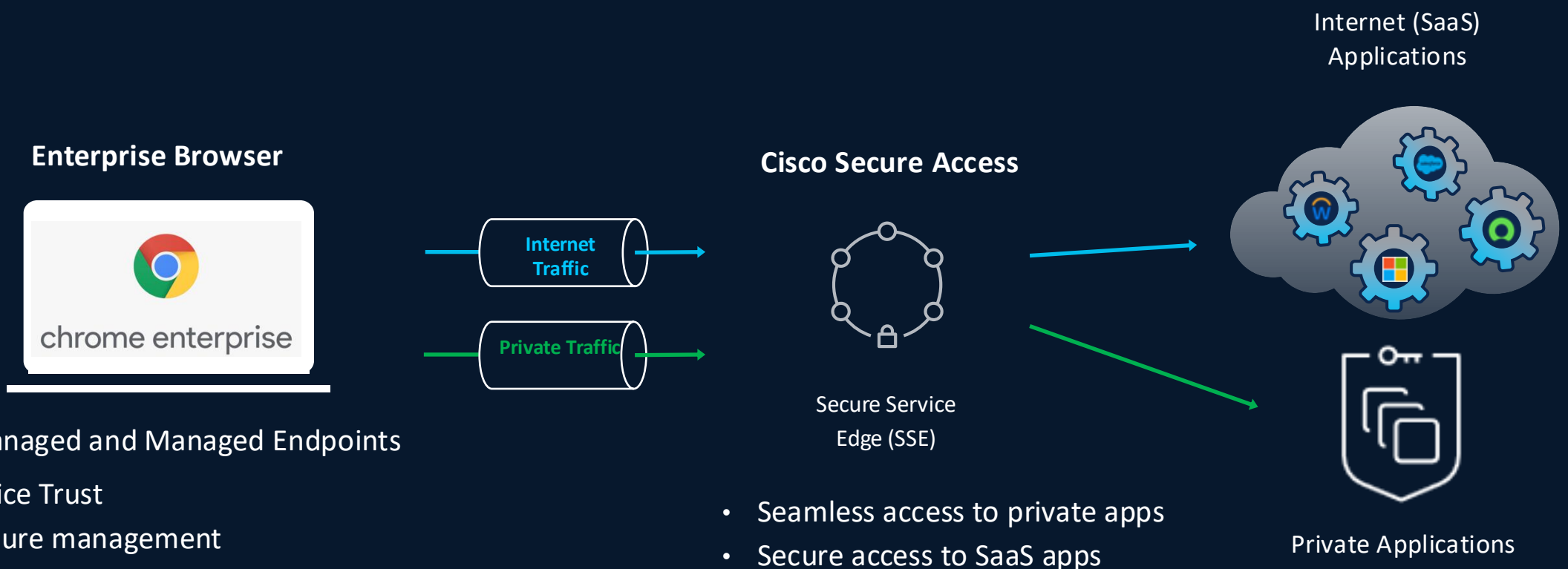
Before users can access resources using client-based Zero Trust Access, their endpoint devices must be enrolled. Manage enrollment methods for your organization here. Help

Windows and macOS devices enroll using: SSO Authentication | Certificates

Android and iOS devices enroll using SSO Authentication only.

Secure Access with Enterprise Browser

Zero Trust Access to Private Apps and Internet Apps



Unmanaged and Managed Endpoints

- Device Trust
- Posture management
- DLP
- Copy-paste controls, Block Screenshots
- Block file upload/download
- Print control
- 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
- Advanced Malware protection
- RBI

Home
Experience Insights
Connect
Resources
Secure
Monitor
Admin
Workflows

Overview

The Overview dashboard displays status, usage, and health metrics for your organization. Use this information to address security threats and monitor system usage. Help

Connectivity

Last 24 Hours

You have 1 connector groups with no associated private resources. To assign resources, navigate to Connector Groups

Network tunnel groups 28 total

- 22 Disconnected
- 1 Warning
- 5 Connected

Resource connector groups 5 total

- 1 Disconnected
- 1 Warning
- 3 Connected

Data Transfer

Last 24 Hours

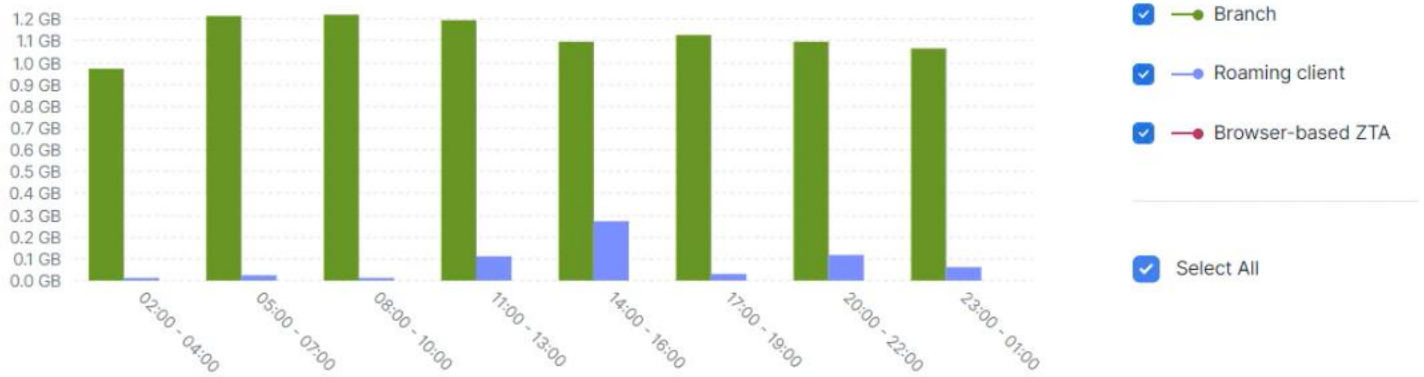
TOTAL USAGE

Usage data - delayed up to 30 min.

9.64 GB Total traffic
32.99 MB Increase (last 24 hours)

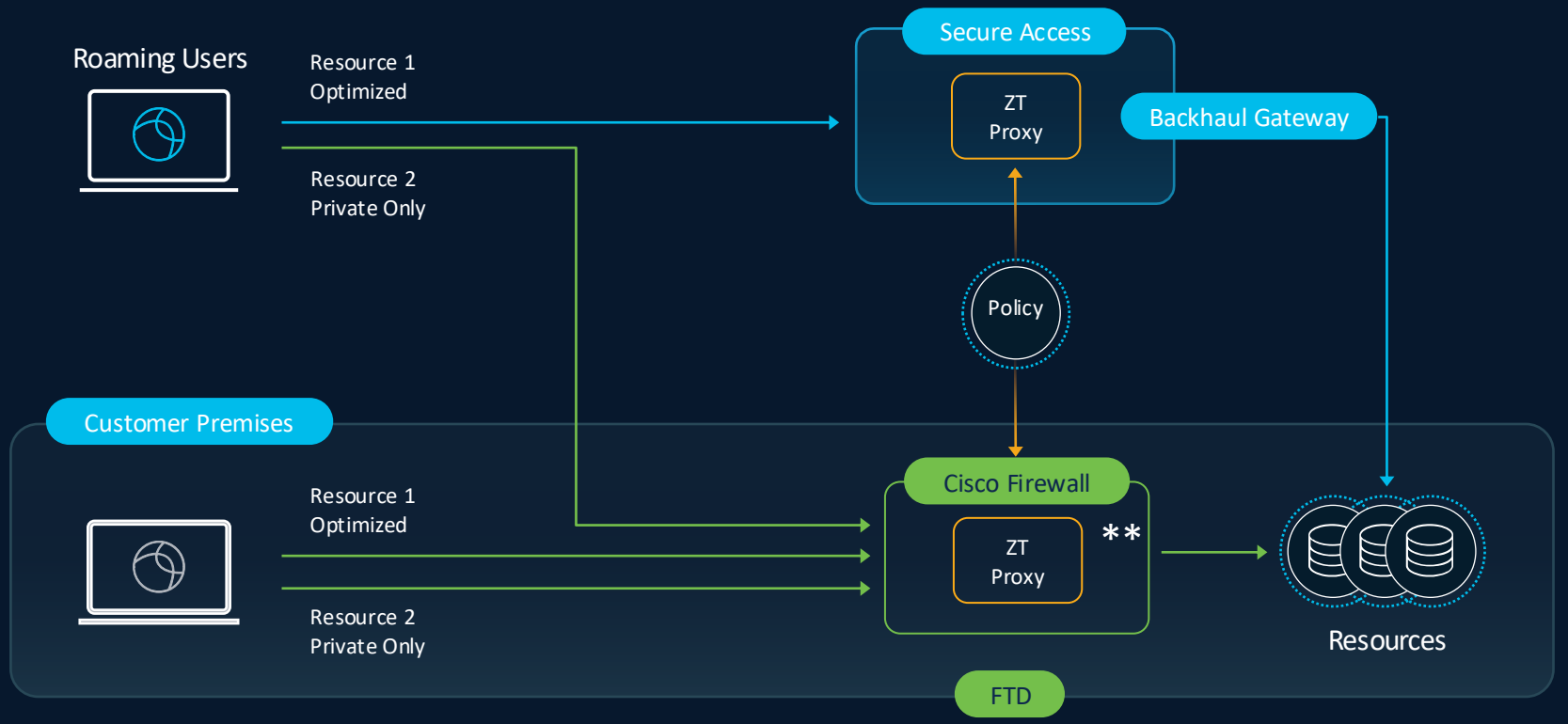
162.66 MB Received
24.46 MB Increase (last 24 hours)

9.48 GB Sent
8.53 MB Increase (last 24 hours)



Hybrid Private Access for Flexible Enforcement

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



** Roadmap: policy enforcement on 8k routers

* Capabilities are in private preview.

