CISCO Connect

# Cisco Secure Access

Seamless Zero Trust Security

Eric Yandle
Solutions Engineer

Hunter McMillan
Solutions Engineer


February 5, 2026

# Agenda

1. Welcome to Cisco Secure Access
2. Modern Challenges with Hybrid Workforce
3. Core Capabilities
4. Identity Intelligence
5. AI Security

# Discovering Cisco Secure Access

# What We Hear From Leaders

“I need security that can keep up with latest attack strategies.”

“Security gets in the way of productivity for my employees.”

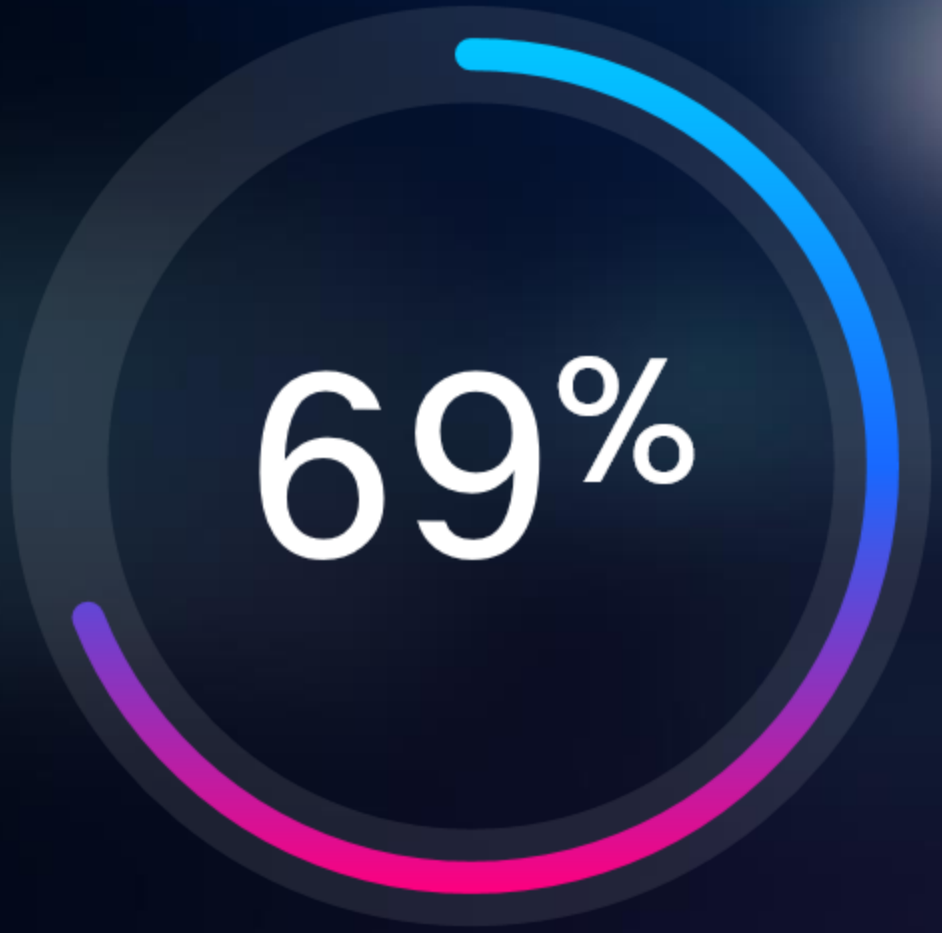
“There are too many disparate security tools creating blind spots and risk”

# Modern Security Must Be...

Safer for everyone and everything

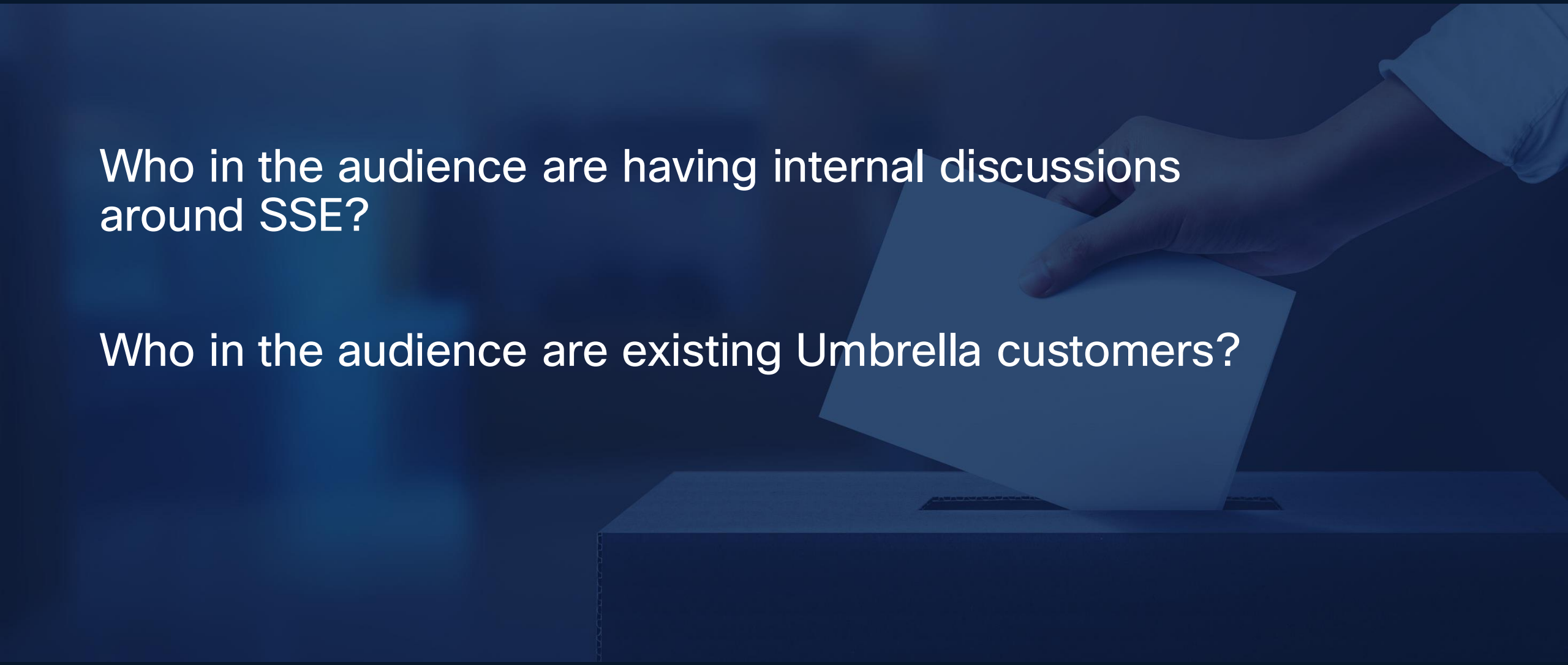
Better for users

Easier for IT




of businesses want to adopt a security service edge (SSE) platform within the next 2 years

# Show of Hands...



Who in the audience are having internal discussions around SSE?

Who in the audience are existing Umbrella customers?

# What's Driving Interest in Security Service Edge (SSE)?

- Adjustments in the mix of cloud and on-premise applications/data
- Frequent changes in the mix of users/locations/devices
- Evolving threats and attack tactics
- Shortage of security talent/resources
- The need for zero trust security

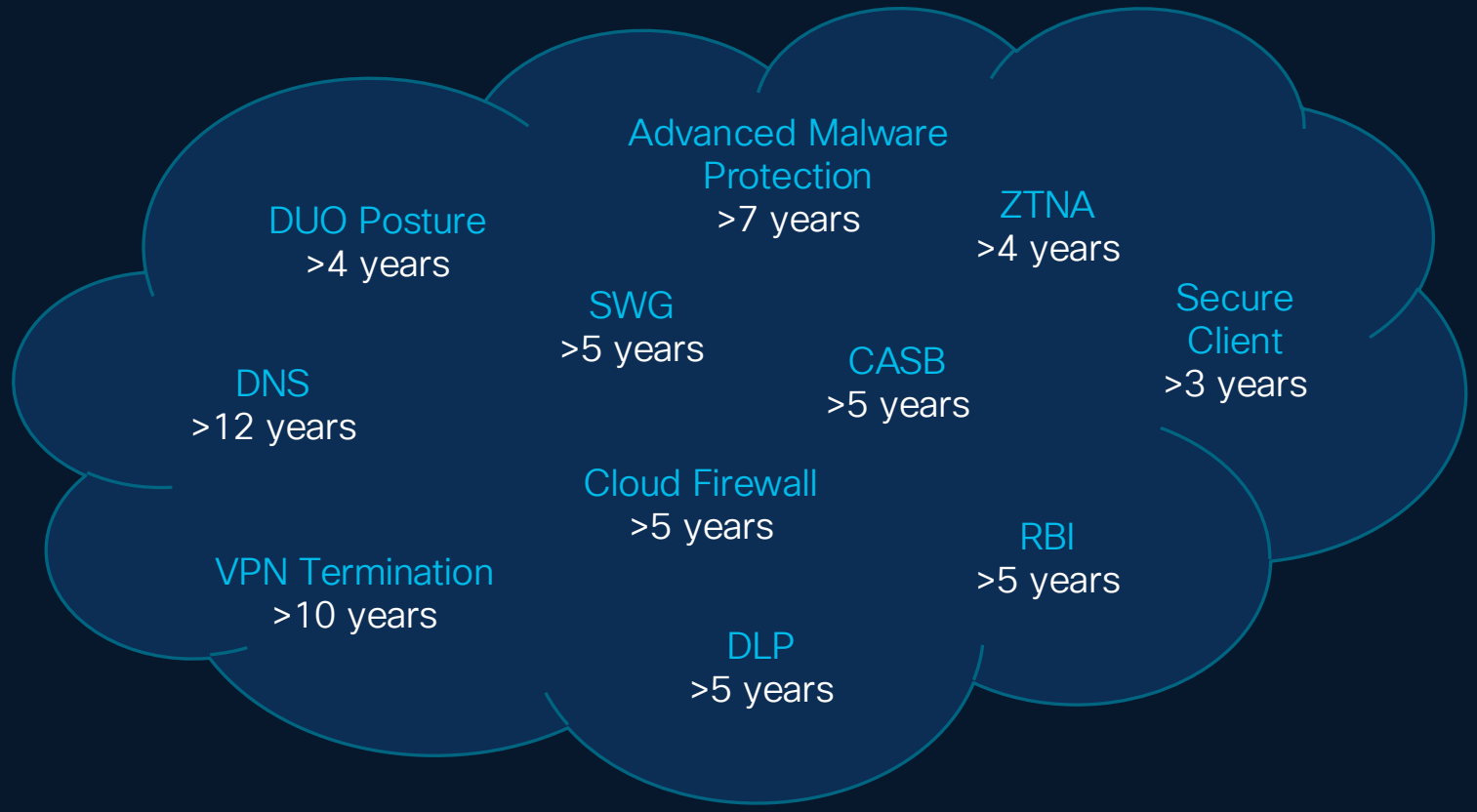
Tool sprawl and complexity are increasing risk and decreasing productivity

# 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

# Cisco Secure Access: Extended SSE Protection

## SSE core capabilities

Secure web gateway

Zero trust network access

Firewall as-a-service

Cloud access security broker

Data loss prevention

Advanced malware protection

Sandbox

## + So much more

VPN as-a-service

Digital experience monitoring

AI Access and usage controls

Local ZTNA enforcement options

IPS with Talos threat intelligence

Enterprise browser integration

Remote browser isolation

Policy verification

DNS security



# Cisco Secure Access

Go beyond core Secure Service Edge (SSE) to better connect and protect your business

