CISCO Engage | Tech Day

Universal ZTNA from Cisco

Wes Noonan, SSCO Solutions Engineer

Wednesday, October 15, 2025

“To secure ourselves against defeat lies in our own hands, but the opportunity of defeating the enemy is provided by the enemy himself.”

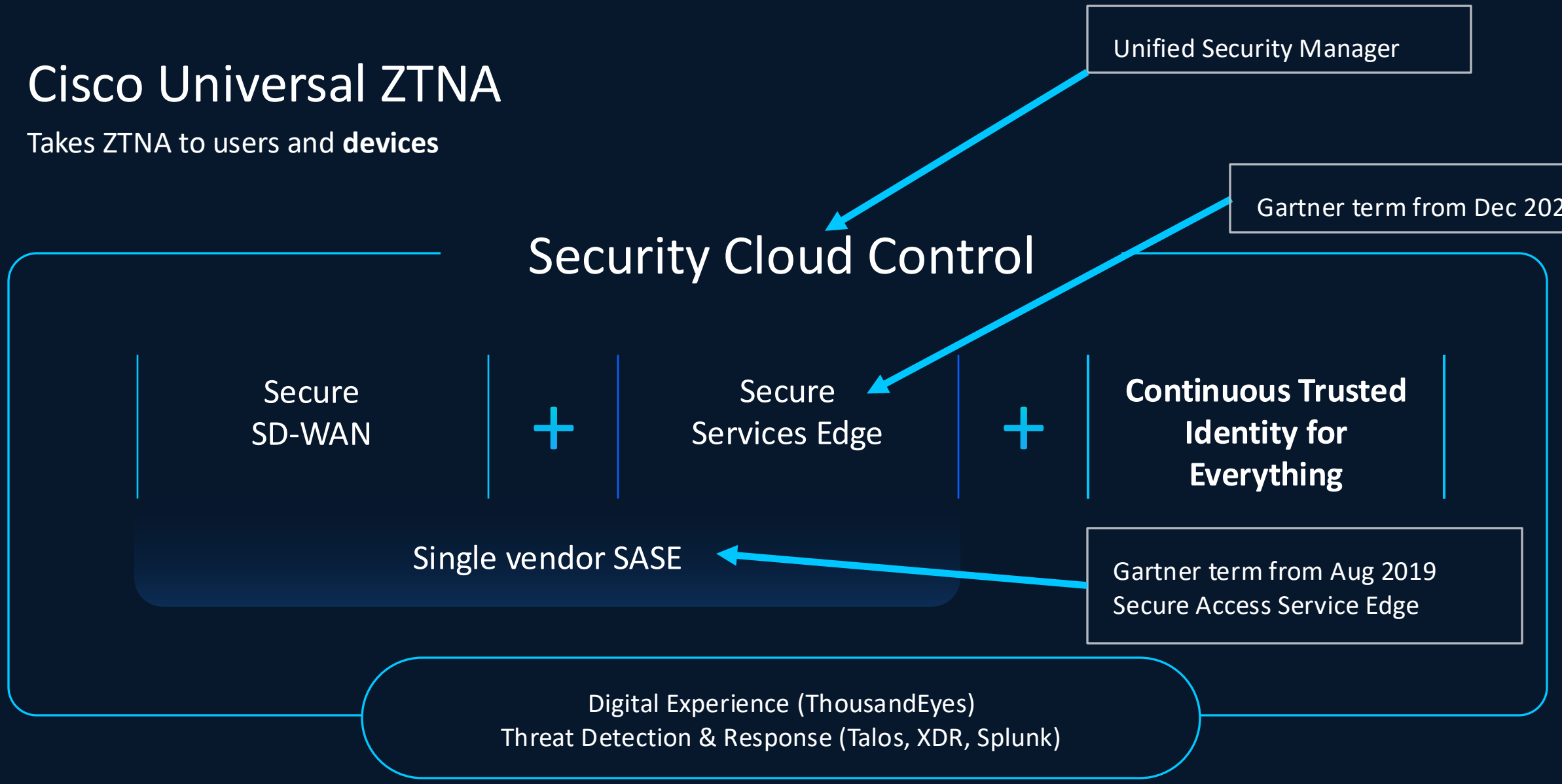
Sun Tzu

How does the industry define Universal ZTNA?

Universal Zero Trust ~~Network~~ Access
applies zero-trust principles uniformly to
all users, devices, and things for consistent,
risk based least-privilege access everywhere.

Cisco Universal ZTNA

Takes ZTNA to users and **devices**



Cisco Universal ZTNA

Every device, person, thing, everywhere

Zero downtime:
Experience and Policy Assurance

Zero impostors:
Identity Trust

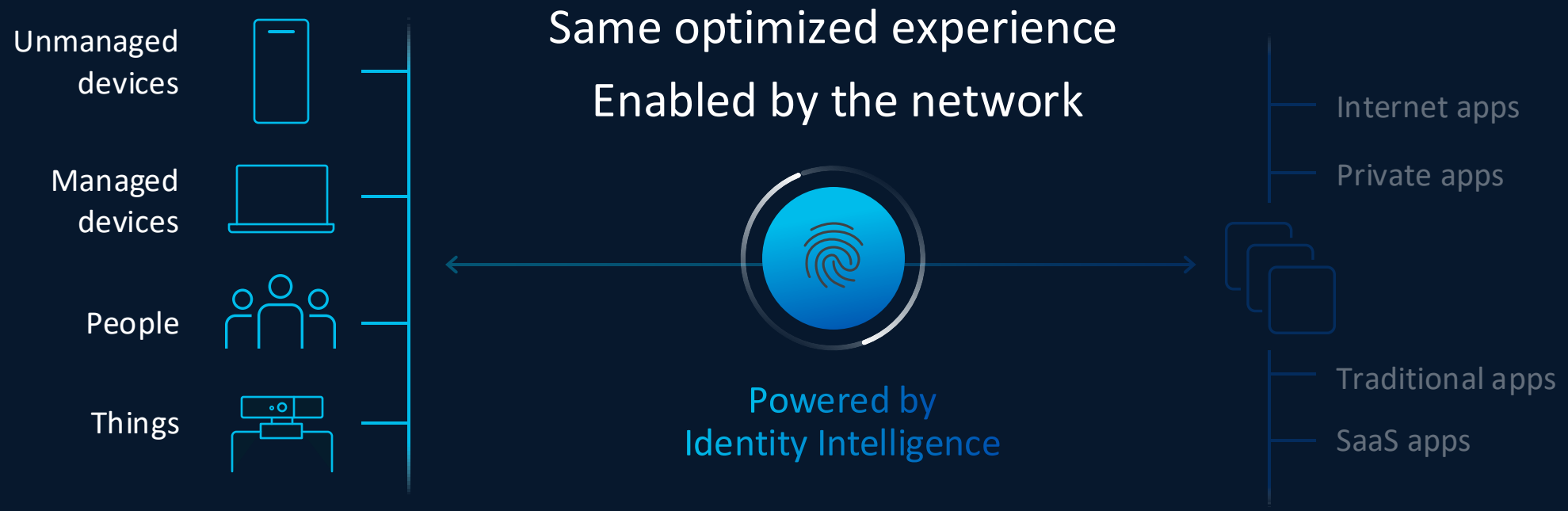
Data Loss Prevention | Remote Browser Isolation | AI Access
Firewall as a Service | Secure Web Gateway | Zero Trust Network Access
Cloud Access Security Broker | DNS Security | VPNaaS

Consistent Security:
Security Service Edge

Zero friction:
We do the plumbing.