Organization
GSSO-GSAT
Home

Products
AI Defense
Firewall
Hypershield
Multicloud Defense
Secure Access
Secure Workload

Platform services
Favorites
Identity Intelligence
Security Devices
Shared Objects
Platform Management

Home

Set default homepage

Top Insights & Alerts

12 Active Insights

All Insights

Access Control Policy Anomalies

Data source: Test-abc | Cloud-delivered FMC

AIOps has detected 32 anomalies in Access Control policy 'Test-abc'.

28d ago — Details

Best practices and recommendations

Data source: ftdv-test6

AIOps has detected 6 needs review checks.

24d ago — Details

Best practices and recommendations

Data source: ftdv-test5

AIOps has detected 6 needs review checks.

24d ago — Details

Multicloud Defense

Multicloud Defense

Account Resources

21 VPCS/ VNets	35 Security Groups	31 Route Tables	69 Subnets
8 Instances	1 Load Balancers	0 Tags	1 Applications

Security Considerations

- 1 Applications not protected
- 20 VPCs/VNets not protected
- 0 Service VPC/VNets without Gateways

Overall Inventory

32 Total Devices

RA VPN Sessions

The Identity Layer: Cisco Identity Intelligence

Identity is the New Perimeter—and the Primary Target.

Gap

Blind Trust

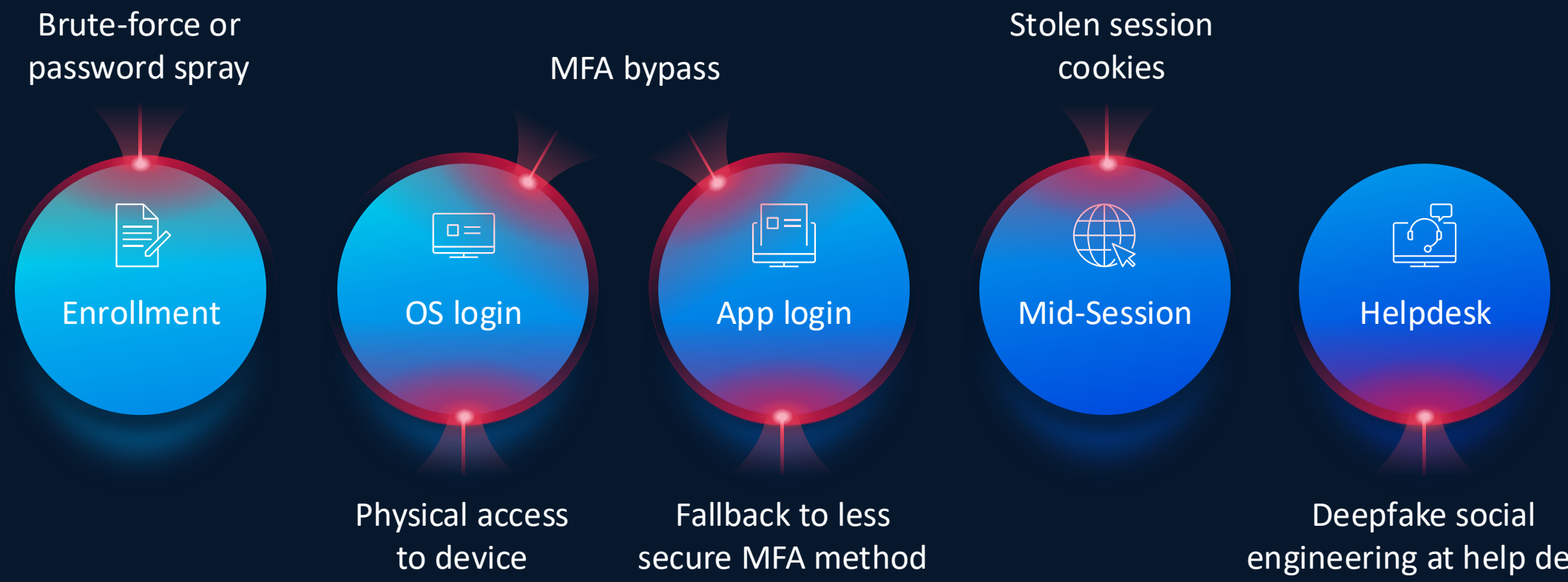
60%

of Talos IR cases involved identity components

44%

of identity attacks specifically targeted Active Directory

Attackers expect you to have MFA



Duo IAM

Security-First Identity

End to end phishing resistance

Unified Identity intelligence

World-class user experience

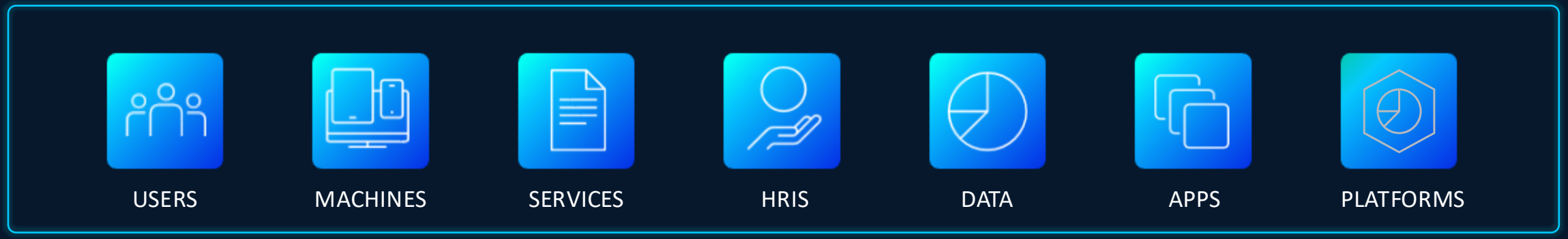
Run standalone as your primary IdP, directory and SSO.

Integrate with your existing IAM as an identity broker.

Deploy as alternate directory for your third parties.

FIDO2, Hardware Tokens

Cisco Identity Intelligence



SailPoint
Dragos
Crowdstrike
Salesforce
Cisco ISE
Okta
PingIdentity
Auth0
Microsoft
Google
Cyberark
Amazon


Cisco Identity Intelligence
USERS
MACHINES
SERVICES
HRIS
DATA
APPS
PLATFORMS
RELATIONSHIPS
LOGS
SESSIONS
LOCATION
FACTORS
EMAILS
UID
ROLE
CONNECTED
IDENTITIES
IOT
PASSKEYS
BROWSERS
UNMANAGED
USER DEVICES
MDM
INFRASTRUCTURE
PERMISSIONS
GROUPS
SUBSET
ACCESSED THROUGH
workday
okta
ON PREM
SaaS
aws
WORKLOADS

The Engine: Identity Intelligence.

Trust is not a binary state granted at login.
It is a continuous, risk-aware assessment.

cisco

Organization
Demo Organization

Platform menu

Secure Access

Home
Experience Insights
Connect
Resources
Secure
Monitor
Admin
Workflows

Platform services

Favorites
Identity Intelligence
Platform Management

Get started with Cisco Secure Access

Choose how you want to start protecting your organization's users and then follow the tasks listed here to get started. Help

1/3 steps complete.

1 **Configure infrastructure** — Not Started

Connect your organization's infrastructure to Secure Access.

Secure resources and access — Done

Define your private resources, endpoint posture profiles, IPS, security profiles and access policies.

3 **Configure end user connectivity** — Not Started

Configure DNS Servers, Zero Trust Access, virtual private networks and view instructions for packaging the Cisco Secure client.

Give feedback

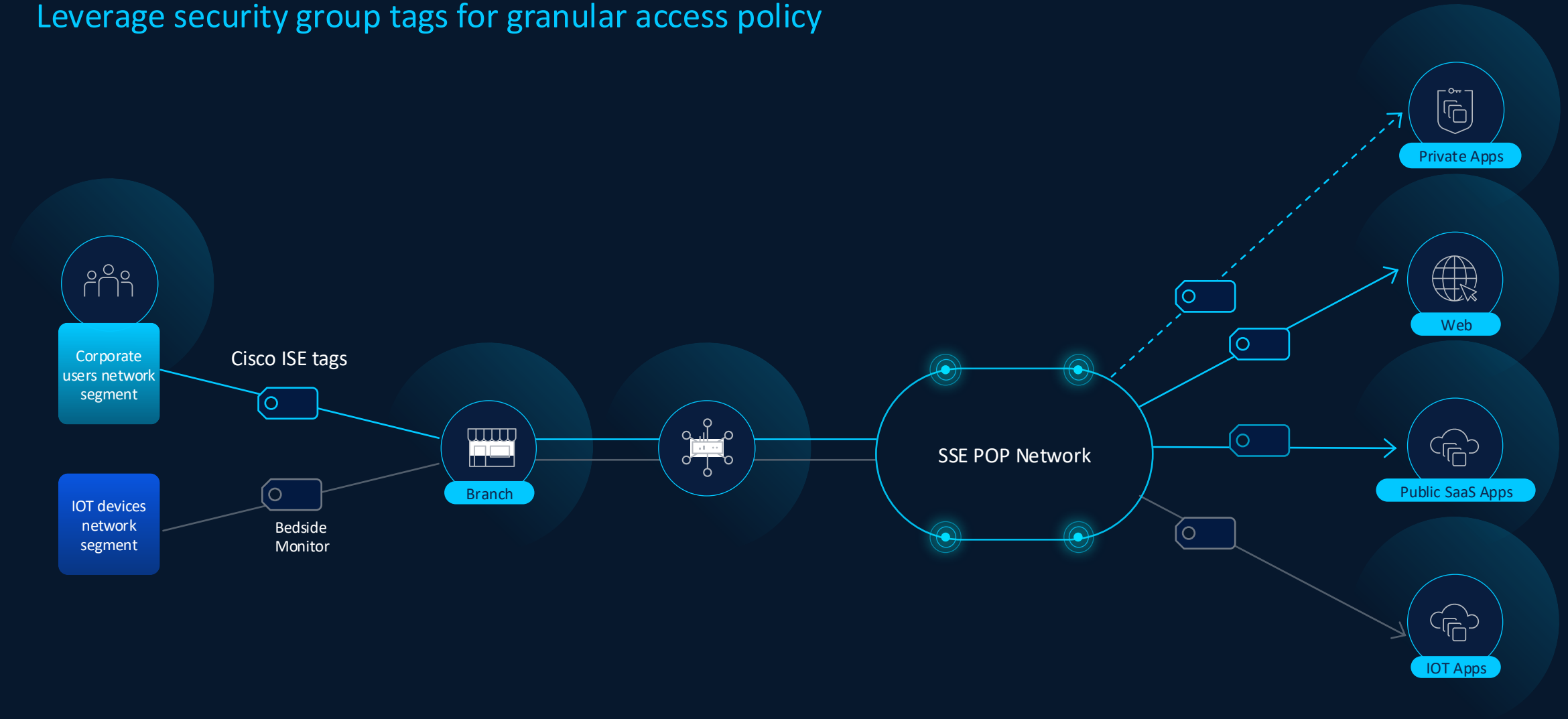
Overview

The Overview dashboard displays status, usage, and health metrics for your organization. Use this information to address security threats and monitor system usage. Help

Things are people too.