## 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)

# Seamless Access

We handle the plumbing

Go to work

Private Apps

Internet Apps

Traditional Apps

SaaS & AI Apps

# One Client, Multiple Functions

# Cisco Secure Client

Suite of security service enablement modules

AnyConnect VPN (Core)

ZTA Module

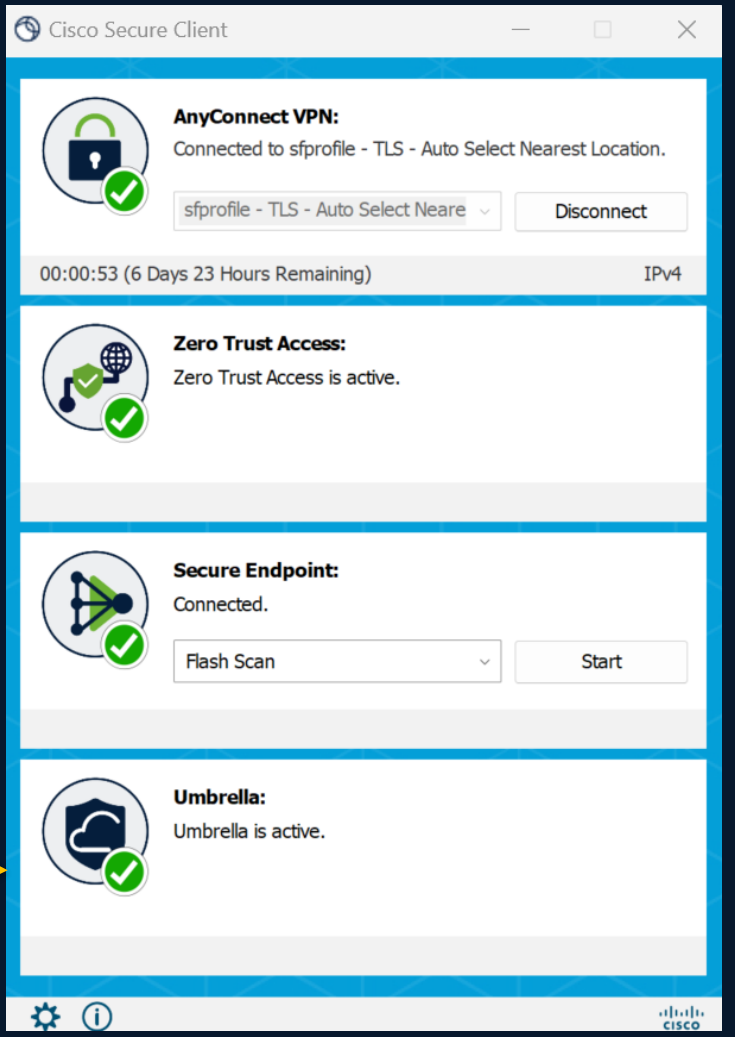
Secure Endpoint (AMP)

Roaming Module

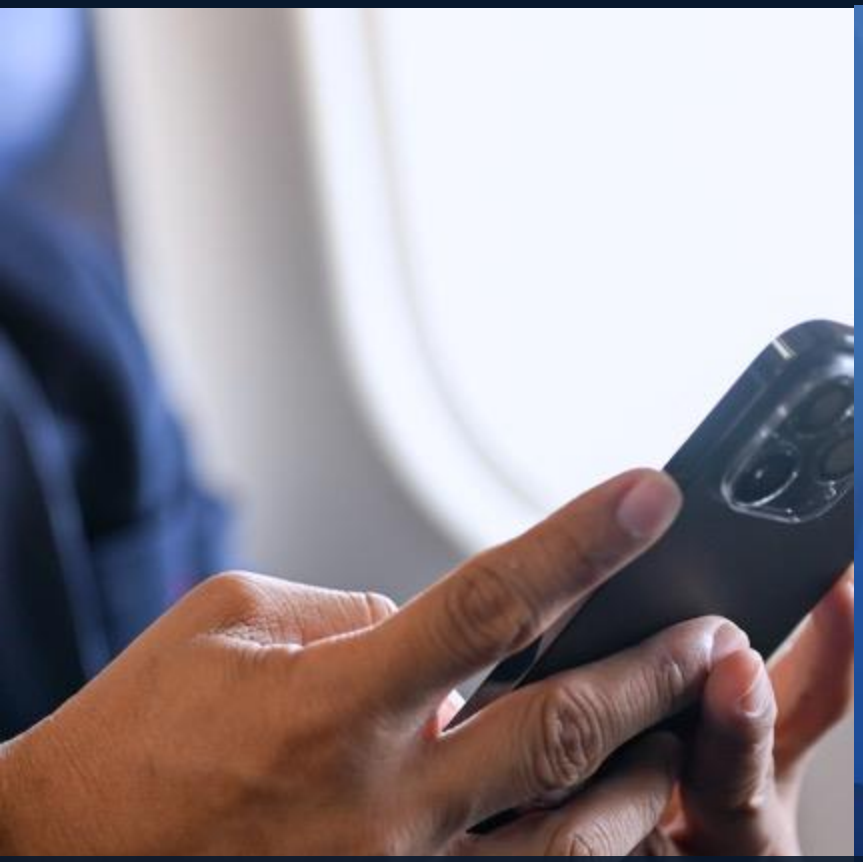
Thousand Eyes (No UI)

Cloud Management Module (No UI)

Diagnostic and Reporting (DART)



# High Speed Access: MASQUE / QUIC / VPP / Global Peering




~300% faster than VPN on a plane

No application bypass needed

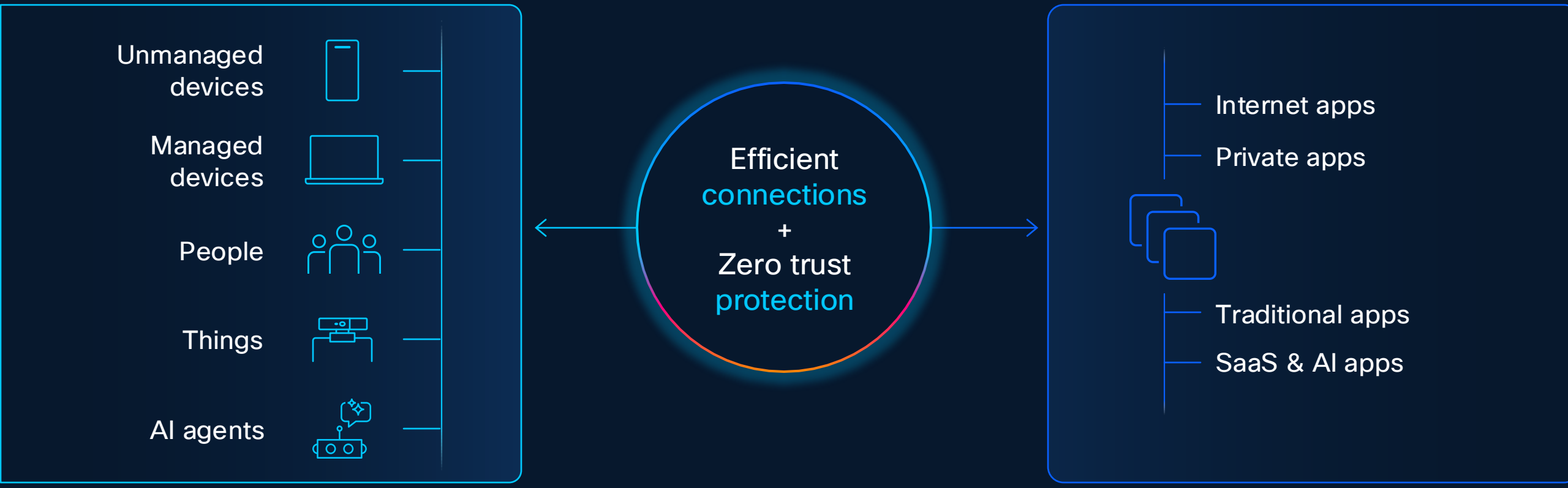
High performance for the field

# Customer Story: Peco Foods

# Zero Trust Access

# The Complexity of a Distributed Edge

# The Distributed Edge Complicates Zero Trust




| Remote | Campus | Branch | Airplane | Oil rig | Stadium | Field | ... |
|---|---|---|---|---|---|---|---|

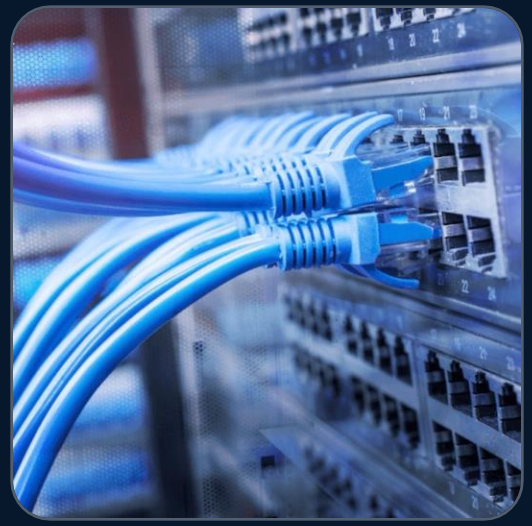
# The Power of a Unified Platform

## Tight integrations across Cisco portfolio

High performance

Identity-driven security

Resilience



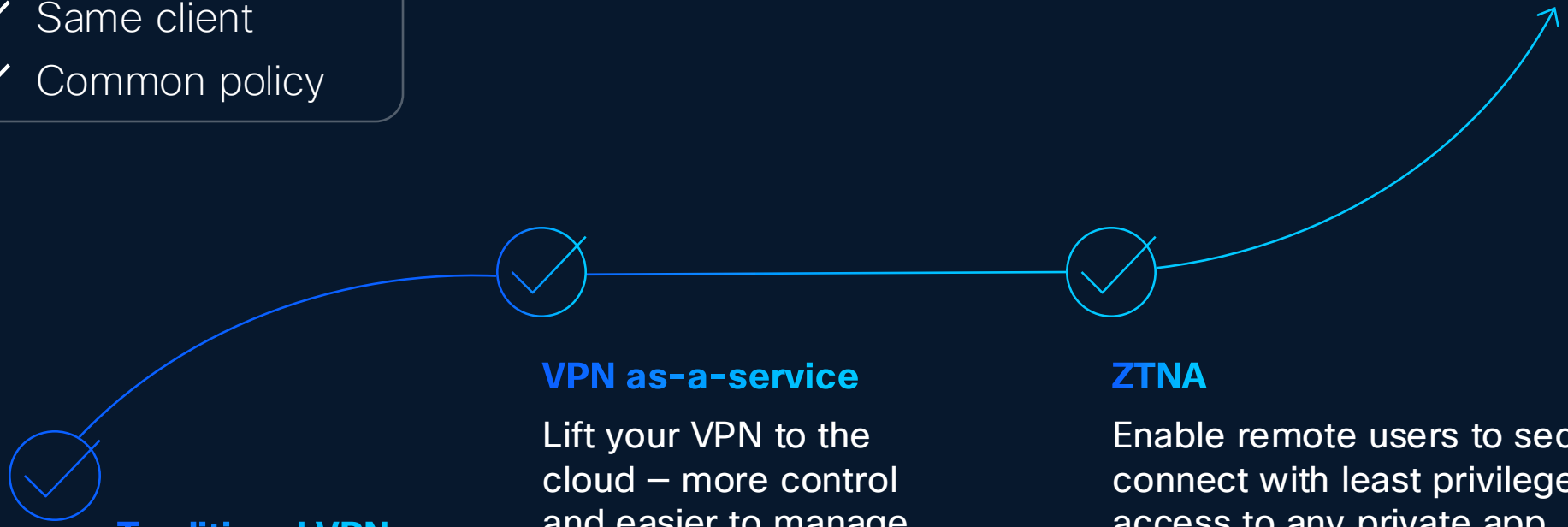
AI-powered, highly optimized operations



cisco

# Flexible Journey to Zero Trust Access

- ✓ 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 any private app.