- Traditional Apps
- Private Apps
- Internet Apps
- SaaS Apps

Universal ZTNA from Cisco



Remote

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

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*

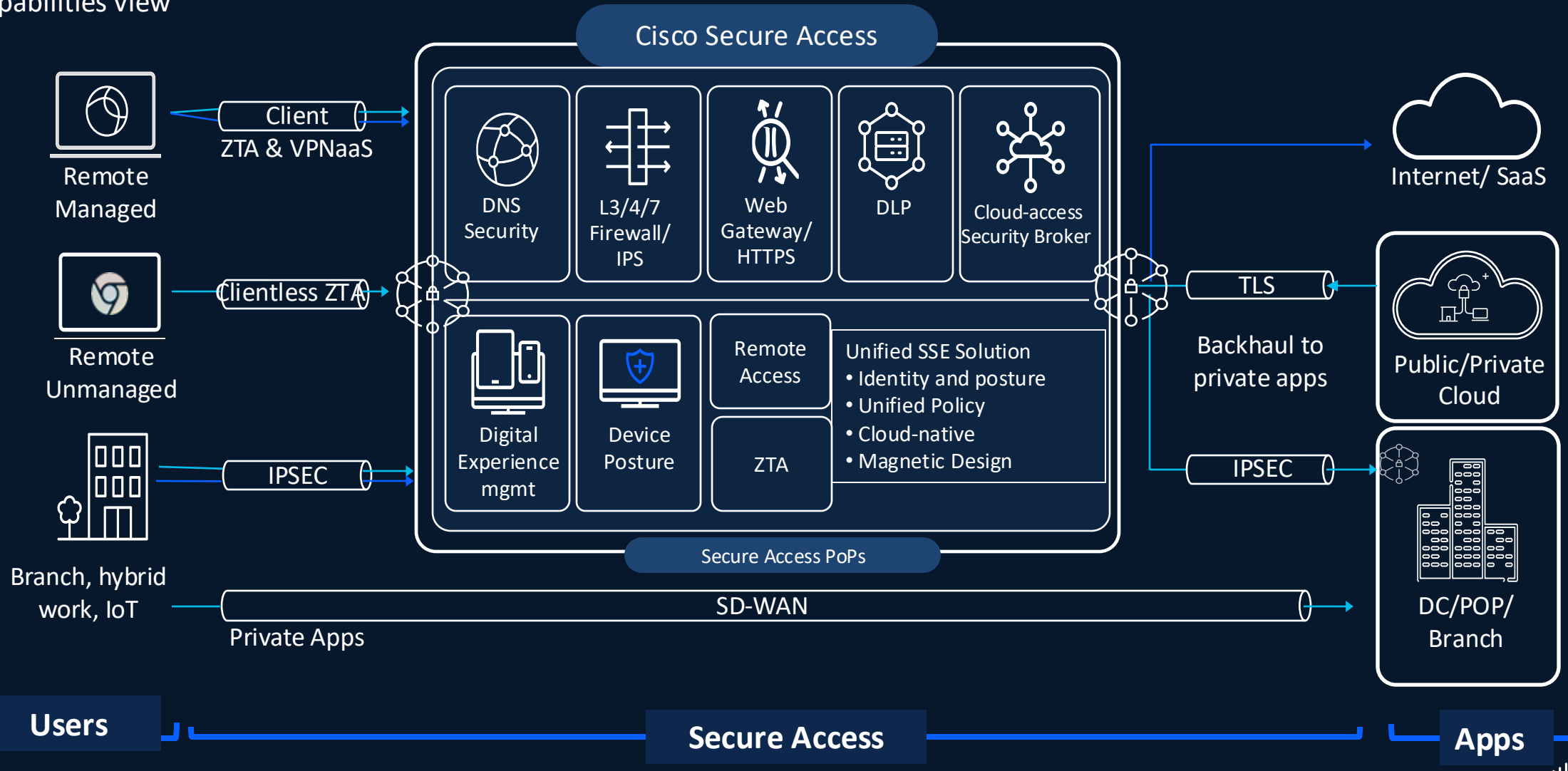
Add-on solutions

- SD-WAN
- XDR
- DUO MFA/ SSO
- CSPM

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

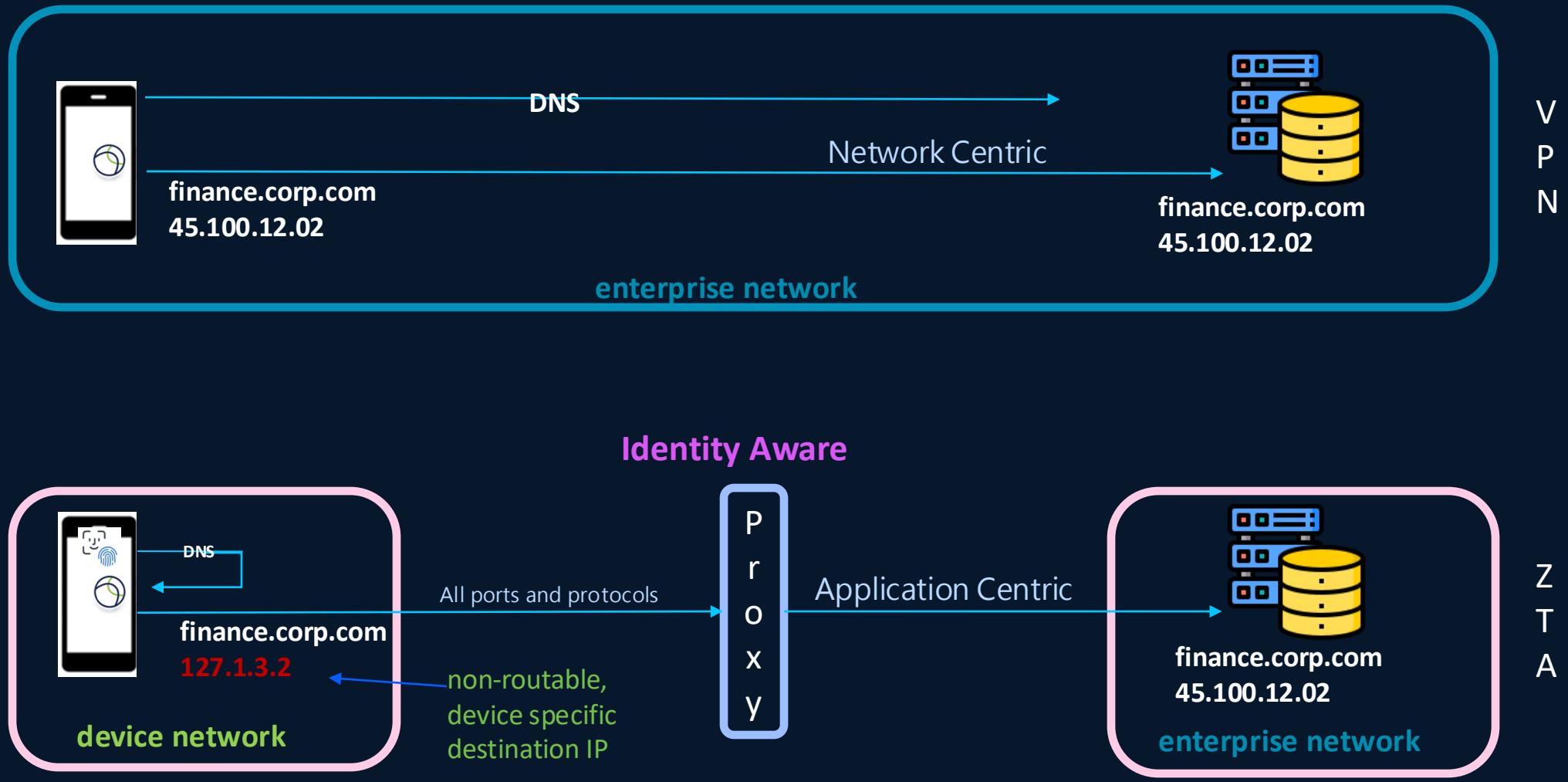
Cisco Secure Access

Capabilities view



Zero Trust Access
“Zero Friction”

VPN vs Zero Trust Access



Zero Friction: Transparent UZTNA

STEP 1
Authenticate,

STEP 2
Access application

We do the plumbing

Continuously assess Identity and posture transparently

Identity Intelligence
Session Theft Protection
Seamless Login

Traditional apps

Private apps

Internet apps

SaaS apps

Zero Friction: Single Client

One client.
Multiple functions.

RAVPN	SIA, DNS
Device posture	Network/Endpoint Visibility
ZTNA	Digital Experience Monitoring

Use ZTA to secure all internet destinations

NEW! All ports and protocols!