Enforce zero trust using identity context

Leverage security group tags for granular access policy

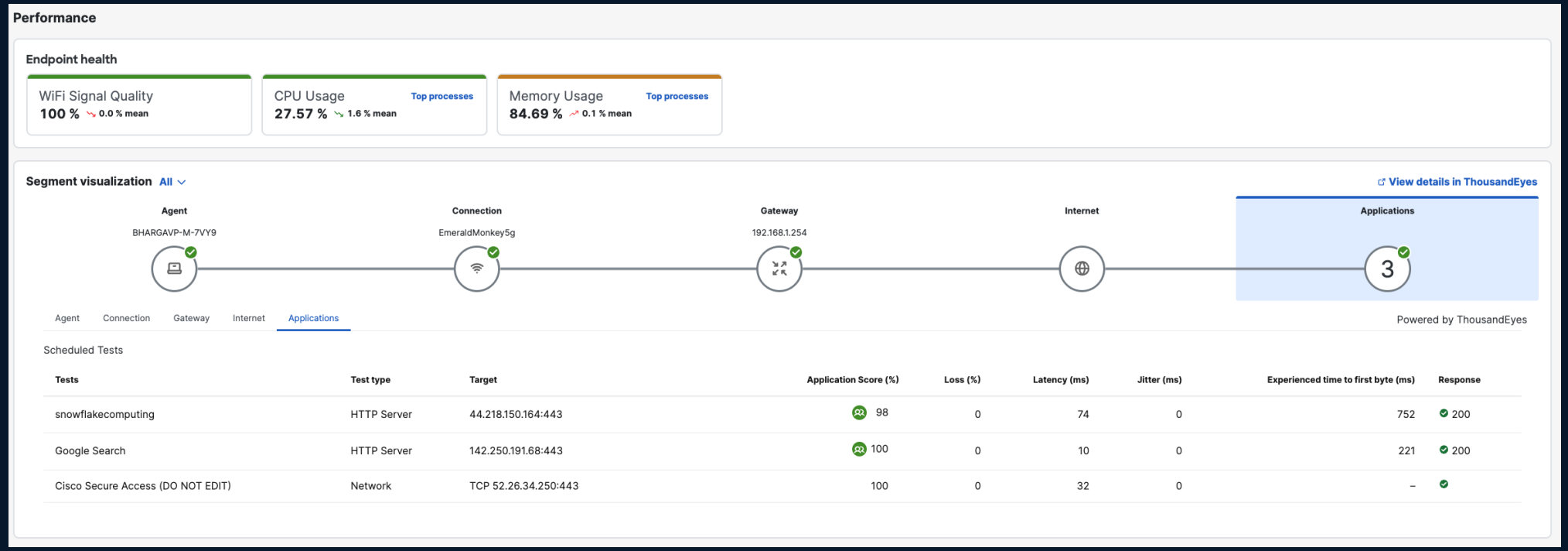


----- = Future

DEM: Actionable Experience Insights

Experience Insights

User experience monitoring for applications and users



Monitor health and performance as users access applications and resources

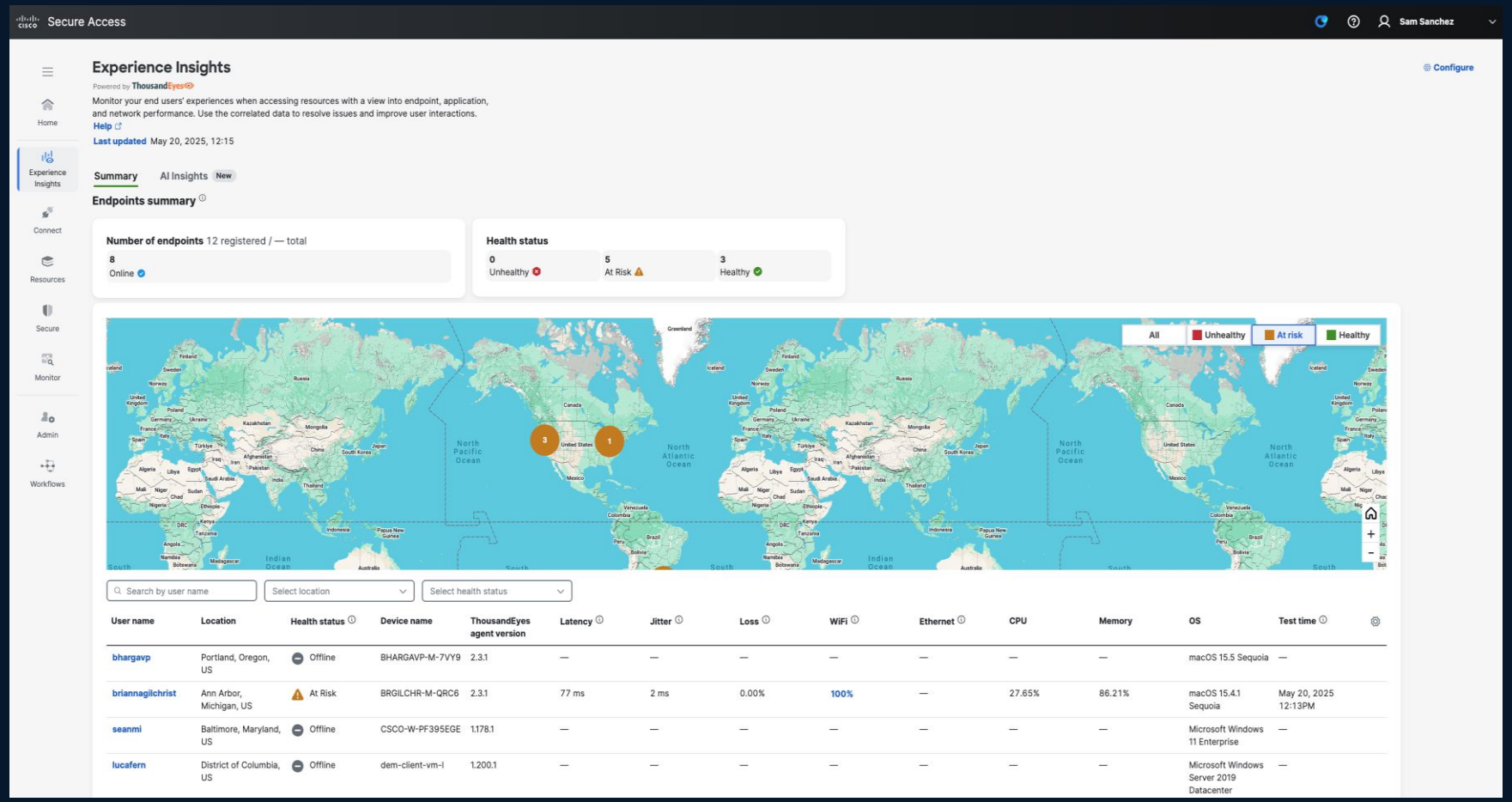
Optimize user productivity by automatically, providing details on the user's experience, enabling faster issue detection and resolution

Monitoring examples:

- Endpoint performance – CPU, memory, Wi-Fi
- Network performance – latency, jitter, loss
- Top 20 SaaS applications performance
- App agnostic synthetic monitoring – Collab, private, public
- User specific ZTA security events
- AI Insights with Troubleshooting Assistant