**Zero Trust Access**

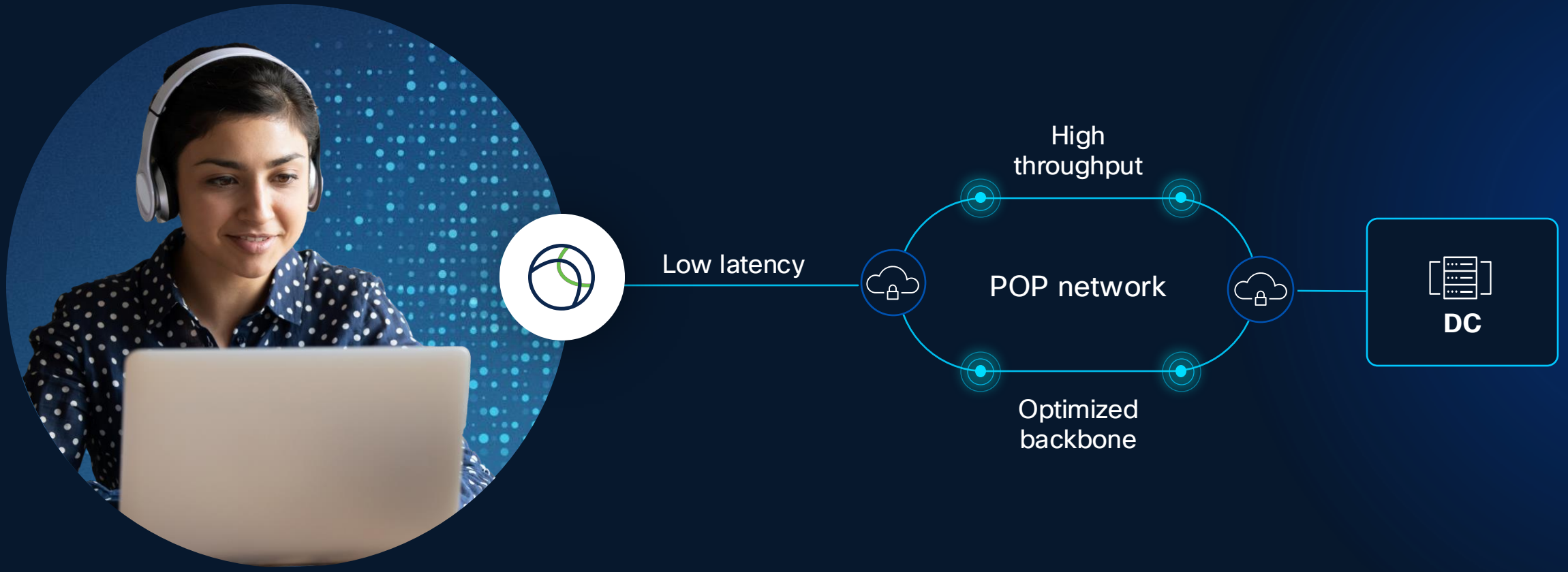
Any user/device/thing securely connect with least privilege access to any app – anywhere.

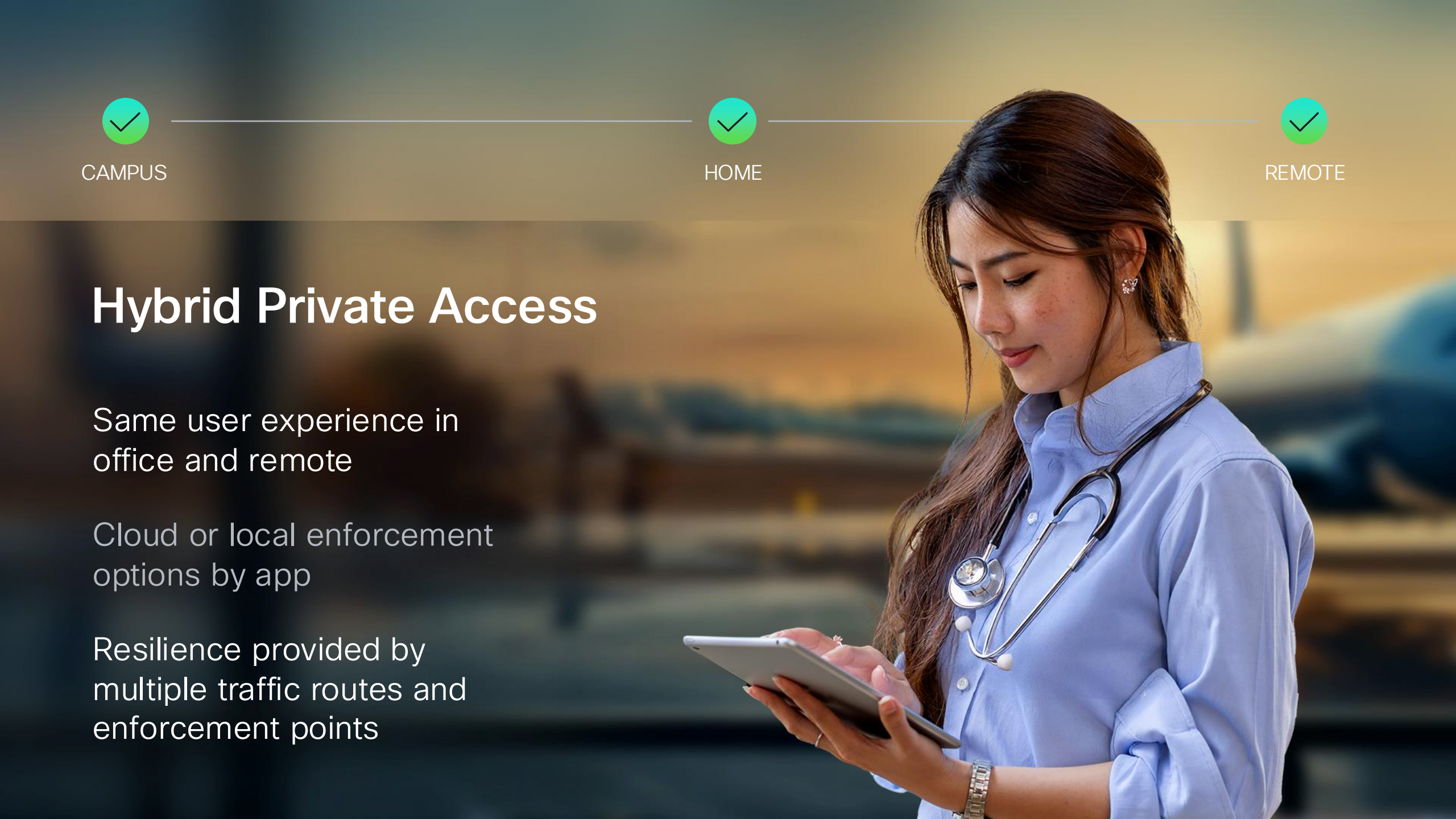


cisco

# Cisco’s Modern PoP Architecture Optimizes User Experience

Highly performant zero trust access – to all kinds of apps and data from anywhere






# Hybrid Private Access

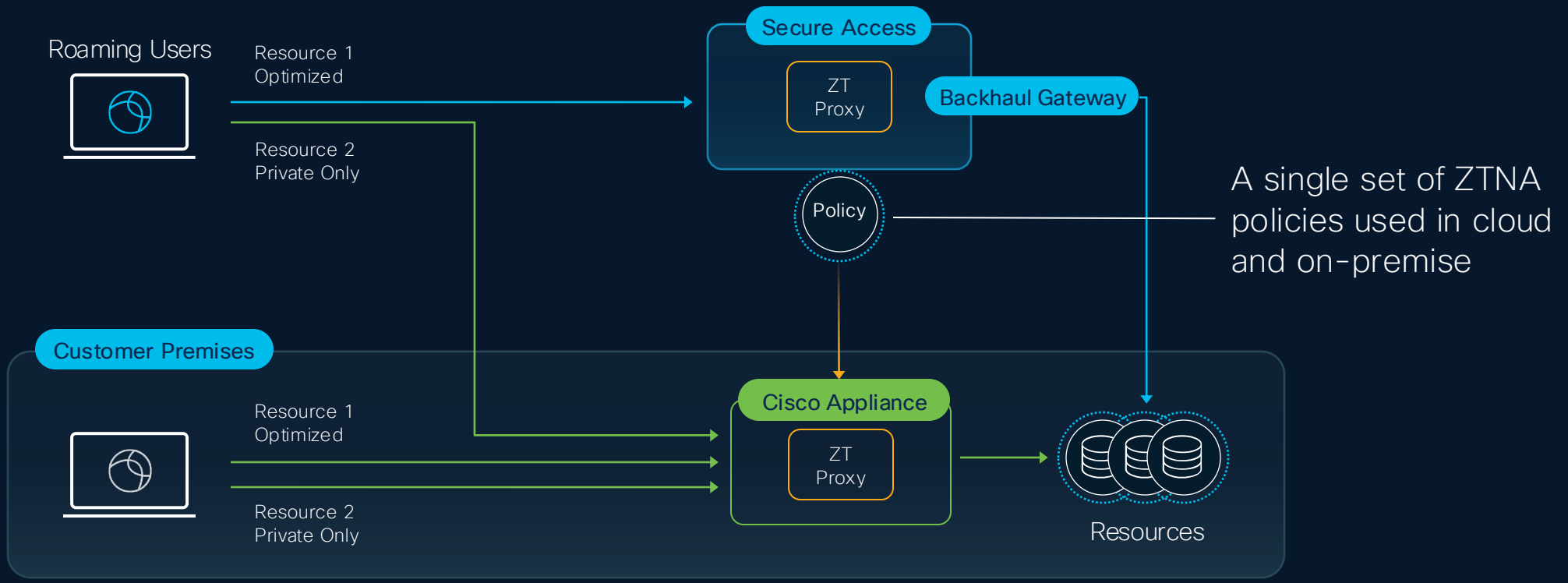
Same user experience in office and remote