- Traditional apps
- Private apps
- Internet apps
- SaaS apps

Secure Internet Access

Single client, multiple functions

Single client, multiple functions

Seamless Access

We handle the plumbing

Go to work

Low Latency
Connectivity

Private Apps

Internet Apps

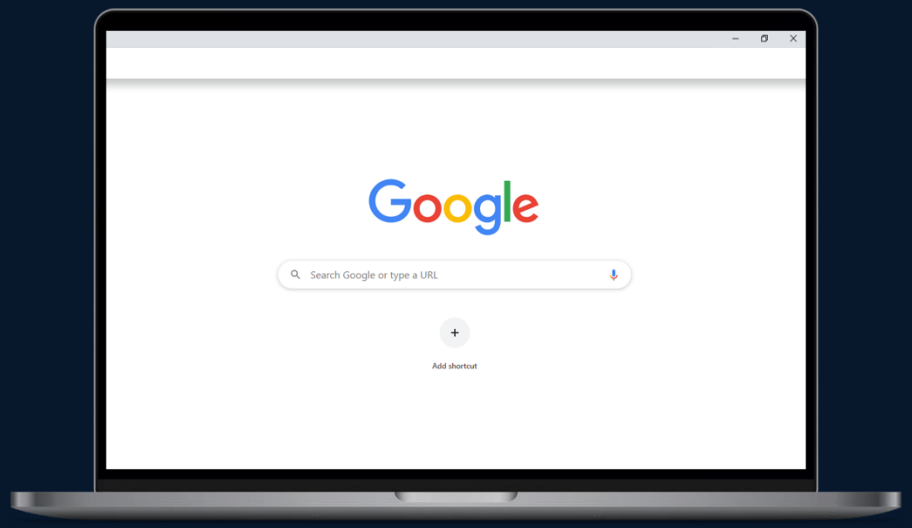
Traditional Apps

SaaS Apps

Modern PoP Architecture

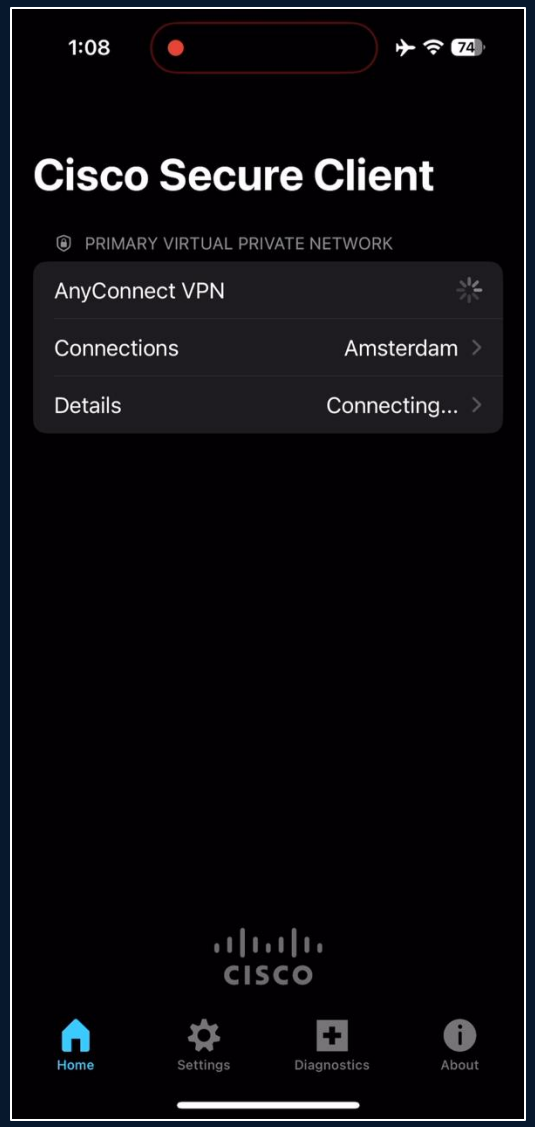
Native Device Support