Global Workforce Visibility

Gain a complete view of user experience, for both remote and hybrid workers



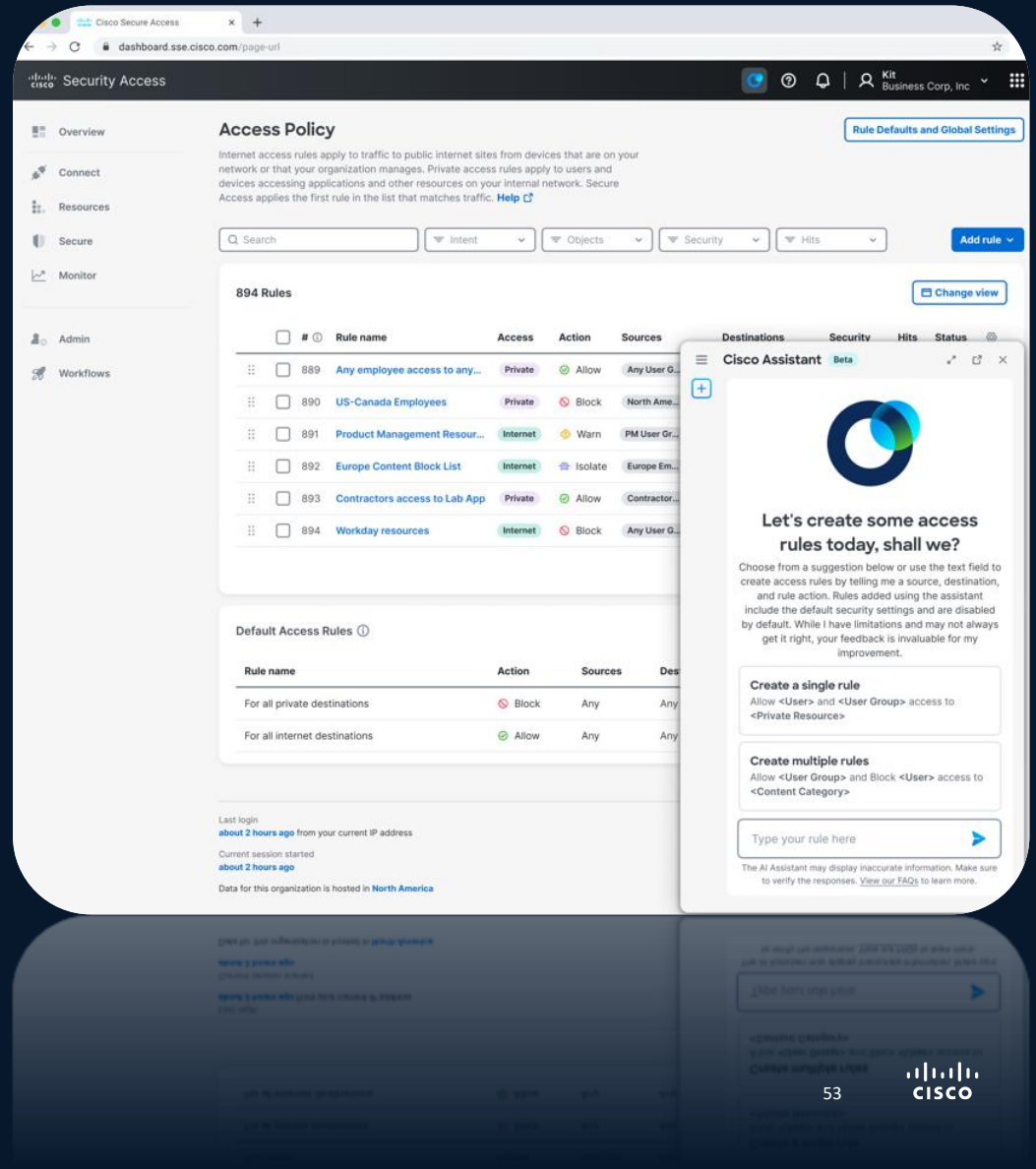
Simplified Experience

- Monitor all endpoints within a single SSE dashboard
- Lightweight ThousandEyes Endpoint Agent included with CSC at no extra cost
- **Continuous monitoring for** efficient troubleshooting

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
- Retains the context of up to five recent prompts



Better Efficacy. Better Experience. Better Economics.

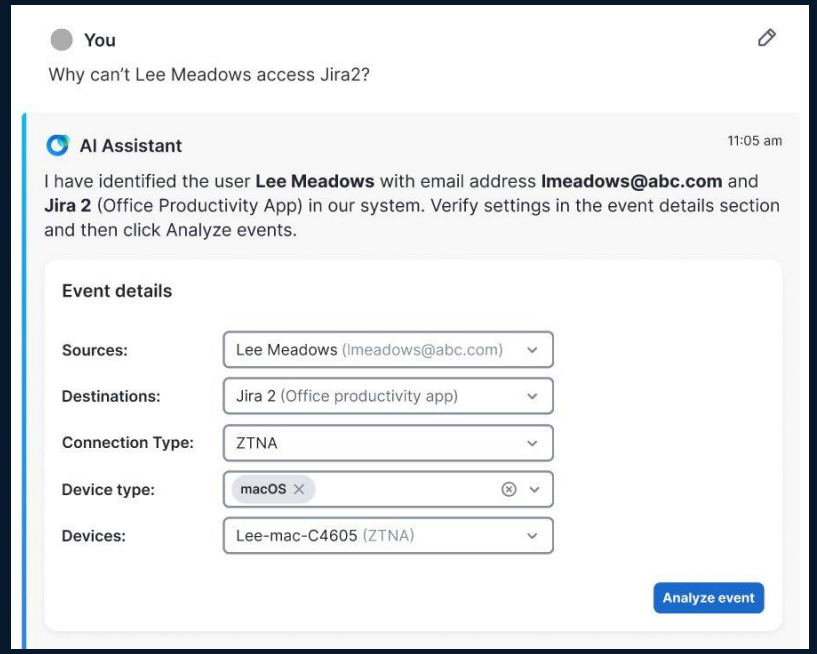
Troubleshooting Assistant

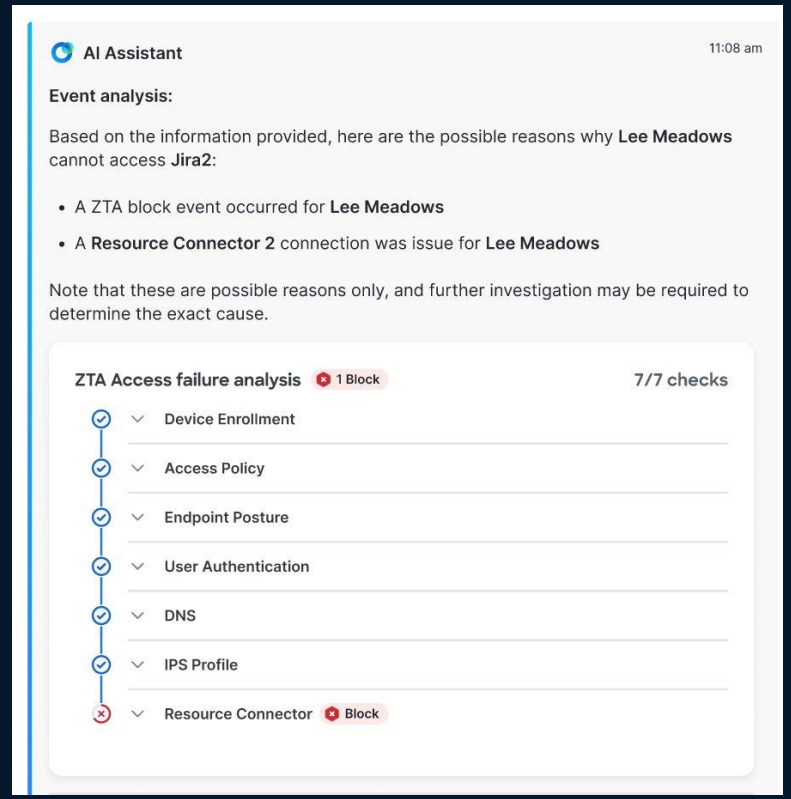
Automate troubleshooting Secure Access

- Private App Access Issue
- Multi Agent Orchestration
- Faster Time to Resolution

Prompts:

"Why can't Lee Meadows access Jira"



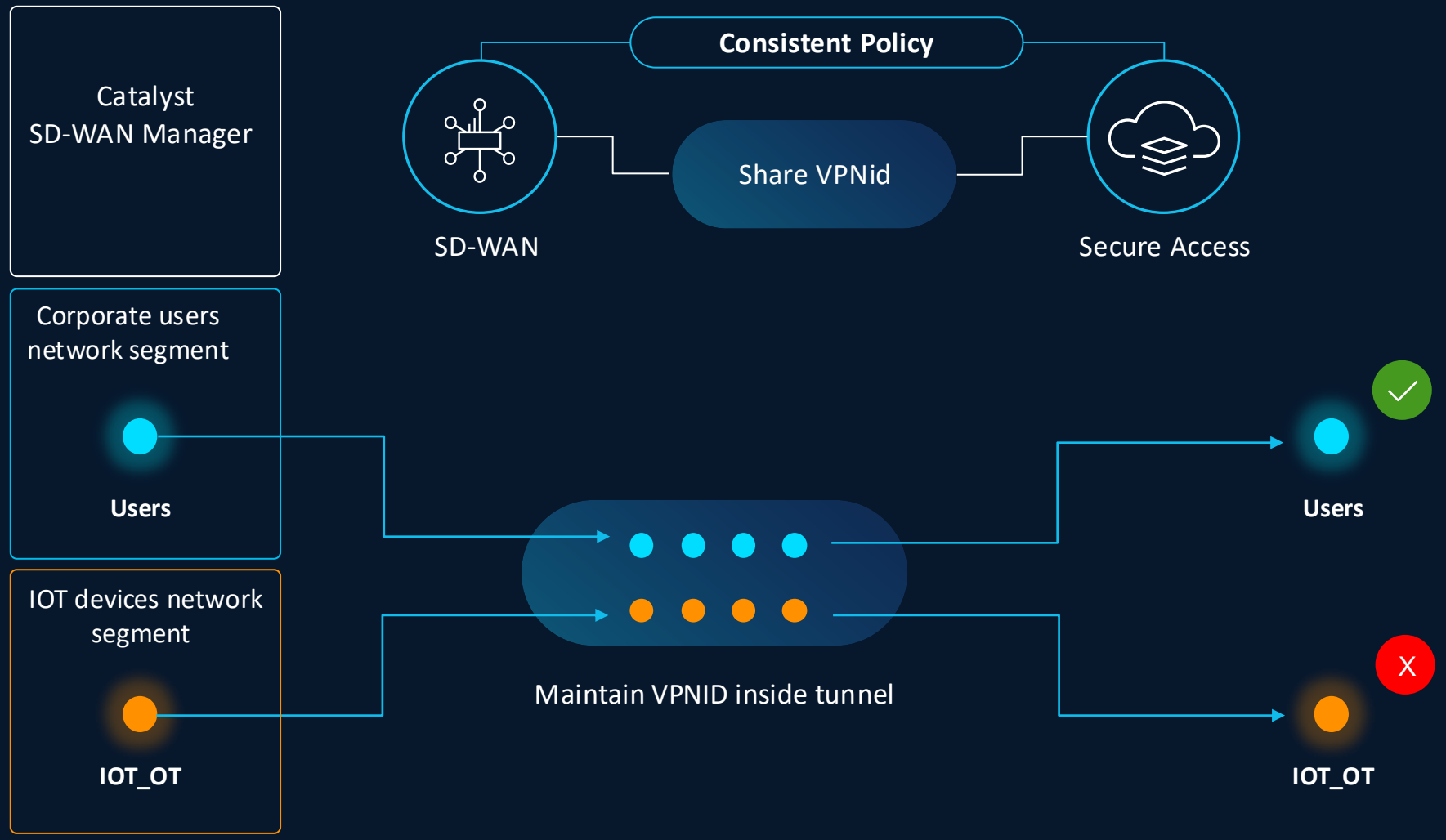


Integrations to the Wired World

Catalyst SD-WAN

VPNid support for consistent segmentation

- VPNiD Based policy across both SDWAN & Secure Access
- Maintain segmentation in branch & in the cloud