Cloud or local enforcement options by app

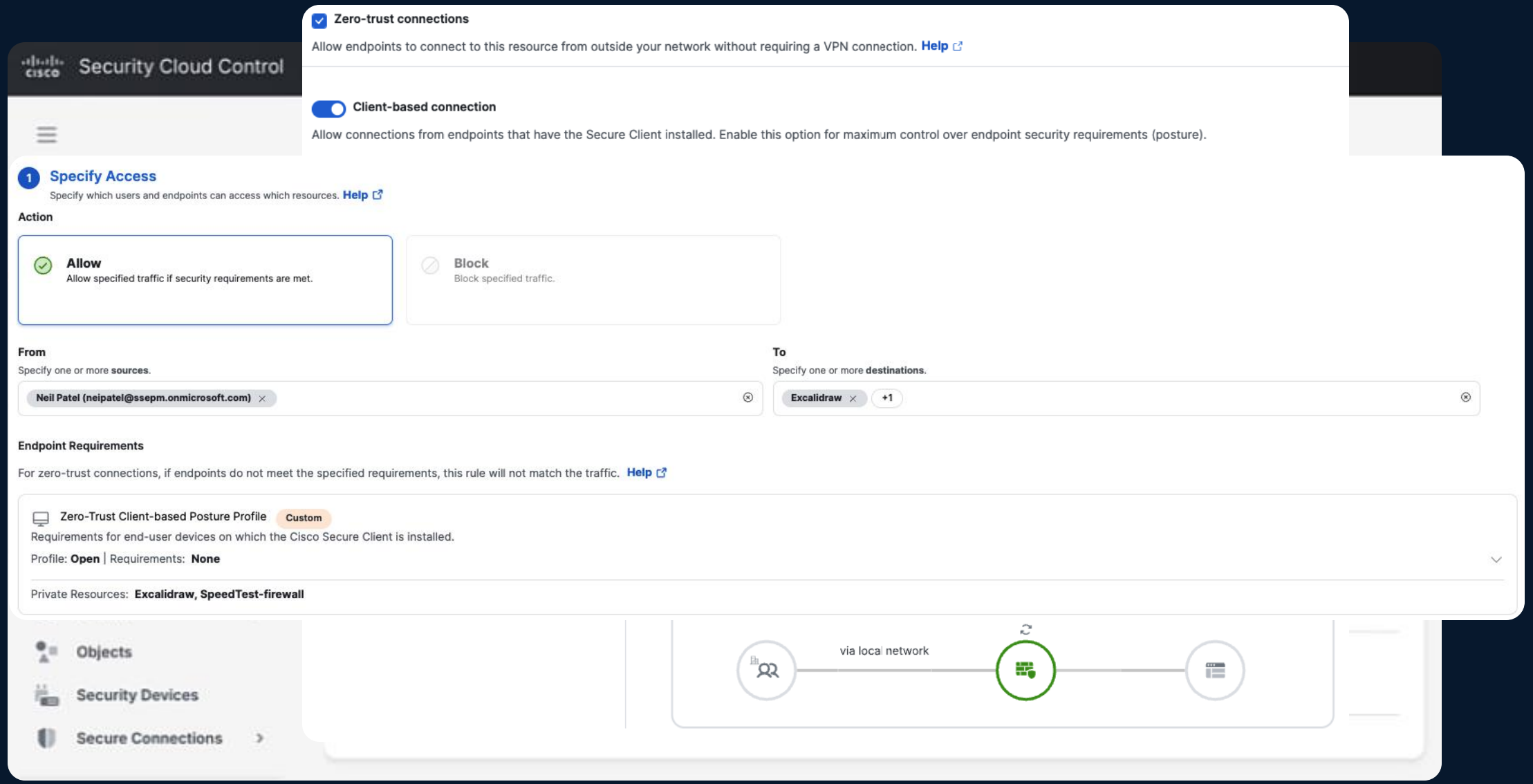
Resilience provided by multiple traffic routes and enforcement points

# Hybrid Private Access for Flexible Enforcement

## Consistent user experience everywhere



# Unified Policy Management and Seamless Integration



# Enterprise Browser

# Cisco and Google Enhance Zero Trust Access

## Google Chrome Enterprise

Browser-based security for web apps

+

## Cisco Secure Access

Cloud-based security for Private apps and more

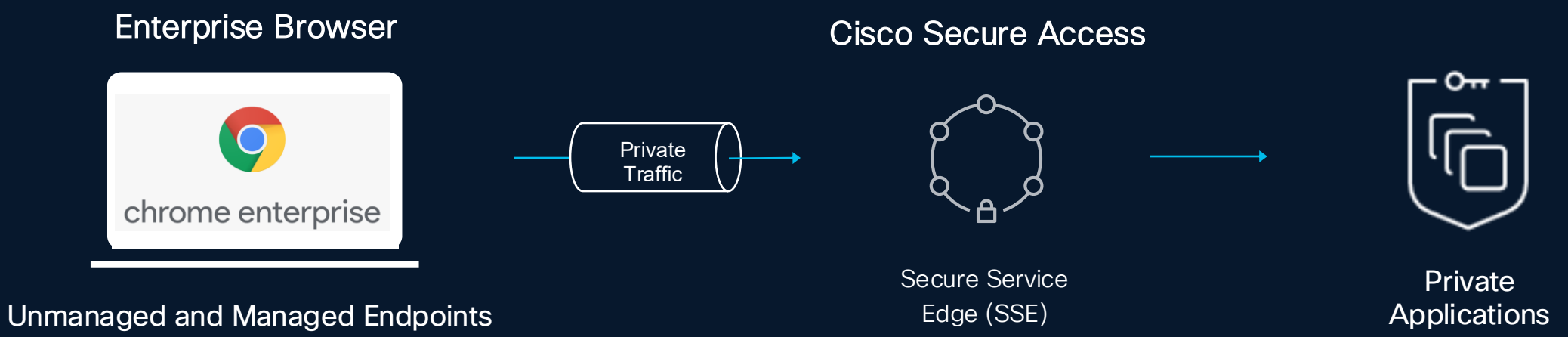
DEVICE TRUST + SECURE ACCESS TO ALL APPS + EXPANSIVE TELEMETRY



cisco

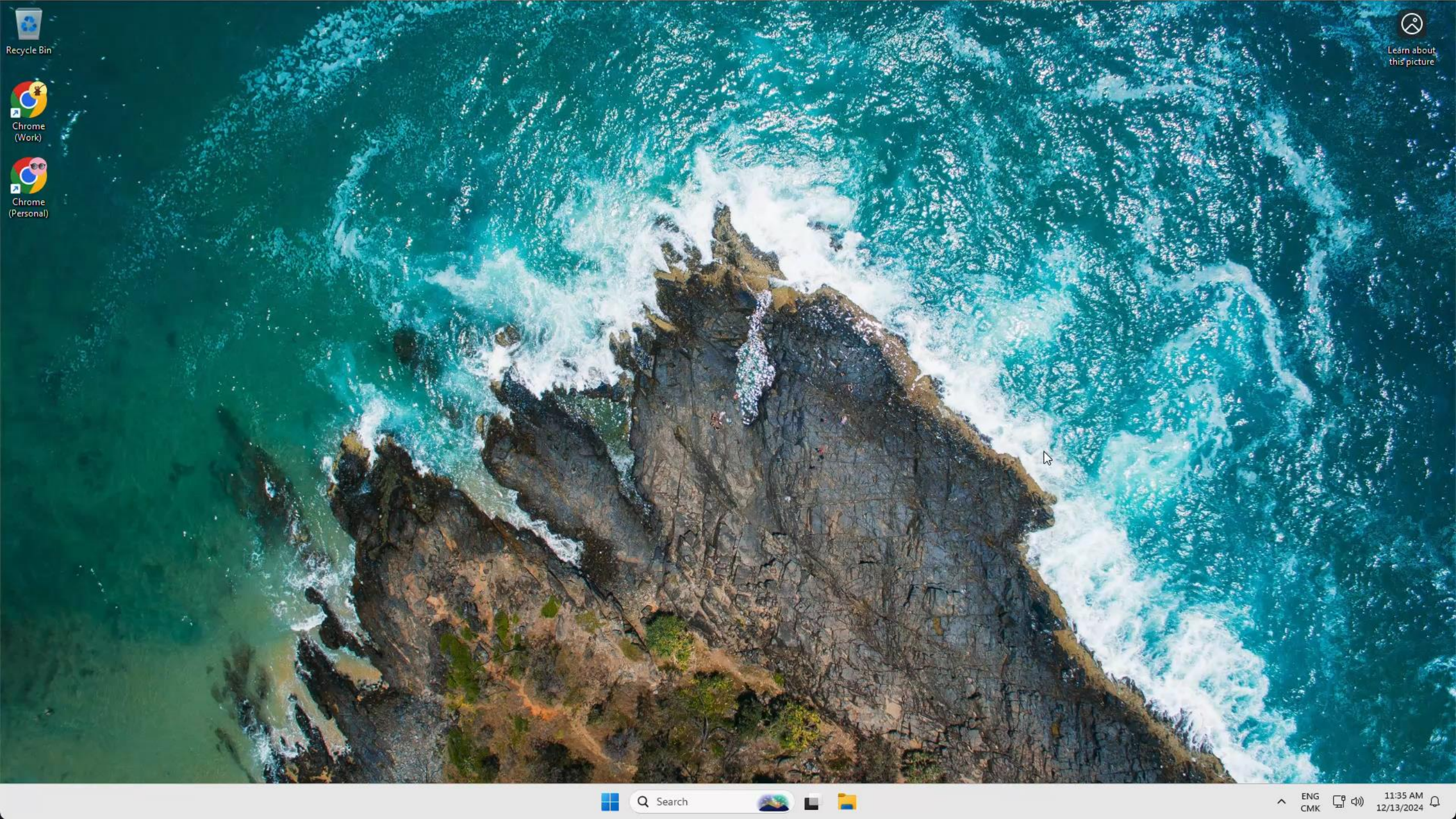
# Secure Access with Enterprise Browser

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

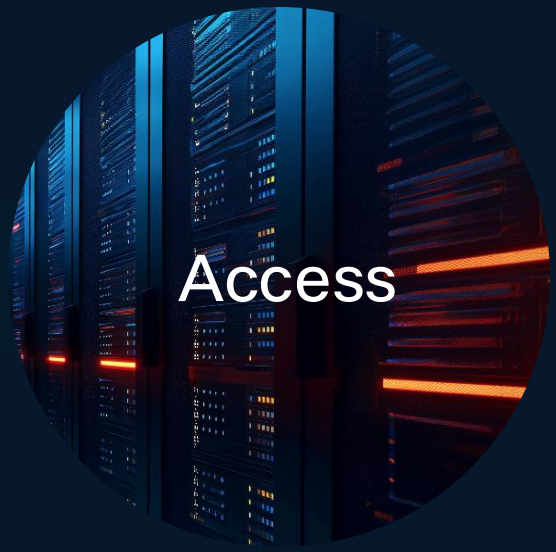

Recycle Bin
Chrome (Work)
Chrome (Personal)
Learn about this picture
Search
ENG
CMK
11:35 AM
12/13/2024

# Identity Intelligence

# Identity Intelligence

## Continuously assess you are who you say you are


BLINDTRUST




## Works with existing IDPs



cisco

Cisco Duo IAM

Cisco Secure Access

Cisco Secure Firewall

# User Trust Level

TRUSTED

NEUTRAL

UNTRUSTED

Cisco Secure Access

dashboard.sse.cisco.com/page-url

Secure Access

Alexander
Business Corp, Inc

Overview
Connect
Resources
Secure
Experience Insights
Monitor
Admin
Workflows

# Overview

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

## Connectivity

Last 24 Hours

### Network tunnels 283 total

- 8 Active
- 36 Inactive
- 161 Unestablished

## Identity Intelligence

Last 24 Hours

### Users

- 22 Untrusted users
- 4253 Neutral users
- 43 Trusted users

### MFA Status

- 159 No MFA
- 21 No strong MFA
- 22 Weak MFA
- 1 MFA Flood
- 1 Telecom MFA Limit Reac
- 3 Admins with Weak MFA

### Security Event Trends

- 30 1% Weak MFA, used to successfully sign in
- 20 15% Unused application for a user

## Usage monitoring

Last 24 Hours

**Total usage**

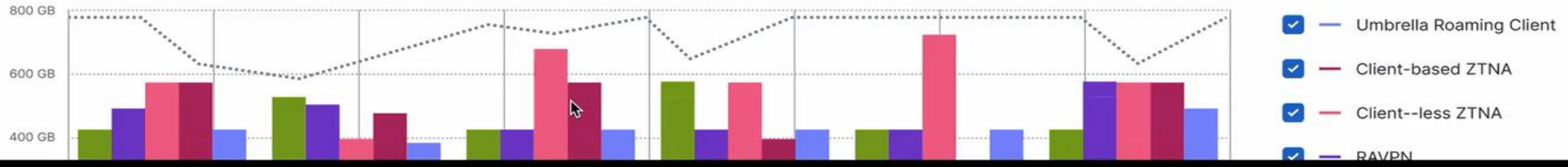
Usage data - delayed up to 30 min.