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

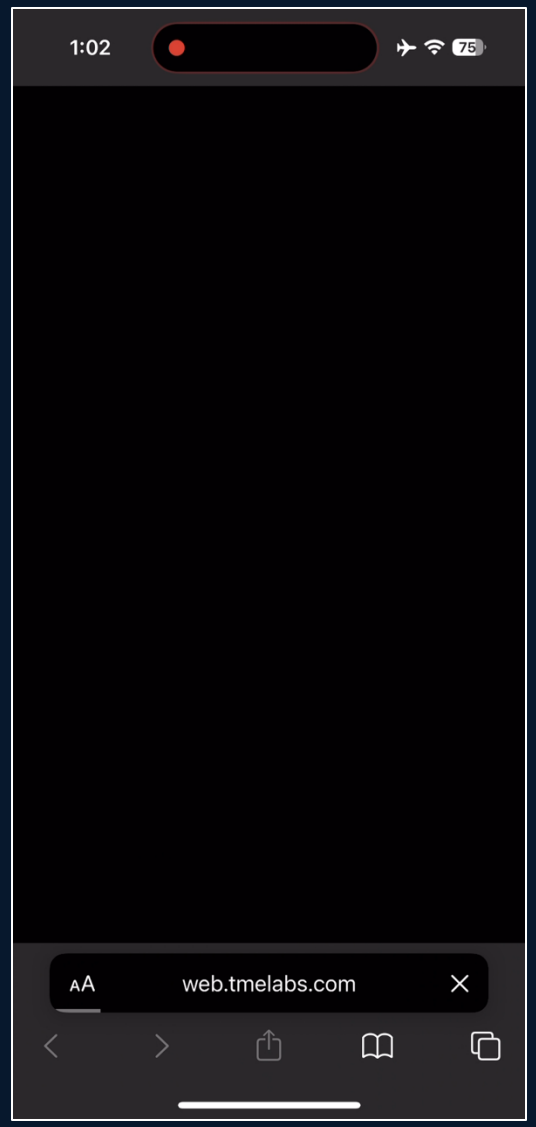


Chrome Enterprise Browser

Native OS Integration

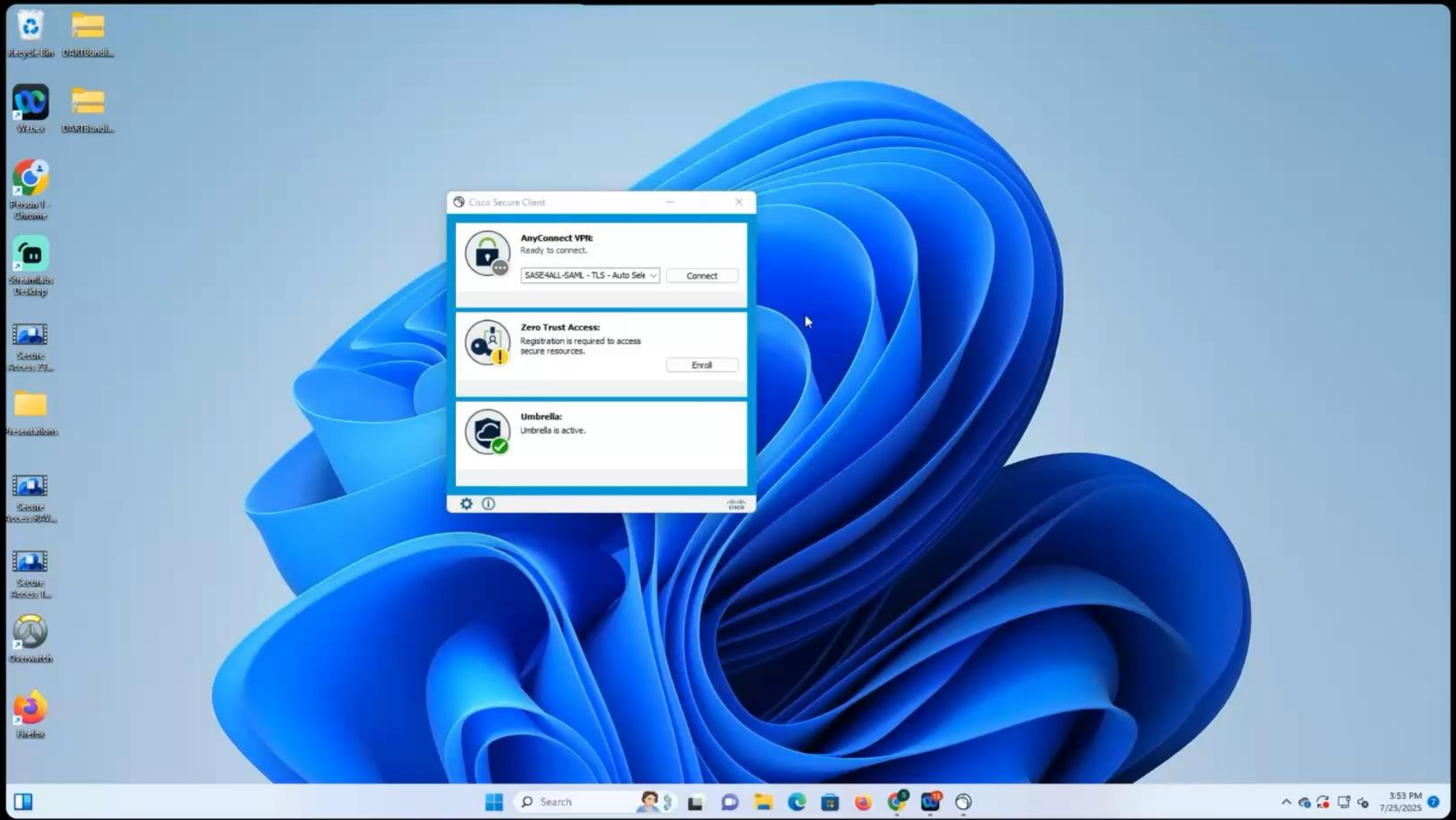


VPN



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

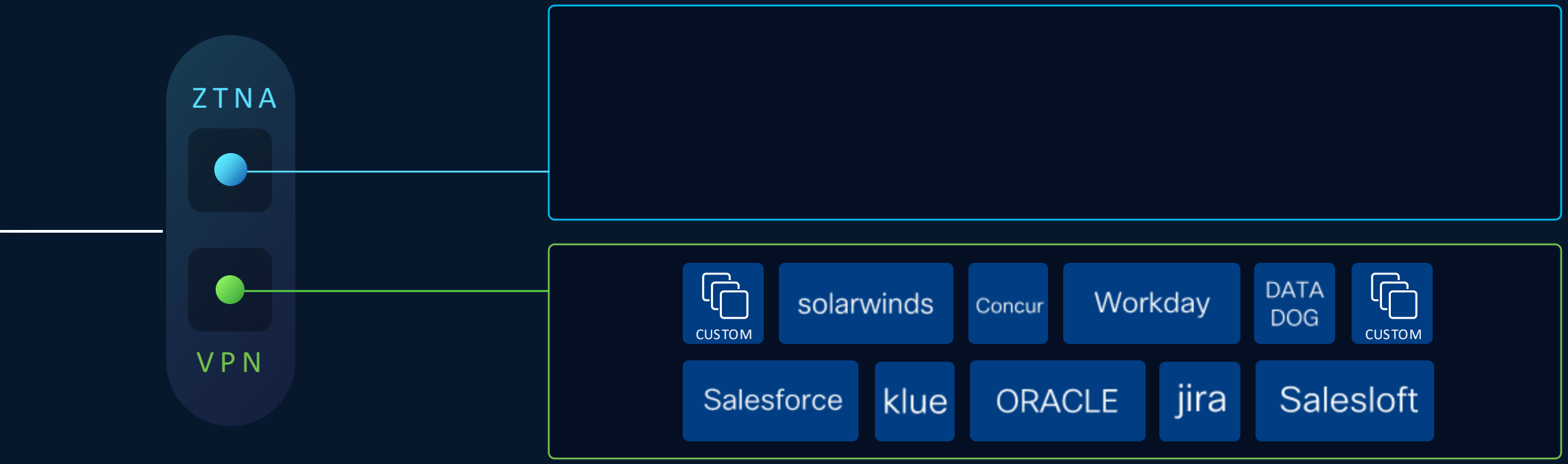
Windows and macOS devices enroll using: SSO Authentication | Certificates

Android and iOS devices enroll using SSO Authentication only.