Identity Services Engine (ISE)

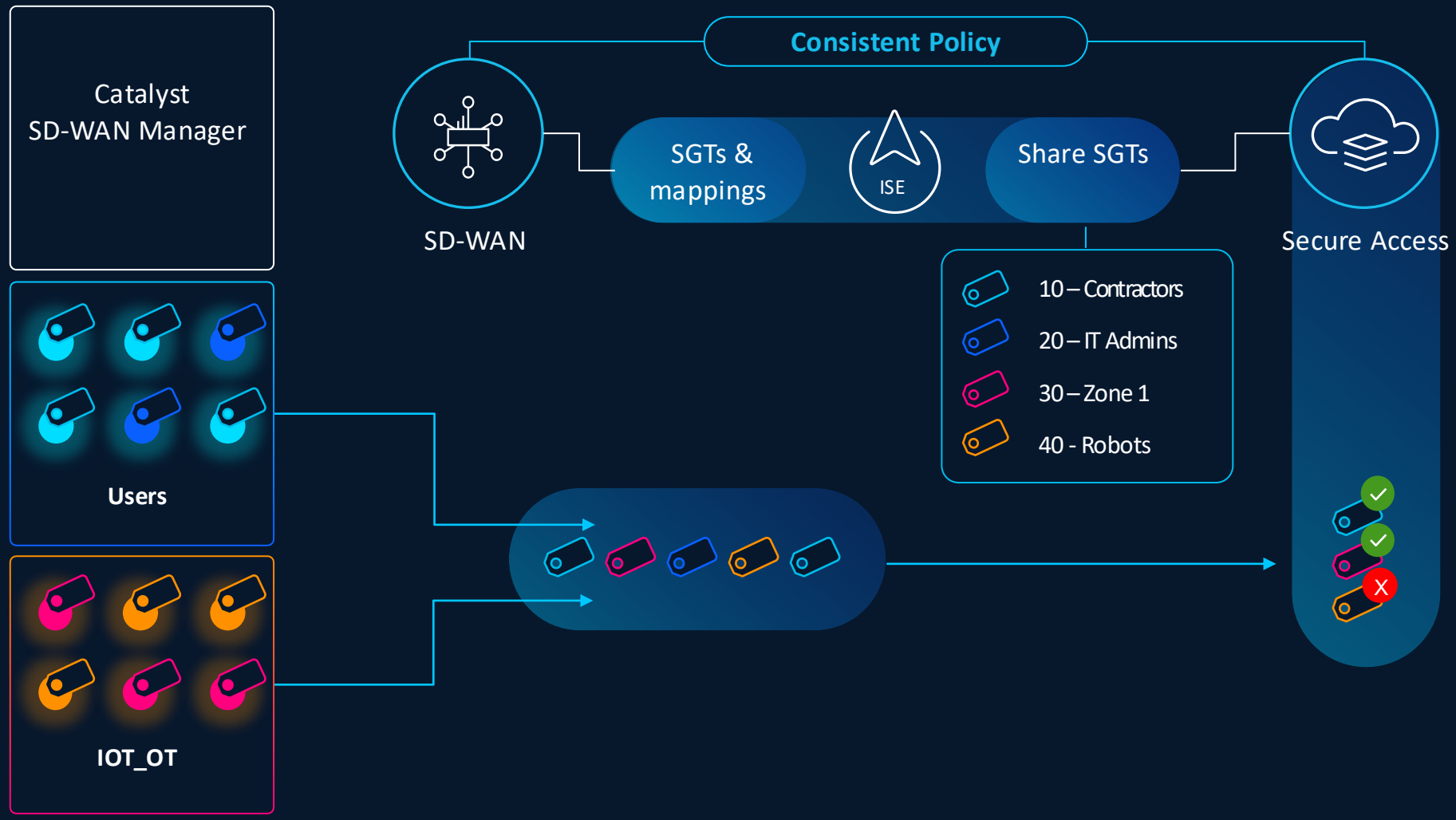
Leverage SGTs for granular access control

SGT Based Policy across network & Cloud

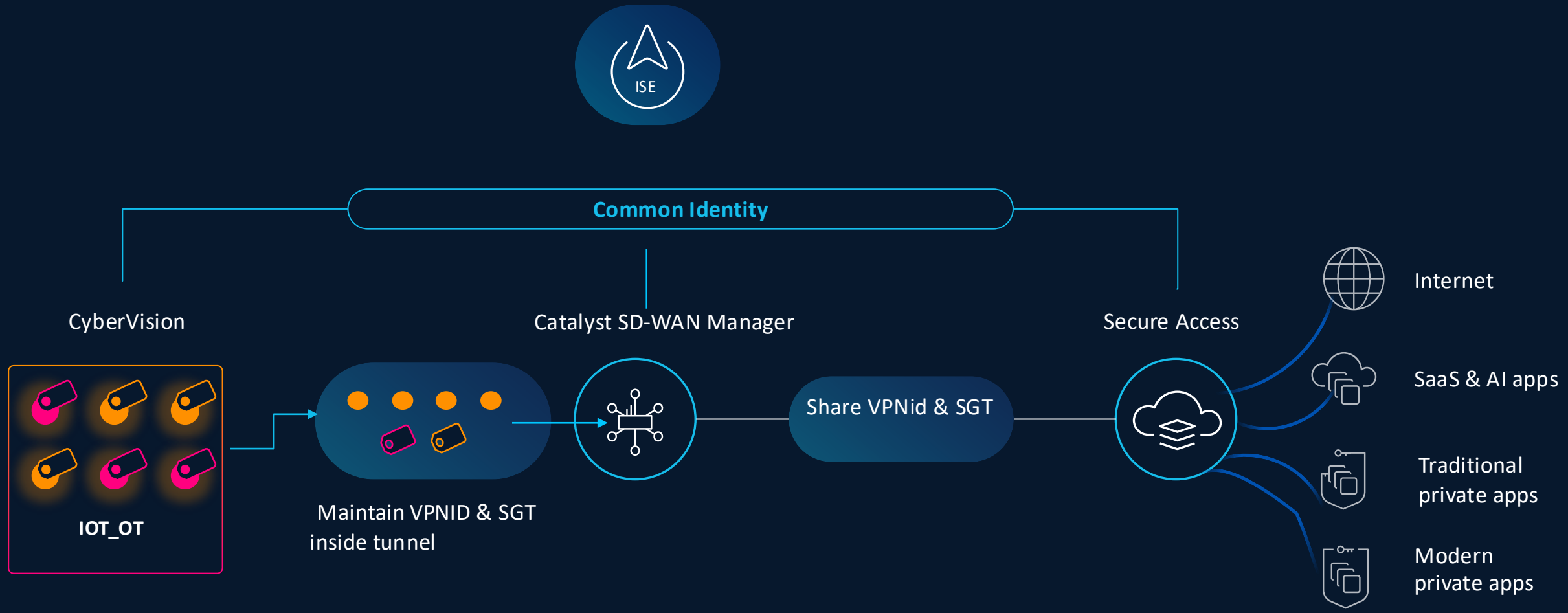
Maintain micro segmentation through Secure Access

Uniquely identify devices and traffic based on context from ISE

Apply policy to SGT Based identity



Demo



HMI1 - TrustSec Segmentation Scenario - HMI1 - Remote Desktop Connection

StartHMI - FactoryTalk View SE Client - [MainDisplay - /SecDemo_Hannover//]

Disable Timer

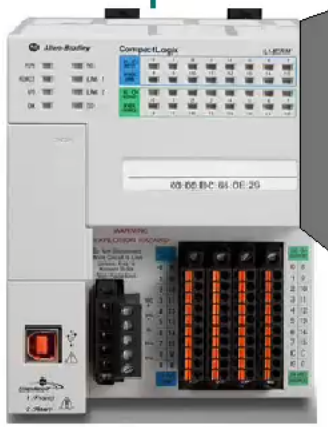
Reset Timer

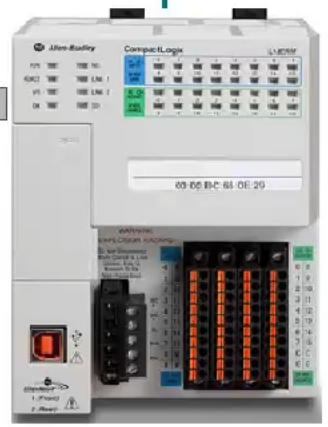
Load Timer from Line

Data IN Cell Controller FROM Line

17 Days 16 Hours 27 Minutes 46 Seconds

CIP Write





Enable Remote Access

Cell 1 Controller

17 Days 16 Hours 58 Minutes 4 Seconds

Line Controller - Cell 2

17 Days 16 Hours 27 Minutes 46 Seconds

Configuration

Type here to search

10:22 AM
8/22/2025

Cisco Eases Your Journey to a Future-Proof Workplace

Traditional Networking

Network level access – cannot control
at app level

SD-WAN*

Protect data and traffic while optimizing user experience, performance & resources

Predictive Path Recommendations

Optimize routing for all clouds, all users, and all apps

SSE*

Consolidate security services and add advanced threat protection everywhere

Seamless transition from VPN to ZTNA

Support for legacy and modern apps

Universal ZTNA

Enable every user and device to securely connect with least privilege access to any app—anywhere.