**765.59 GB** Total traffic

390 GB More than last month

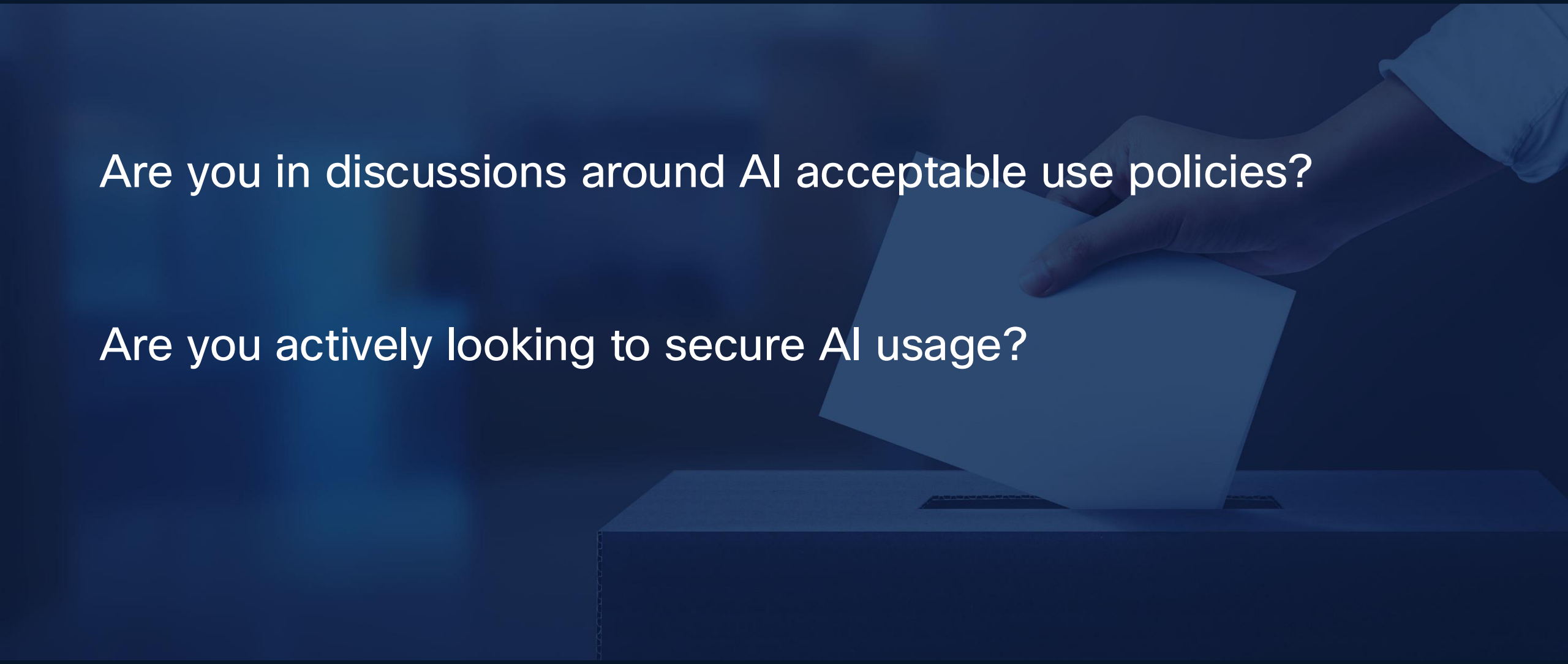
**265.59 GB** Sent

390 GB More than last month



# AI Security

# Show of Hands...

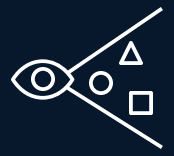


Are you in discussions around AI acceptable use policies?

Are you actively looking to secure AI usage?

# Cisco AI Access

## Securing the use of AI



Visibility

Leakage prevention

Compliant use

**1350+** AI applications



cisco

# AI Guardrail Categories – Security for AI

- Intent Based Detection

## Security

- Prompt Injection
- Response Detection

Both direction analysis is important

## Privacy

- American Bankers Association (ABA) Routing Number (US)
- Bank Account Number (US)
- Credit Card Number
- Driver's License Number (US)
- Plus other common PII

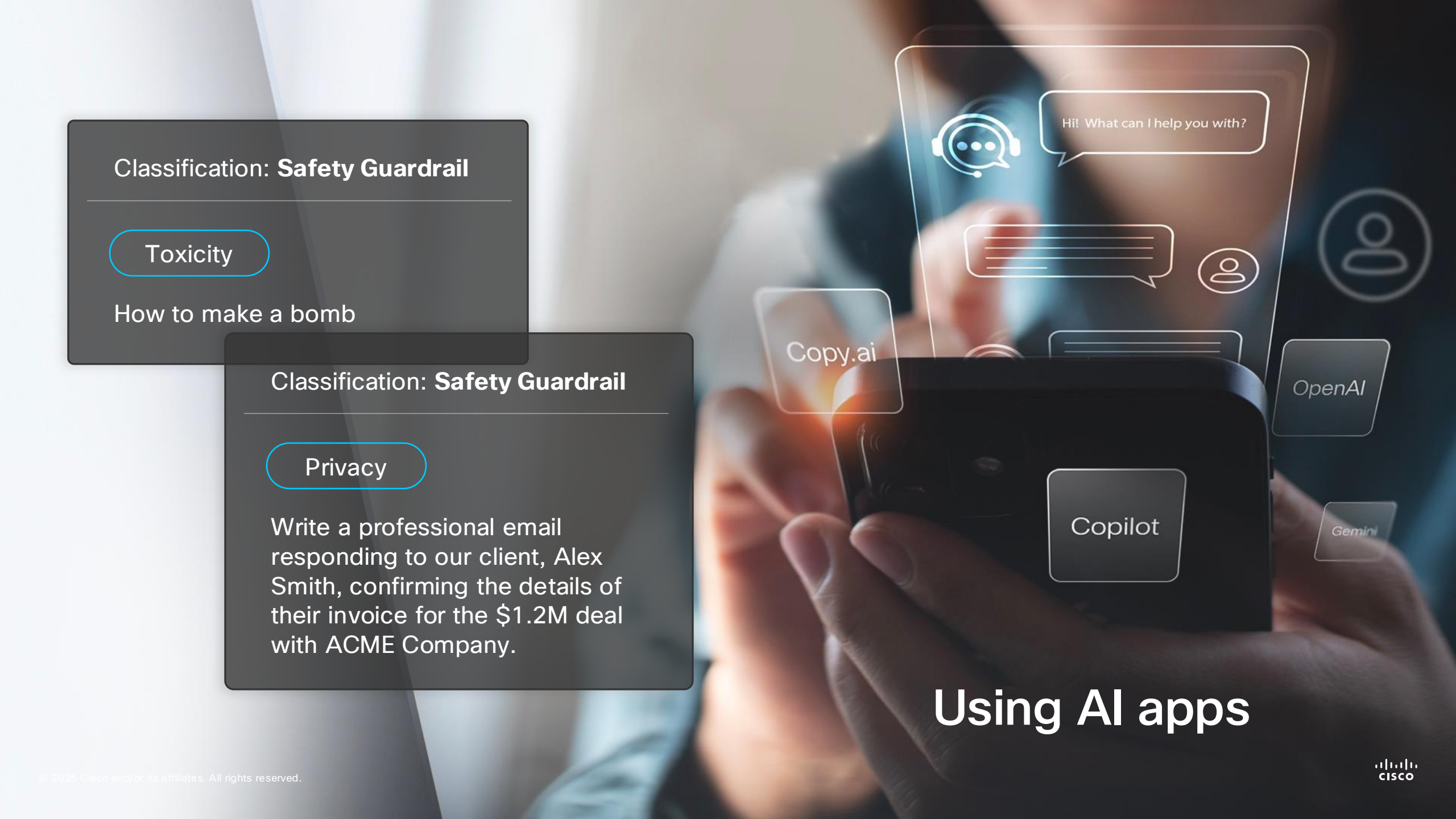
## Safety

- Harassment
- Hate Speech
- Profanity
- Sexual Content & Exploitation
- Social Division & Polarization
- Violence & Public Safety Threats

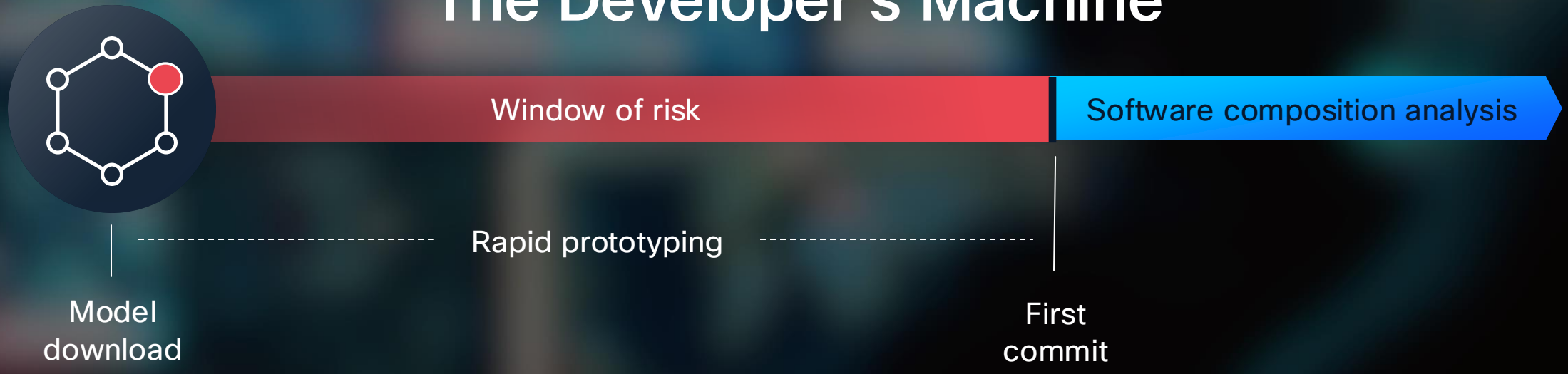
Map guardrails to standards and frameworks like: OWASP MITRE ATLAS