Secure Private App Access

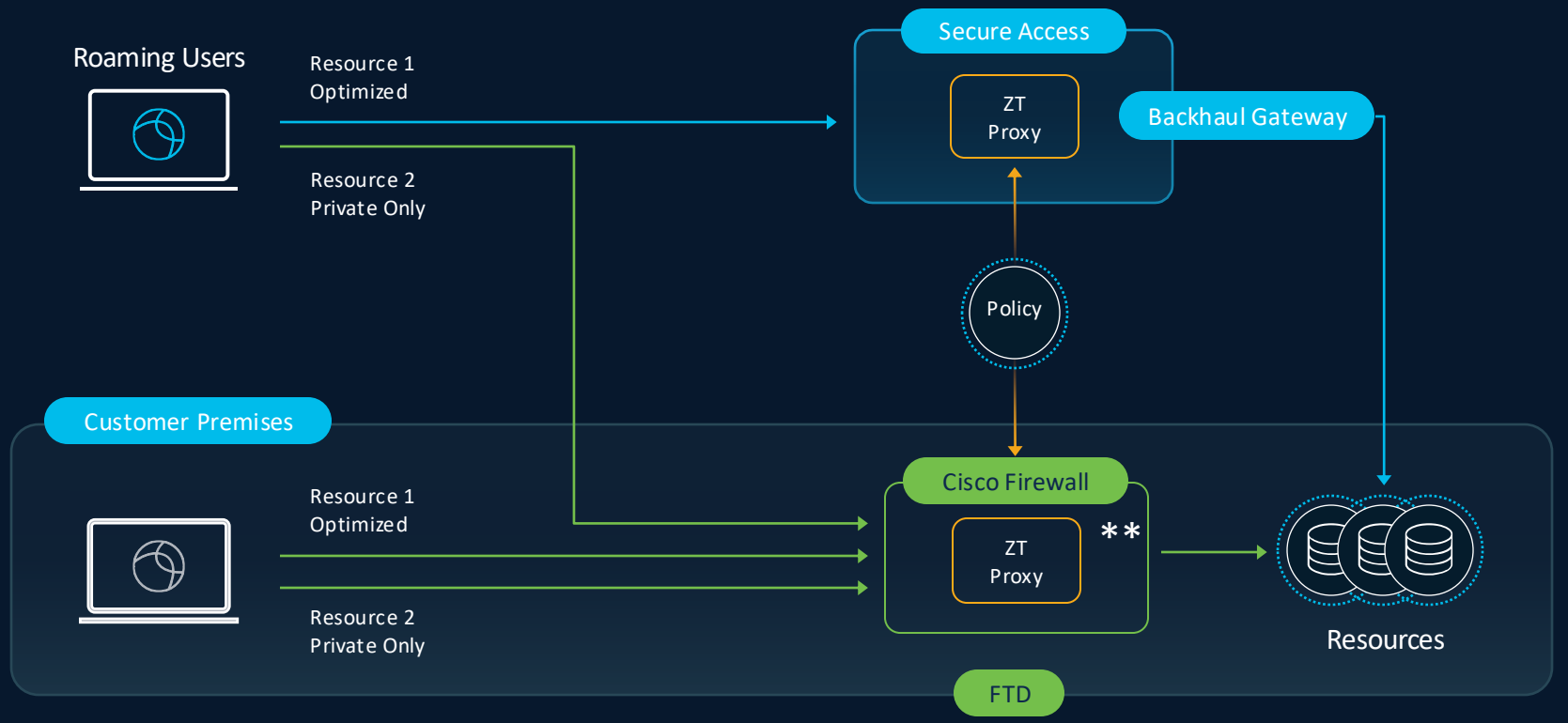
Seamless Experience

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



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.