Hybrid private access

Local enforcement for branch users (no hairpinning)

Identity Edge

Smart authentication for users and devices

*when combined this is known as SASE architecture

Resource Links

- **Cisco Secure Access Youtube Channel**
  https://www.youtube.com/playlist?list=PLHUFHAfReXtxvPs9UJHk9NqI6TWosoQWU

- **Cisco SE Jason Maynard's CSA Youtube Playlist**
  https://www.youtube.com/playlist?list=PLyf18hdY22EROu0KP1v9n9VffD9CuiauD

- **Umbrella & Secure Access Public Space**
  webexteams://im?space=cbd8f630-aeb5-11ec-a33e-6dda58872fda

- **Cisco Secure Access Community on Cisco.com**
  https://community.cisco.com/t5/secure-access/ct-p/secure-access

- **Latest Cisco Secure Access Announcments**
  https://community.cisco.com/t5/secure-access-announcements/tkb-p/secure-access-announcements

Thank you

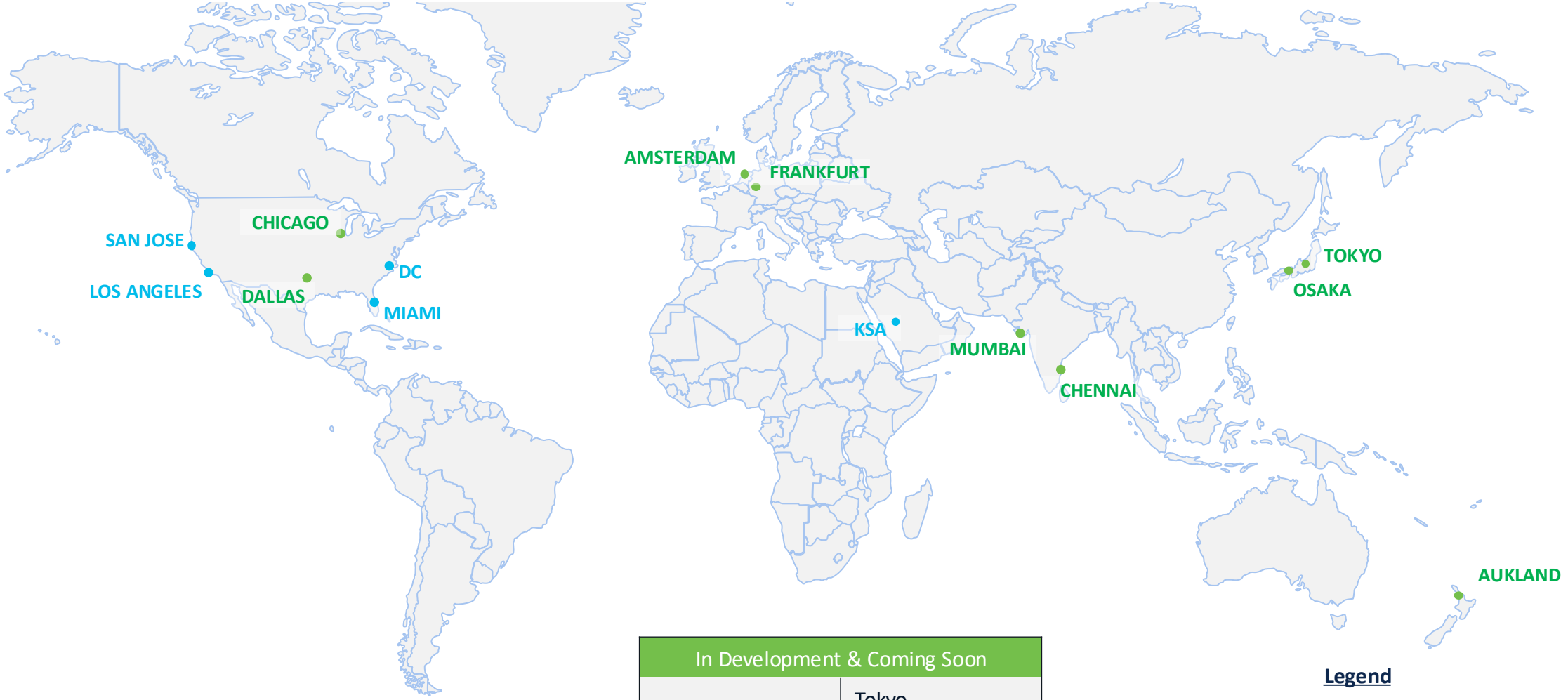
Secure Access Regions – AWS coverage

Coming Soon
Spain

Legend

- Available
- Coming Soon
- Subject to Demand

Secure Access Regions – DCv2 (Physical Edge DC)



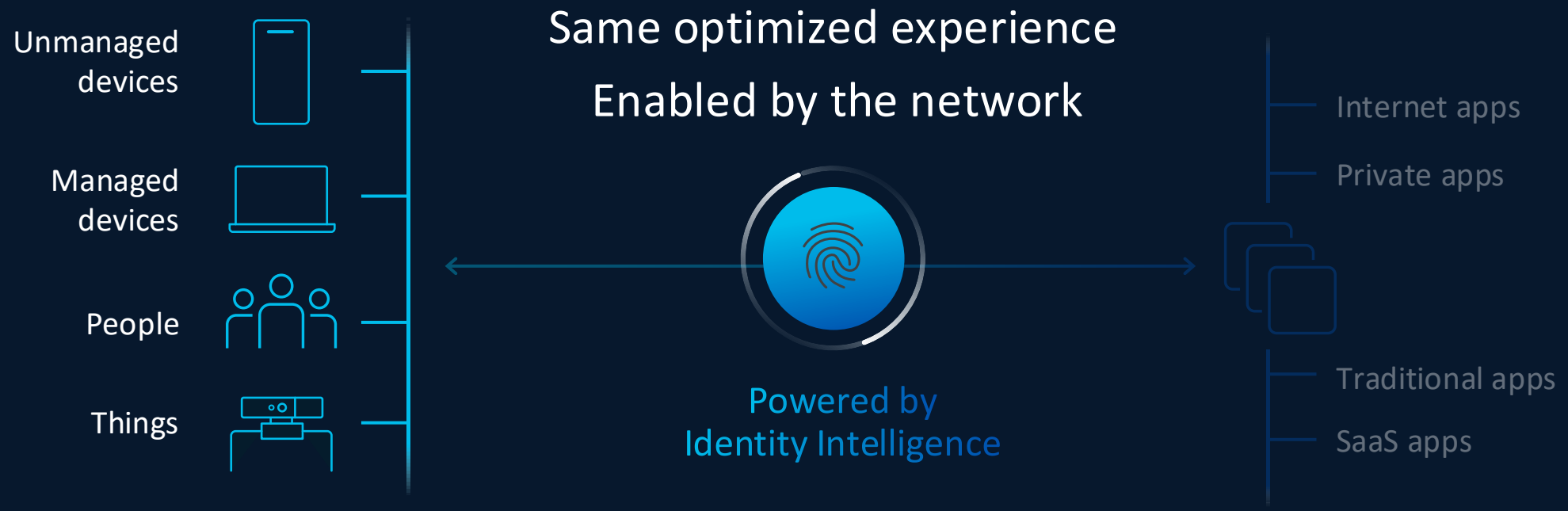
In Development & Coming Soon	
Amsterdam Frankfurt Chicago Dallas	Tokyo Osaka Mumbai Chennai Aukland

Legend

- Available
- In Development

Backup Slides

Universal ZTNA from Cisco



Remote

Remote | Campus | Branch | Airplane | Oil rig | Stadium | Field | •••

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

cisco

Zero Trust Access module – socket intercept

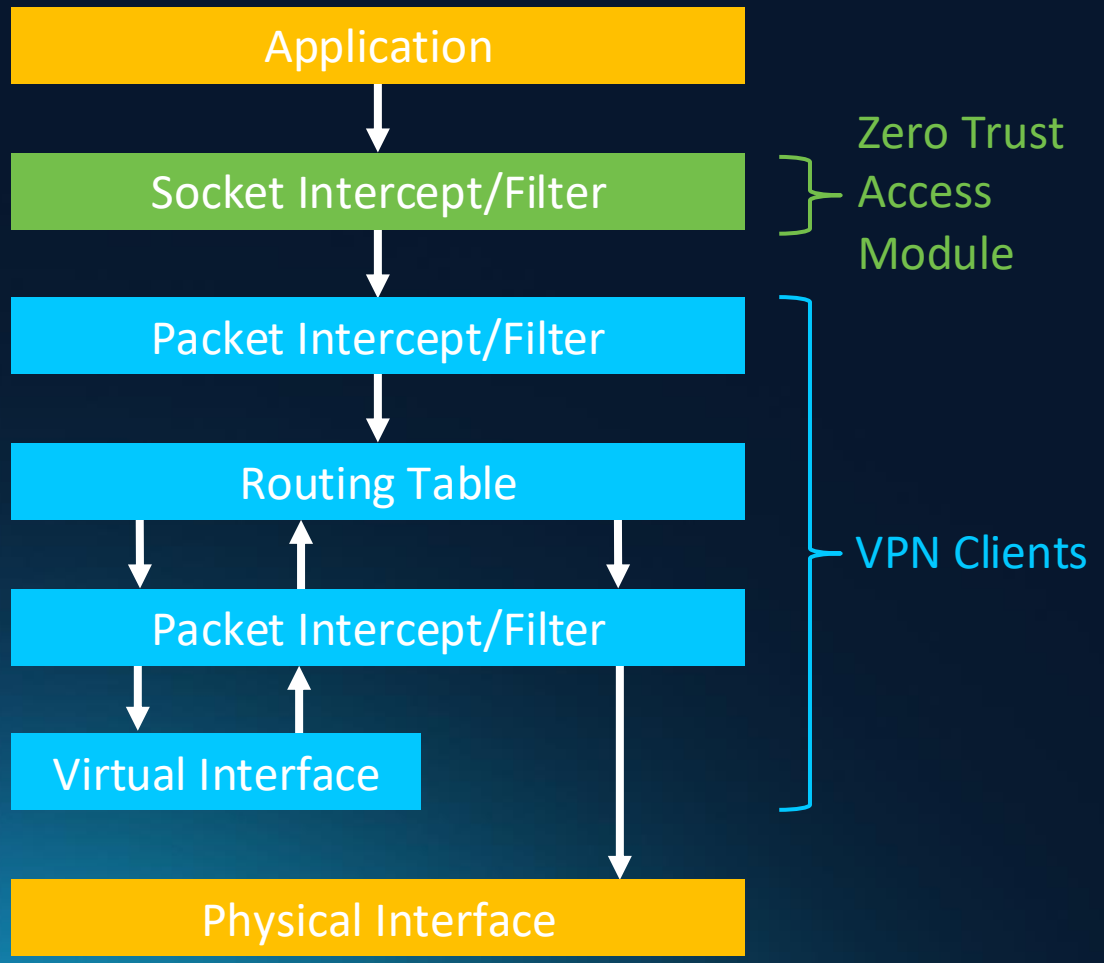
Why use socket intercept?