cisco



# A Key AI Model Risk Blind Spot: The Developer's Machine



# Stop Risky Models Before They Start

Malicious code

IP compliance

Origin compliance

## Pre-use enforcement

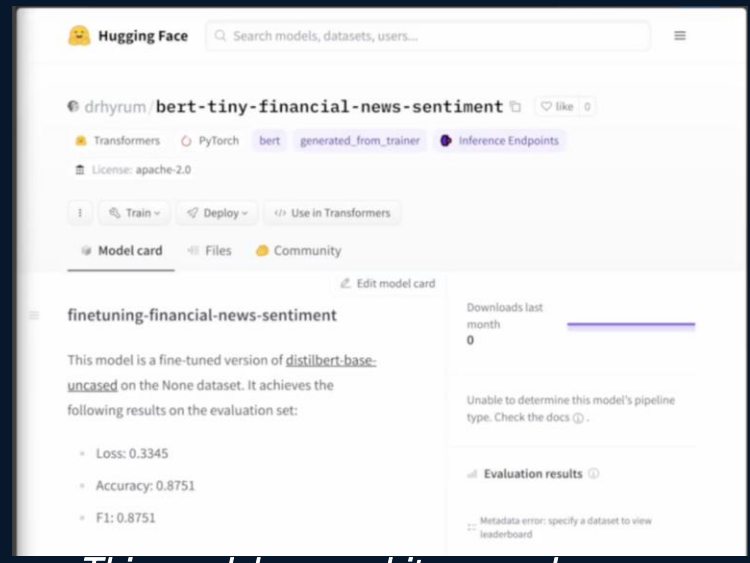


cisco

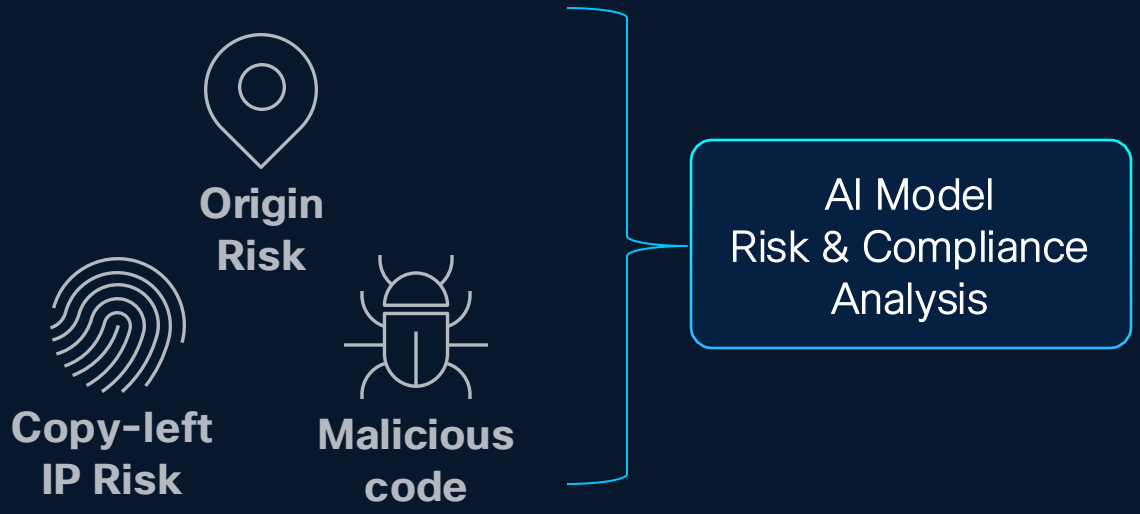
# AI Access – AI Supply Chain Risk Management

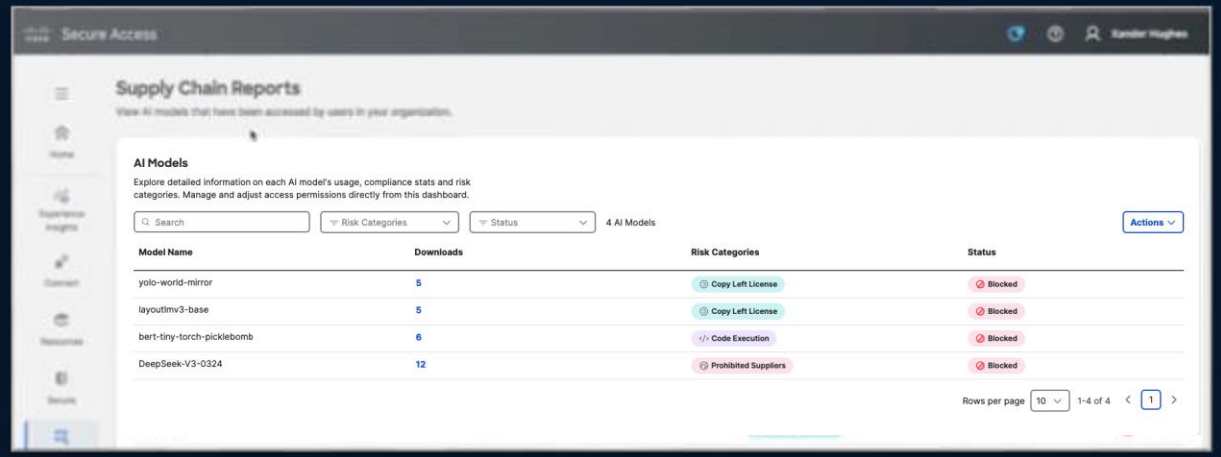
## Enable Safe AI Development

Don't block repos like Hugging Face – permit innovation with granular control.
Powered by "Foundation AI" – Each AI/ML Model is given a Risk Score




*This model runs arbitrary code.*



# AI Guardrails Demo

Organization
ABM Finance Co. - North America

Home

Products
AI Defense
Identity Intelligence
Firewall
Hypershield
Multicloud Defense
Secure Access
Secure Workload

Platform services
Favorites
Security Devices
Shared Objects
Platform Management

## Claim subscription

Claim subscriptions to activate instances in your organization.

Claim

### INTEGRATE IDENTITY PROVIDER (IDP)

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

Configure

### 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

### ACTIVATE SECURE WORKLOAD

Activate Secure Workload to bring security closer to your applications.

Activate

### ASSIGN ROLES

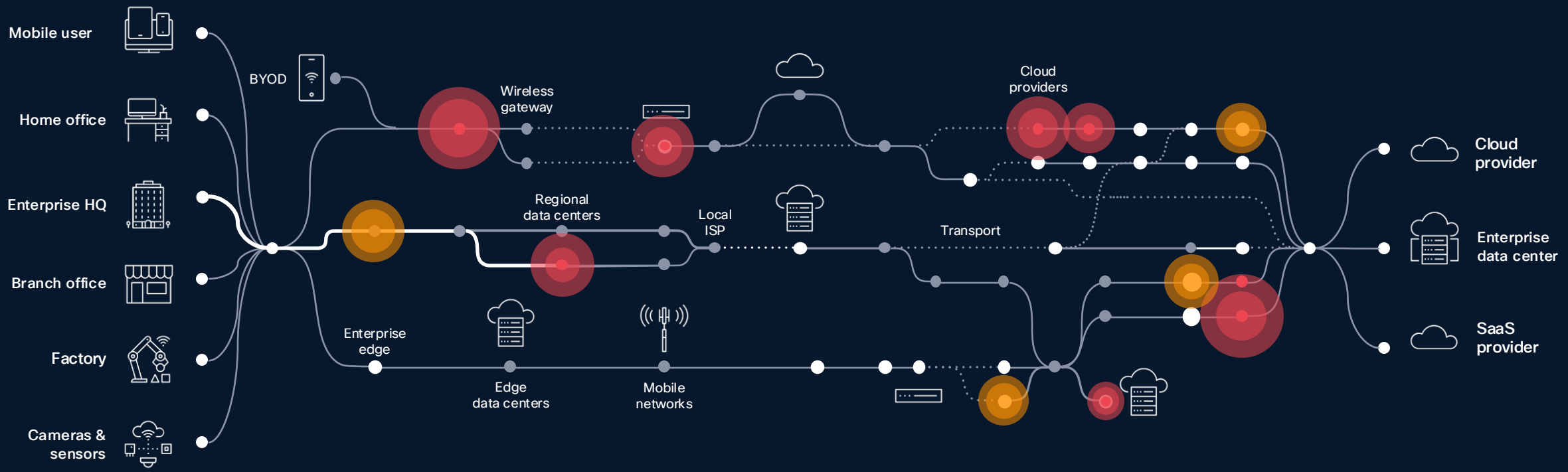
Create organization users and assign roles to control access.

Assign

Demo Flows

# Digital Experience Monitoring

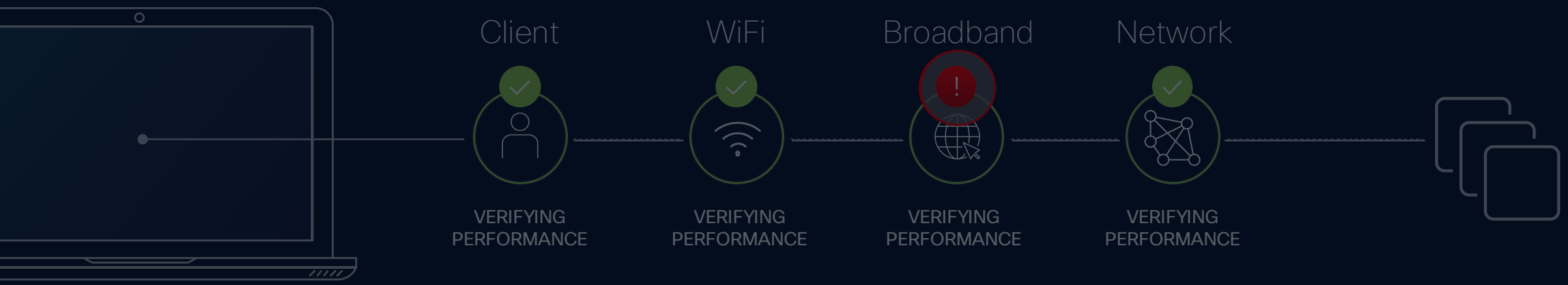
# Complexity Compromises Resilience



# Experience Insights

Node: 01.ca.comcast.net

| | |
|---|---|
| IP Address | 88.86.143.25 |
| Forwarding Loss | 32% (6 of 17 packets) |
| Ave. Response | 67.9 ms |