Hybrid ZTNA Demo

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

Increasing network and security convergence

Cisco SASE

now unified on Secure Access

Flexibility to choose optimal connectivity

Unified security policy managed by Security Cloud Control

Consistent cloud enforcement

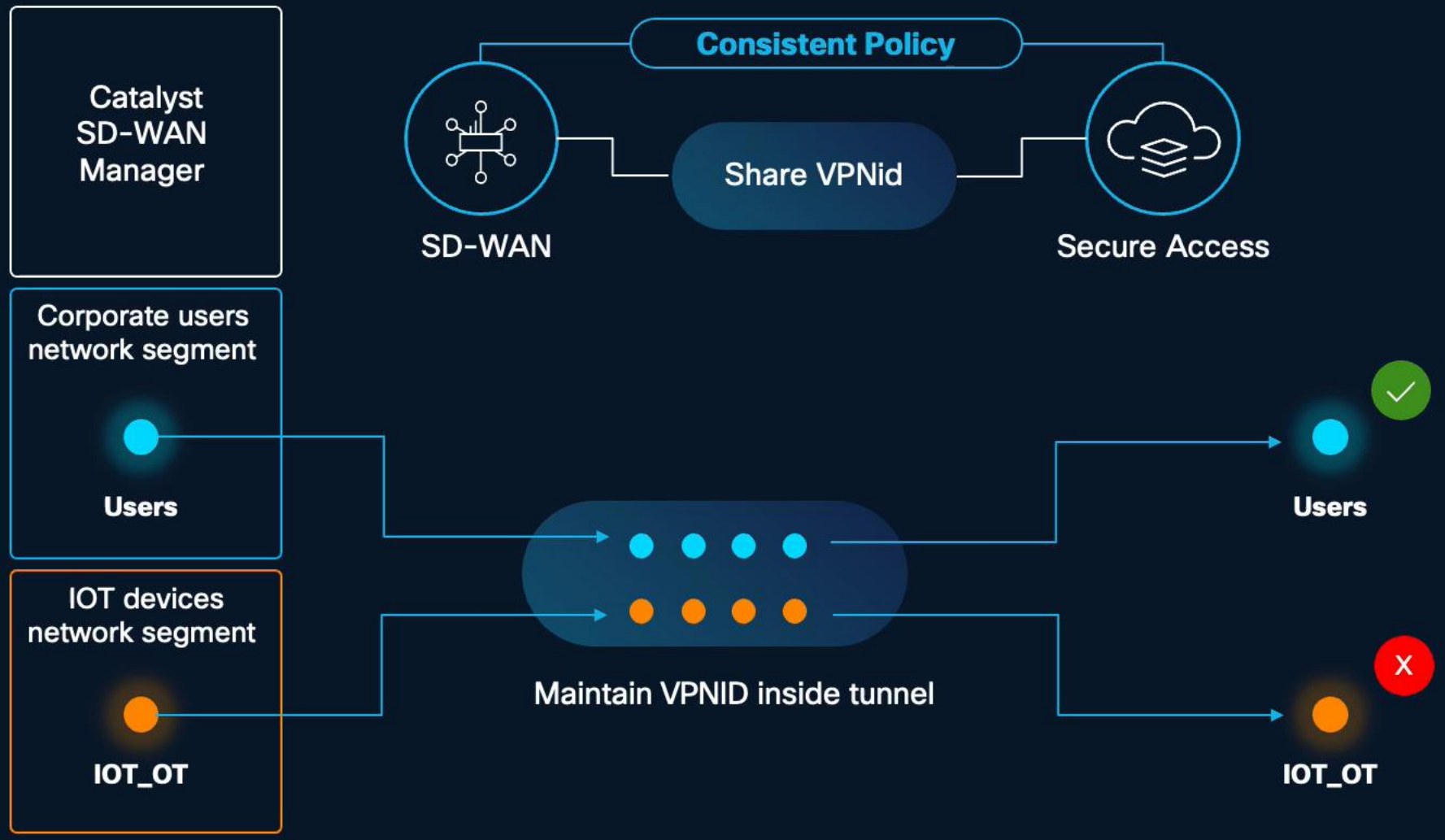
cisco

Context Sharing over SD-WAN Demo

Catalyst SD-WAN

VPNid support for coarse-grained segmentation

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



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		-	

Safe Use of AI Apps and Agentic AI

Using AI apps

Classification: **Safety Guardrail**

Toxicity

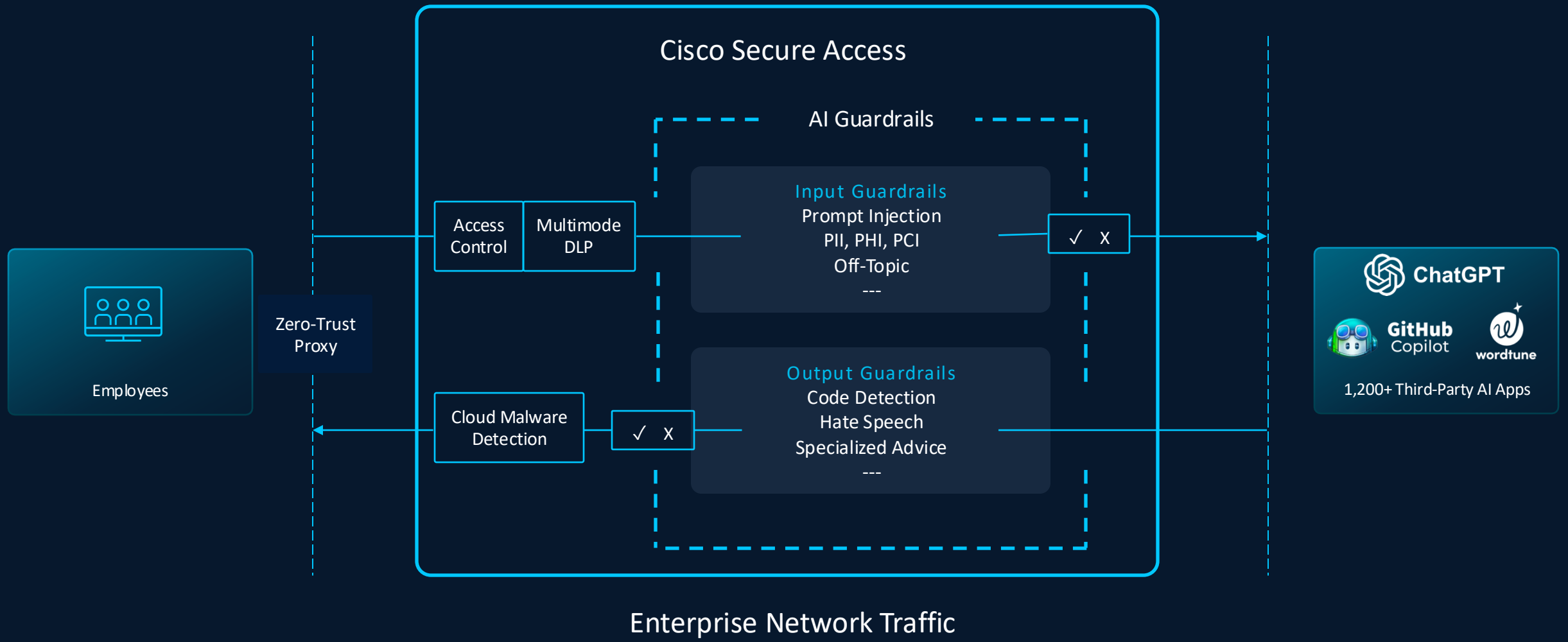
How to make a bomb

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

Data Loss Prevention

dashboard.sse.cisco.com/org/8206406/overview

Johann | Space/Cars | HOME | Health | Security | Camera Video Co... | WhatsApp | Voice - (22) Mess... | MONEY | VILLAGES | Grok | Cisco | Duo | CiscoSecure | All Bookmarks

Secure Access

John Martin

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

Network tunnel groups 18 total

9 Disconnected

9 Connected

Resource connector groups 2 total

2 Connected

FTDs 2 total

2 Failed to sync

Data Transfer

Last 24 Hours

TOTAL USAGE

Usage data - delayed up to 30 min.

1.81 GB Total traffic

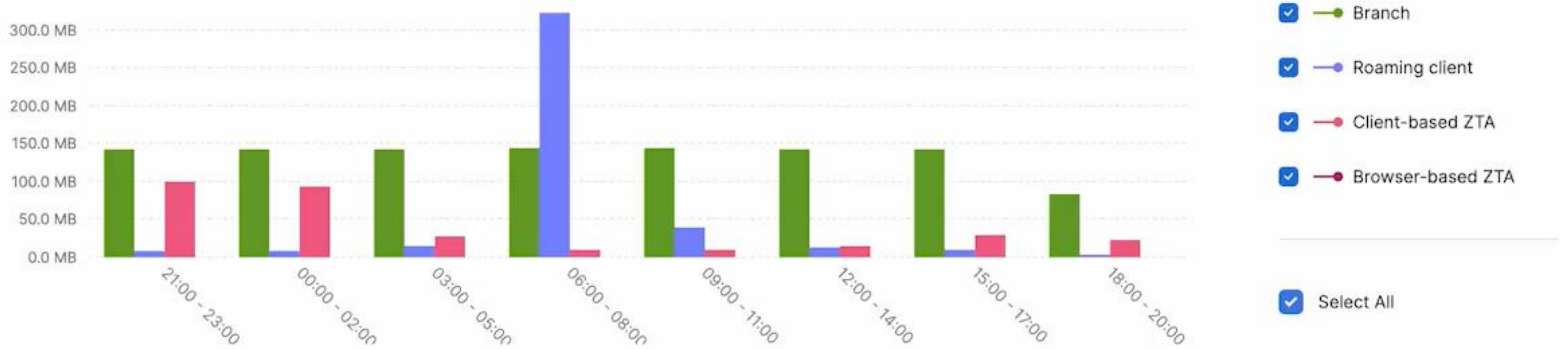
1.61 GB Decrease (last 24 hours)