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

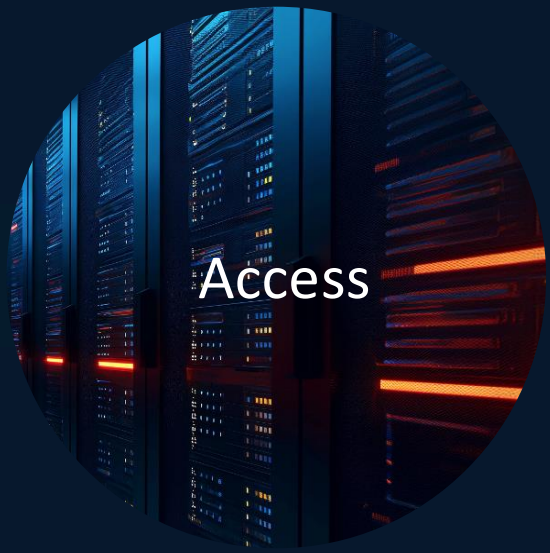
Interoperability with Cisco and non-Cisco VPNs



Identity Intelligence

Continuously assess you are who you say you are

BLIN RUST



Works with existing IDPs

cisco

Cisco Duo IAM

Cisco Secure Access

Cisco XDR

User Trust Level

TRUSTED

NEUTRAL

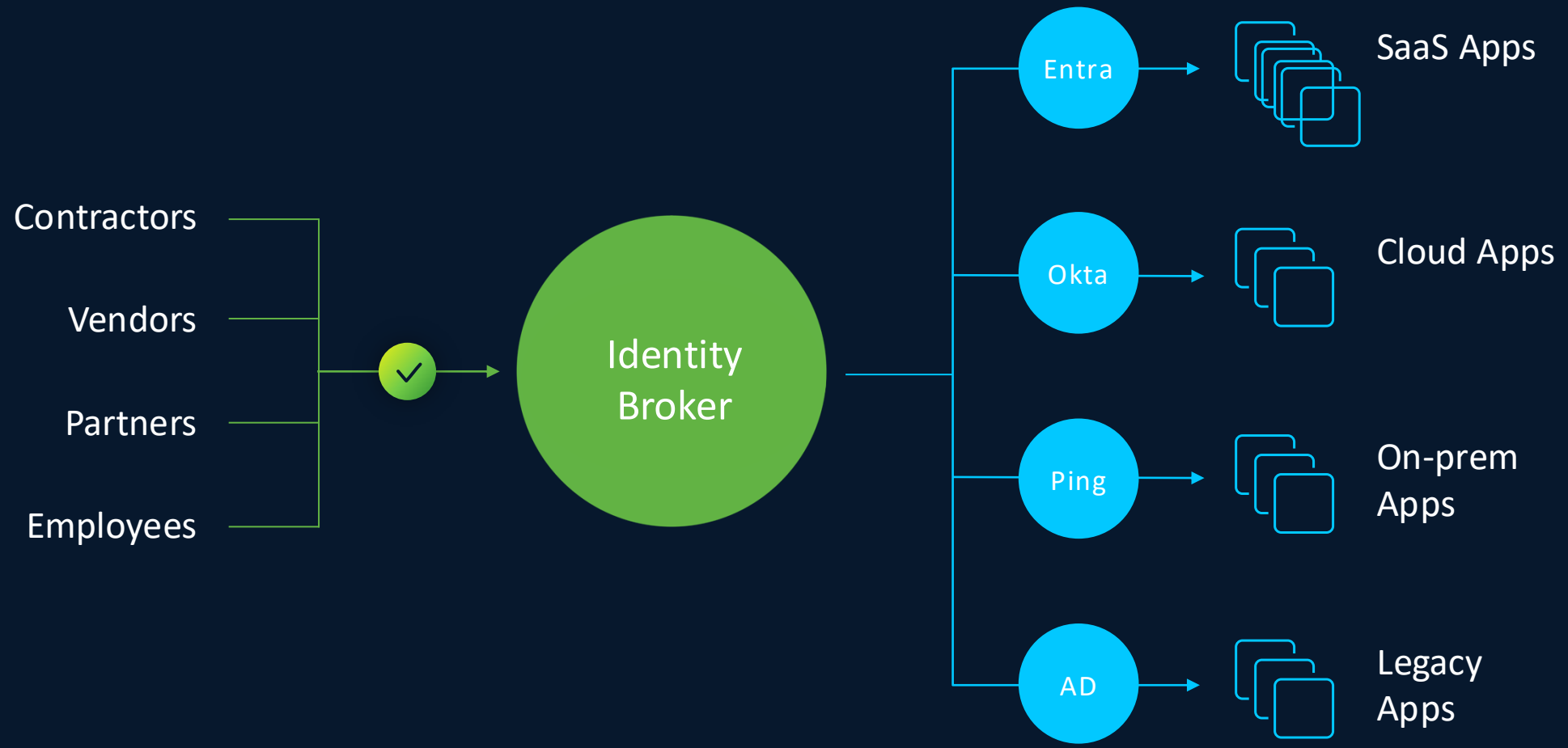
UNTRUSTED

* Capabilities are in private preview.

Standalone IAM when required

Identity broker for existing IAM

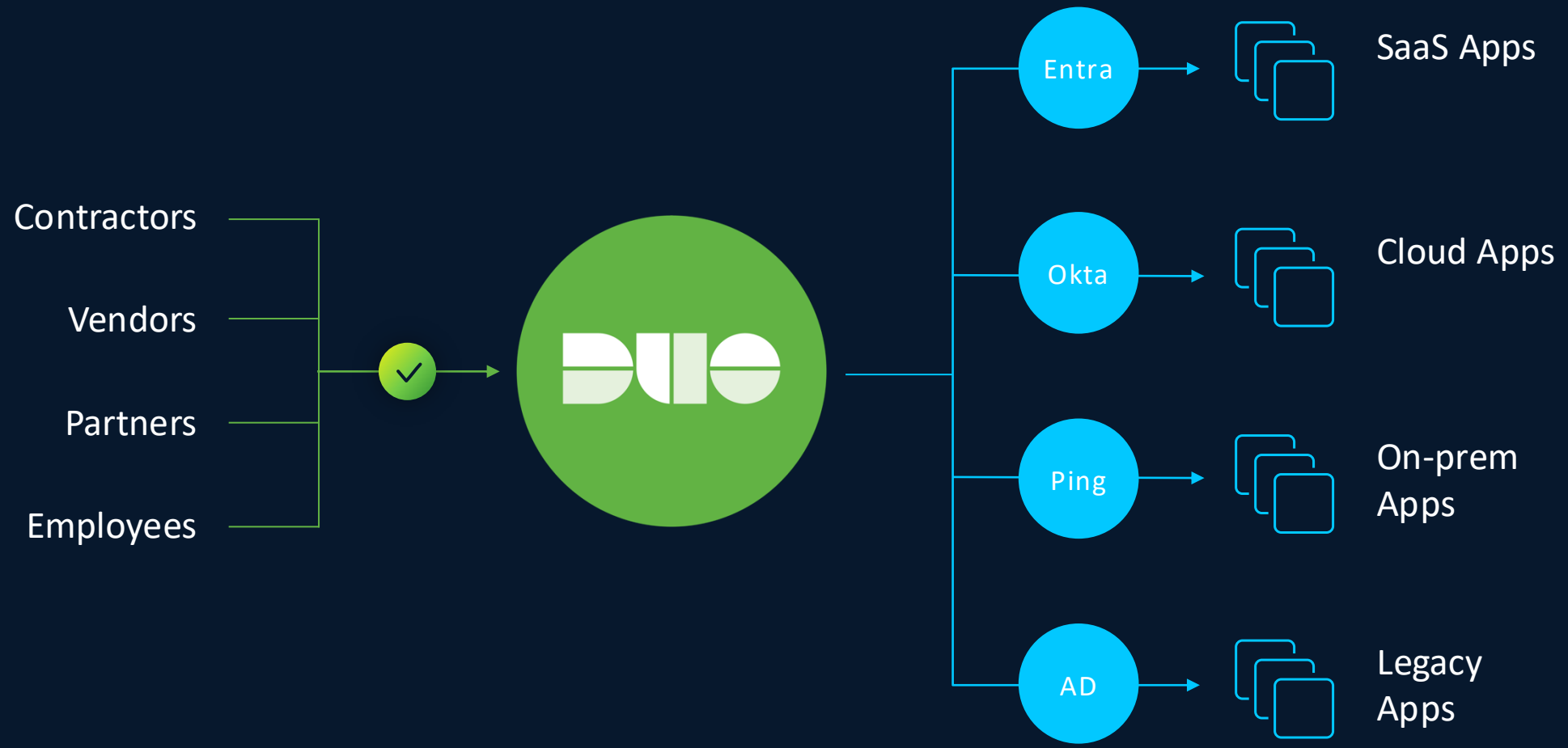
Alternate directory for third-party users