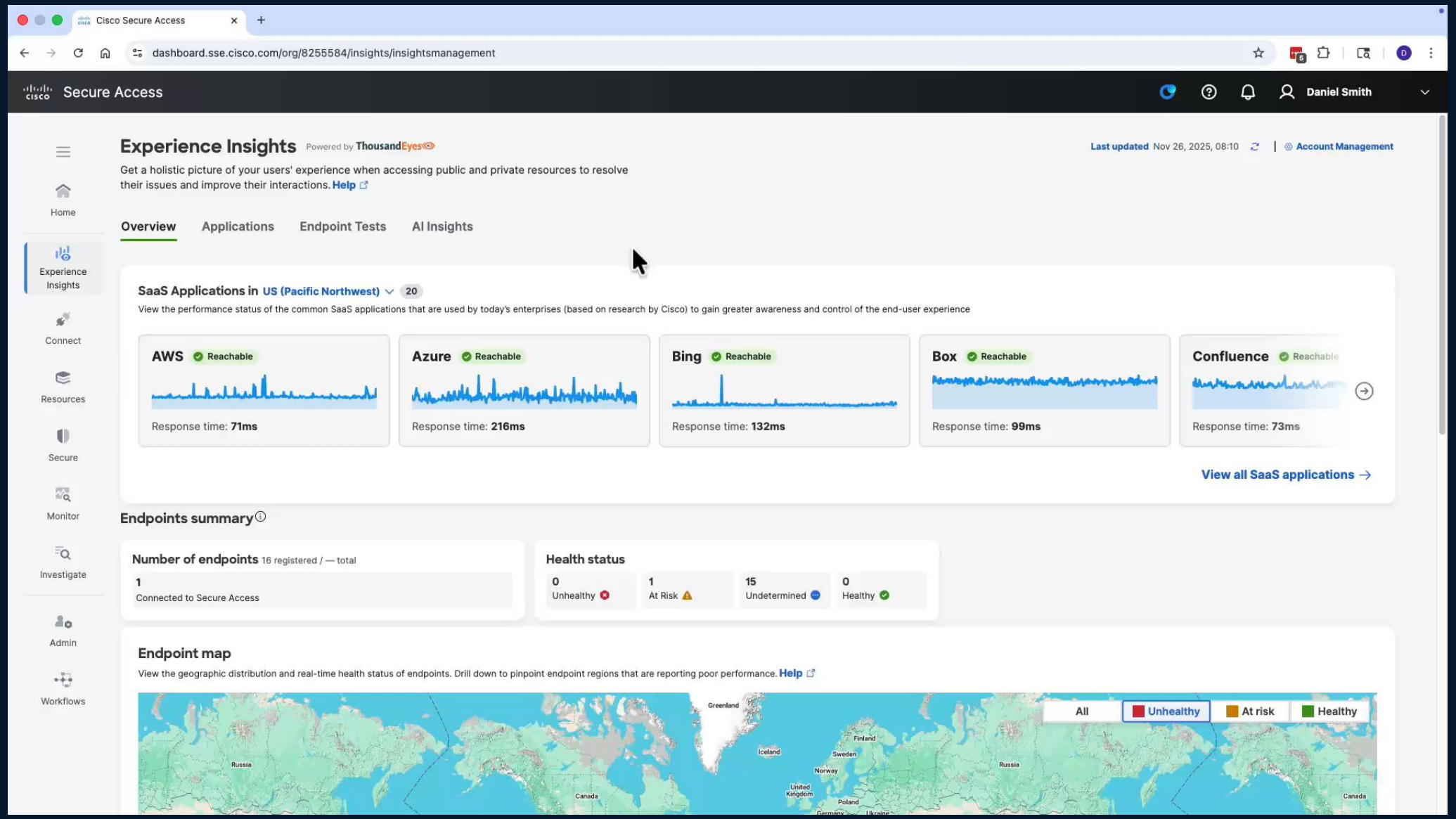


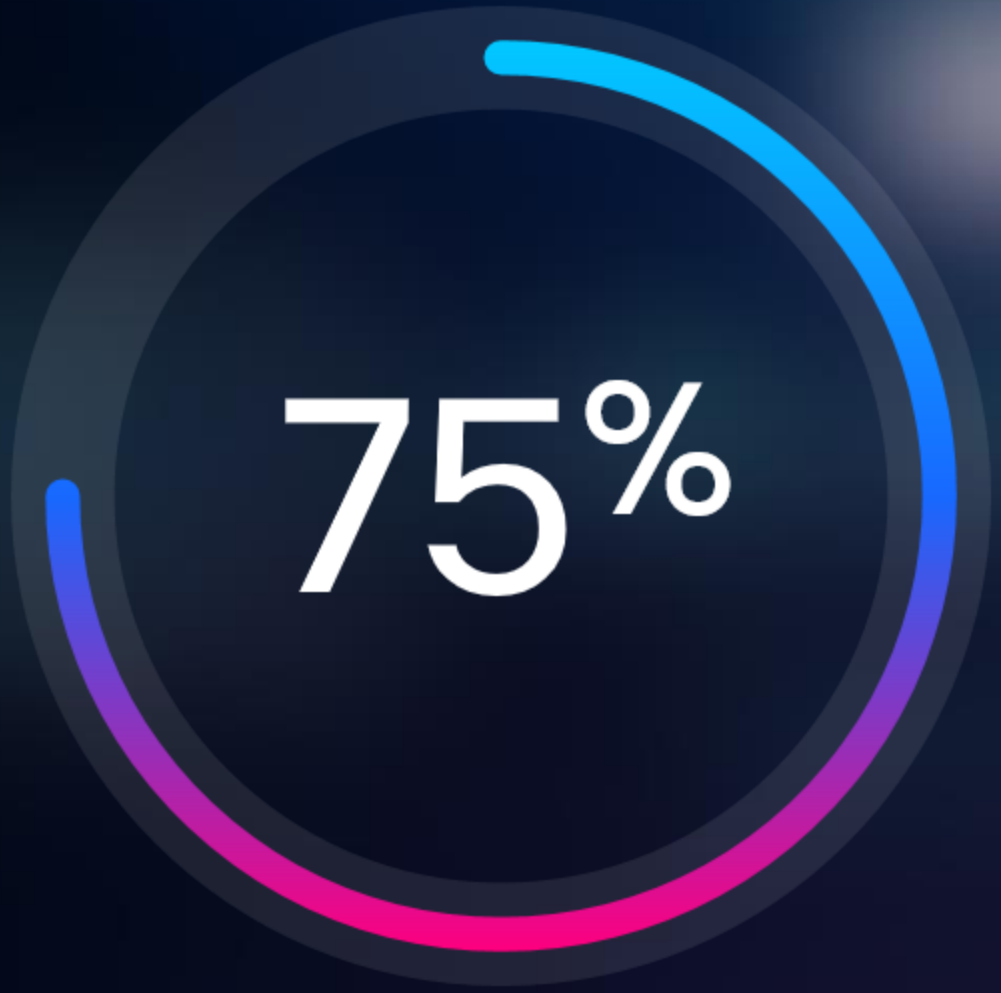



Depictions are examples only.

# Digital Experience Monitoring Demo

# Simplify Troubleshooting





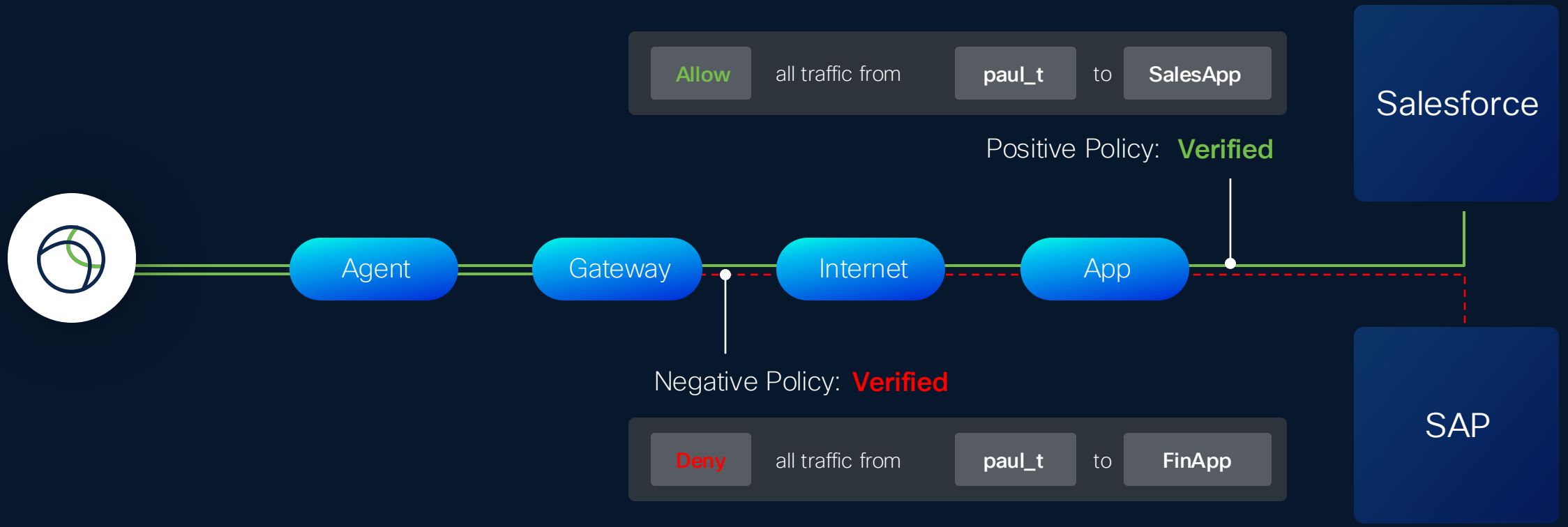

of outages are from misconfigurations

# Cisco AI Assistant & Policy Verification

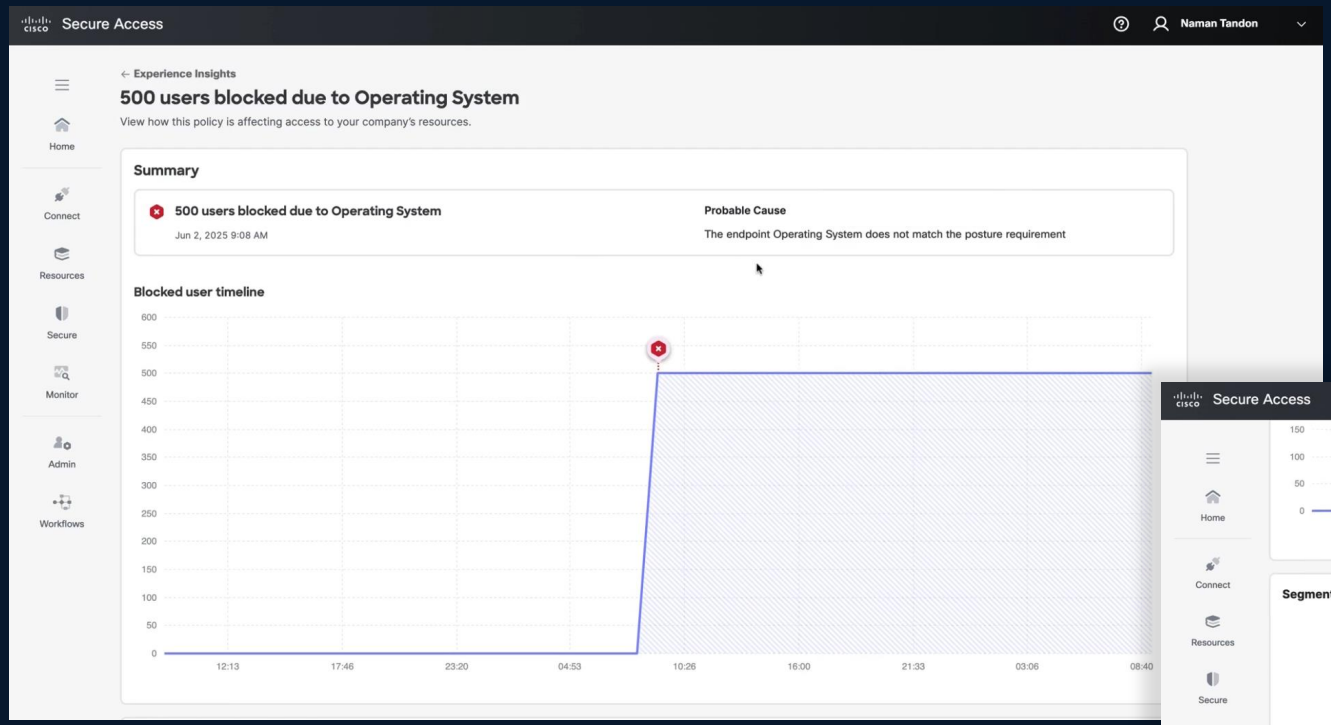
# Policy Verification Predicts the Impact of Changes