347.80 MB Received

247.59 MB Decrease (last 24 hours)

1.46 GB Sent

1.36 GB Decrease (last 24 hours)



Security

Last 24 Hours

Security Activity | Top Security Categories | File Retrospective

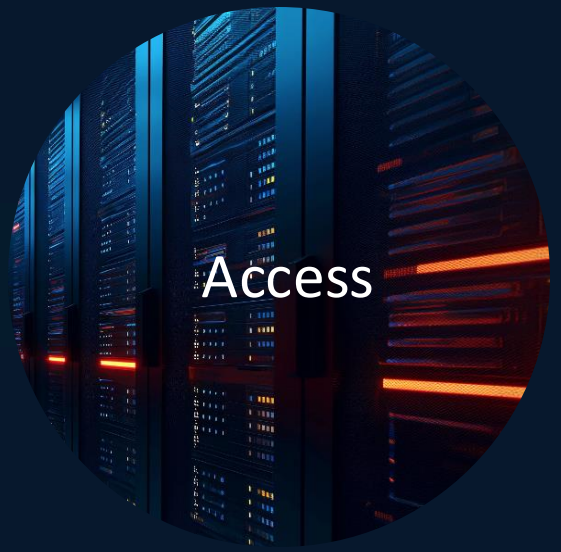
Access Events

Role of identity in a Universal ZTNA approach

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

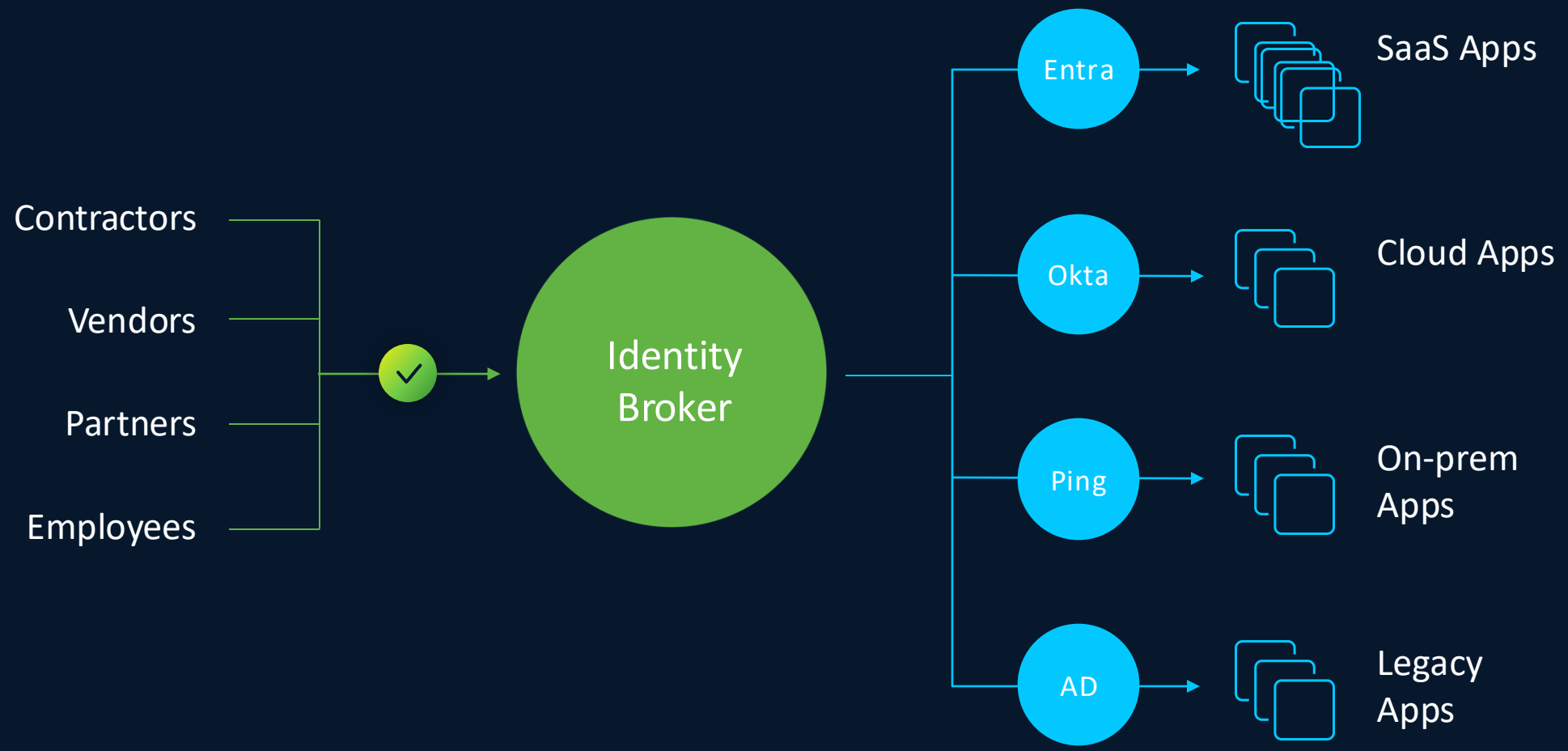
UNTRUSTED

* Capabilities are in private preview.