Standalone IAM when required

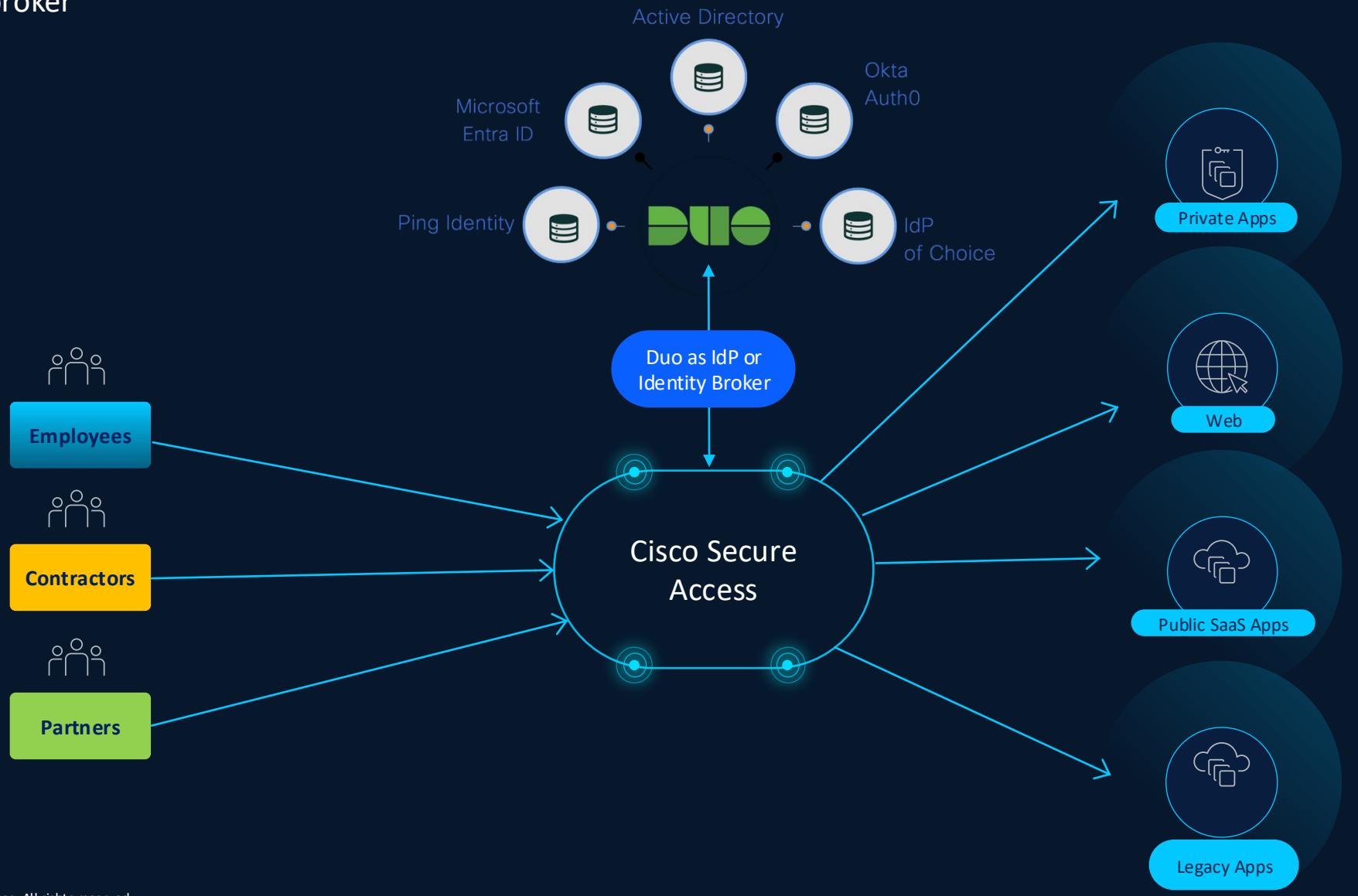
Identity broker for existing IAM

Alternate directory for third-party users



Security-First Identity

Duo as identity broker



End-to-end phishing resistance

FIDO2, Hardware Tokens

End-to-end phishing resistance

Increasing network and security convergence

Context Sharing over SD-WAN Demo

Universal Context Awareness from Network to Cloud

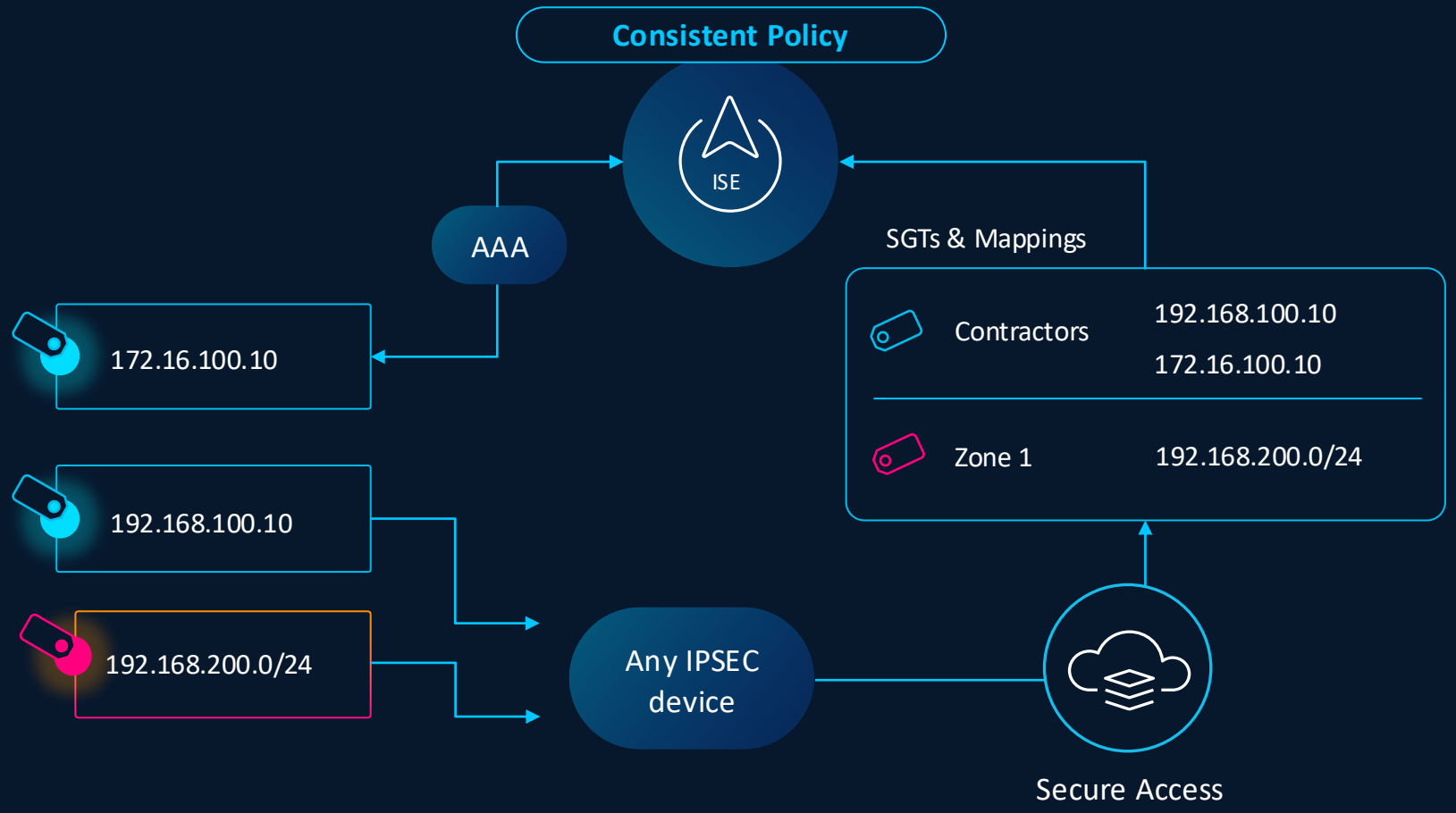
Coming Soon

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



Universal Context Sharing Demo

Home
Connect
Resources
Secure
Monitor
Admin
Workflows

Access Policy

Internet access rules apply to traffic to public internet sites from devices that are on your network or that your organization manages. Private access rules apply to users and devices accessing applications and other resources on your internal network. Secure Access applies the first rule in the list that matches traffic. Help

Rule Defaults and Global Settings

Search by rule name | Intent | Objects | Settings

Add Rule

13 Rules

Customize view

	#	Rule name	Access	Action	Sources	Destinations	Security	Hits	Status
	1	AllowTunnelToInternet	Internet	Allow	testLogicalA... +1	Any		-	
	2	AllowSGTtoAnyInternet	Internet	Allow	Any Security...	Any		-	
	3	AllowAnySGTtoAnyprivate	Private	Allow	Any Security...	Any		-	
	4	AllowSGT8ToSGT9	Private	Allow	SGT-8	SGT-9	-	-	
	5	AllowSGT9TOSGT8	Private	Allow	SGT-9	SGT-8	-	-	
	6	allowTun1ToTun2	Private	Allow	testLogicalA... +1	1 IP Address/CIDR AND 1 Services +3	-	-	
	7	TunnelAllow8888	Internet	Allow	testLogicalA... +1	1 IP Address/CIDR AND 1 Services		-	
	8	TunnelBlock8844	Internet	Block	testLogicalA... +1	1 IP Address/CIDR AND 1 Services		-	
	9	AllowSGT2ToSGT1	Private	Allow	SGT-2	SGT-1	-	-	
	10	AllowSGT2SGT	Private	Allow	SGT-1	SGT-2	-	-	
	11	DenyPing8844	Internet	Allow	SGT-5	Any		-	
	12	AllowSGT6toAny	Private	Allow	SGT-6	Any		-	