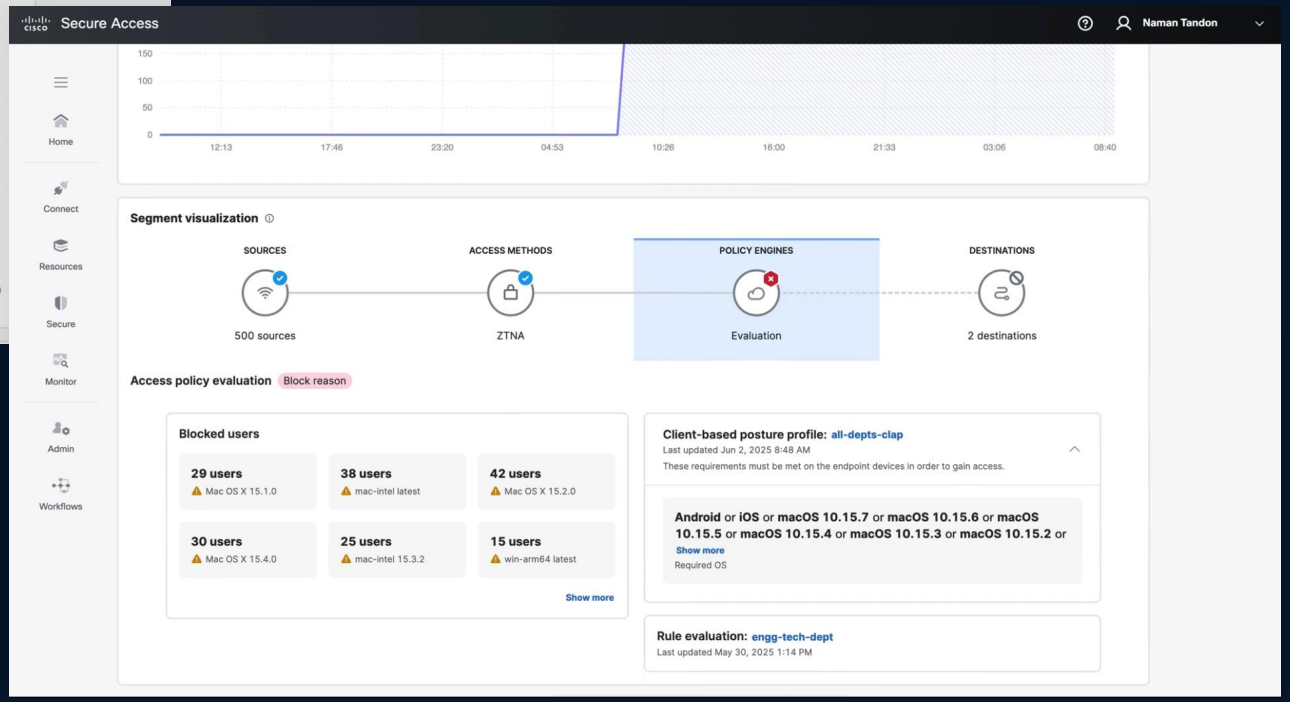

Depictions are examples only.

# Policy Verification Shows the Impact of Changes

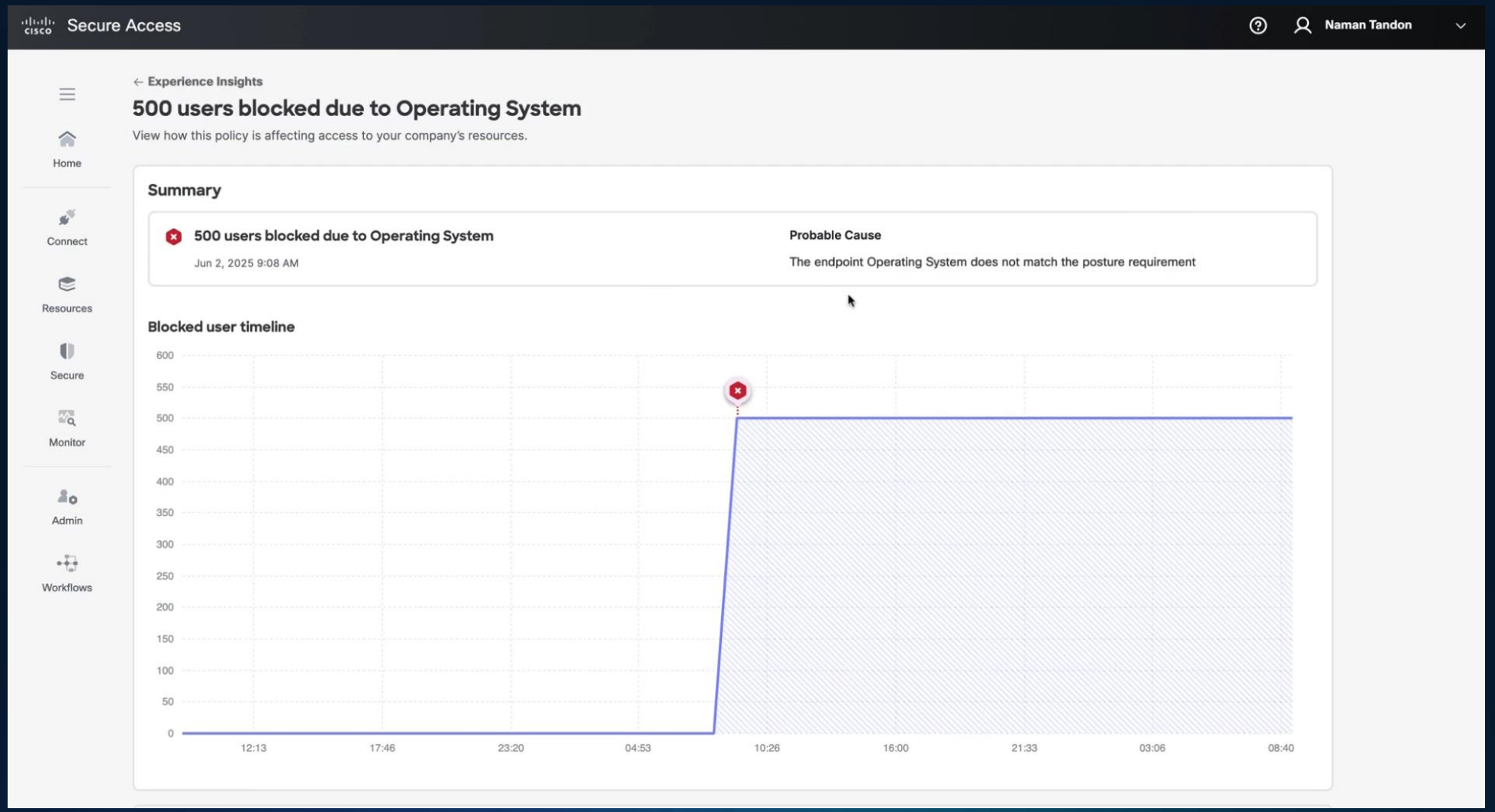


# Policy Verification

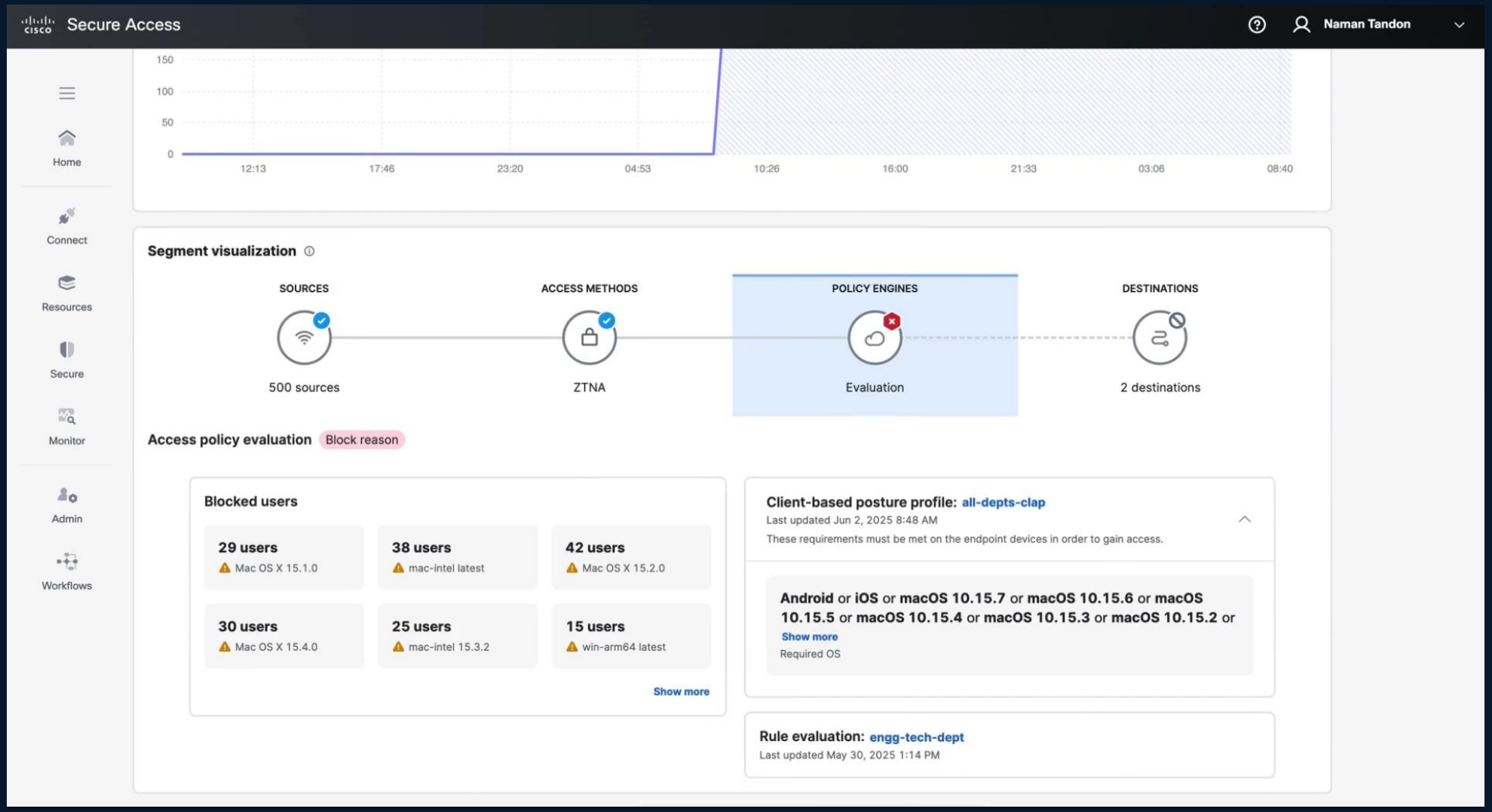


# Policy Verification

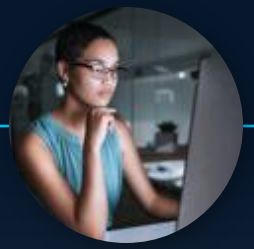


# Policy Verification



# Wrapping Up...

# Why Cisco Secure Access?



## Safer for everyone

Most comprehensive SSE solution with 3x the security capabilities in one cloud service

AI-first Security Service Edge

## Better for users

Seamless, secure access connecting your workforce to anything from anywhere

High-performance zero trust

## Easier for IT

Converged security in one console, one client, one cloud for simplified operations

Fast and efficient operations



cisco

# Recognized for SSE and ZTNA Leadership

FORRESTER®

Rated as Strong Performer in Forrester 2024 SSE Wave

Gartner Peer Insights™

SSE Category 2025
4.8/5 Rating


Rated First in CASB, SWG, DNS Internet Security


Customer Value Leader
Global Security Services Edge


ZTNA Overall Leader Award
KuppingerCole 2024



cisco

CISCO Connect

# Thank you