Standalone IAM when required

Identity broker for existing IAM

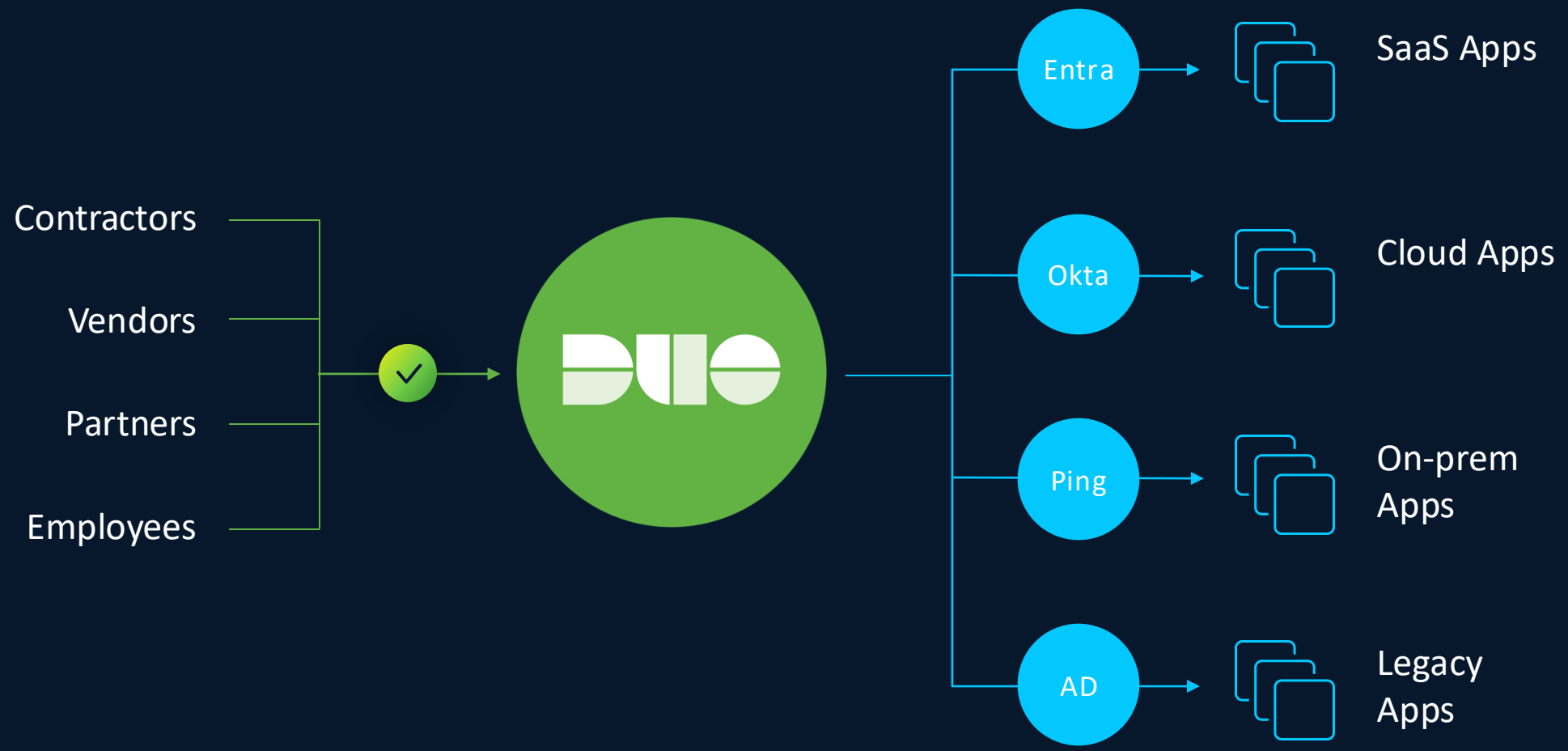
Alternate directory for third-party users



Standalone IAM when required

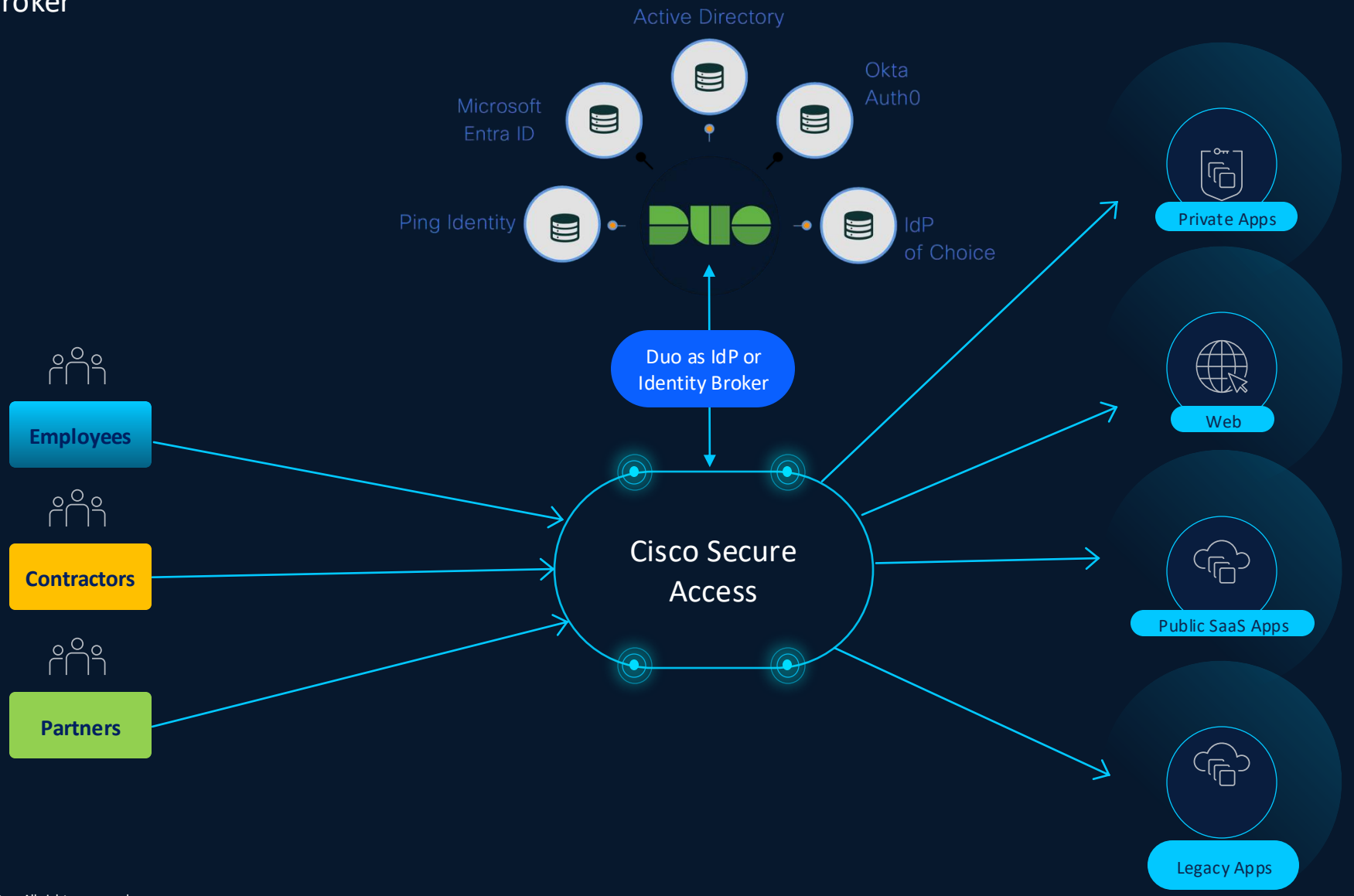
Identity broker for existing IAM

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

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

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

cisco

CISCO Engage | Tech Day

Thank you