

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...



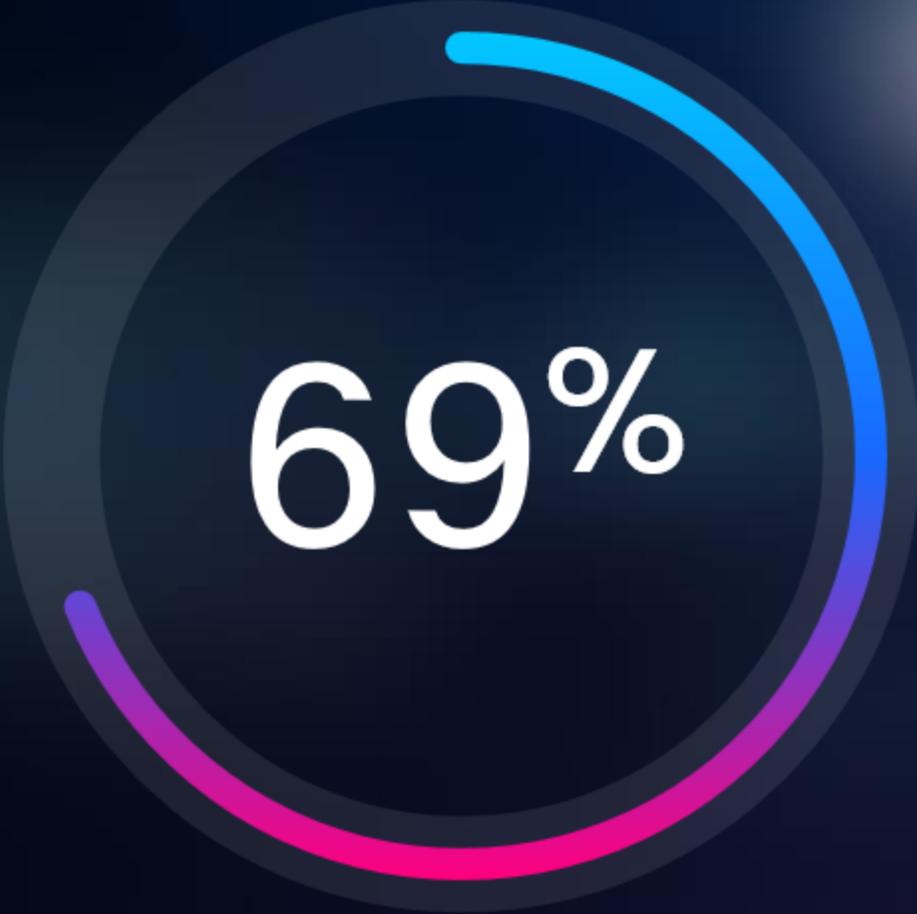
Safer for everyone
and everything



Better for users



Easier for IT



69%

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

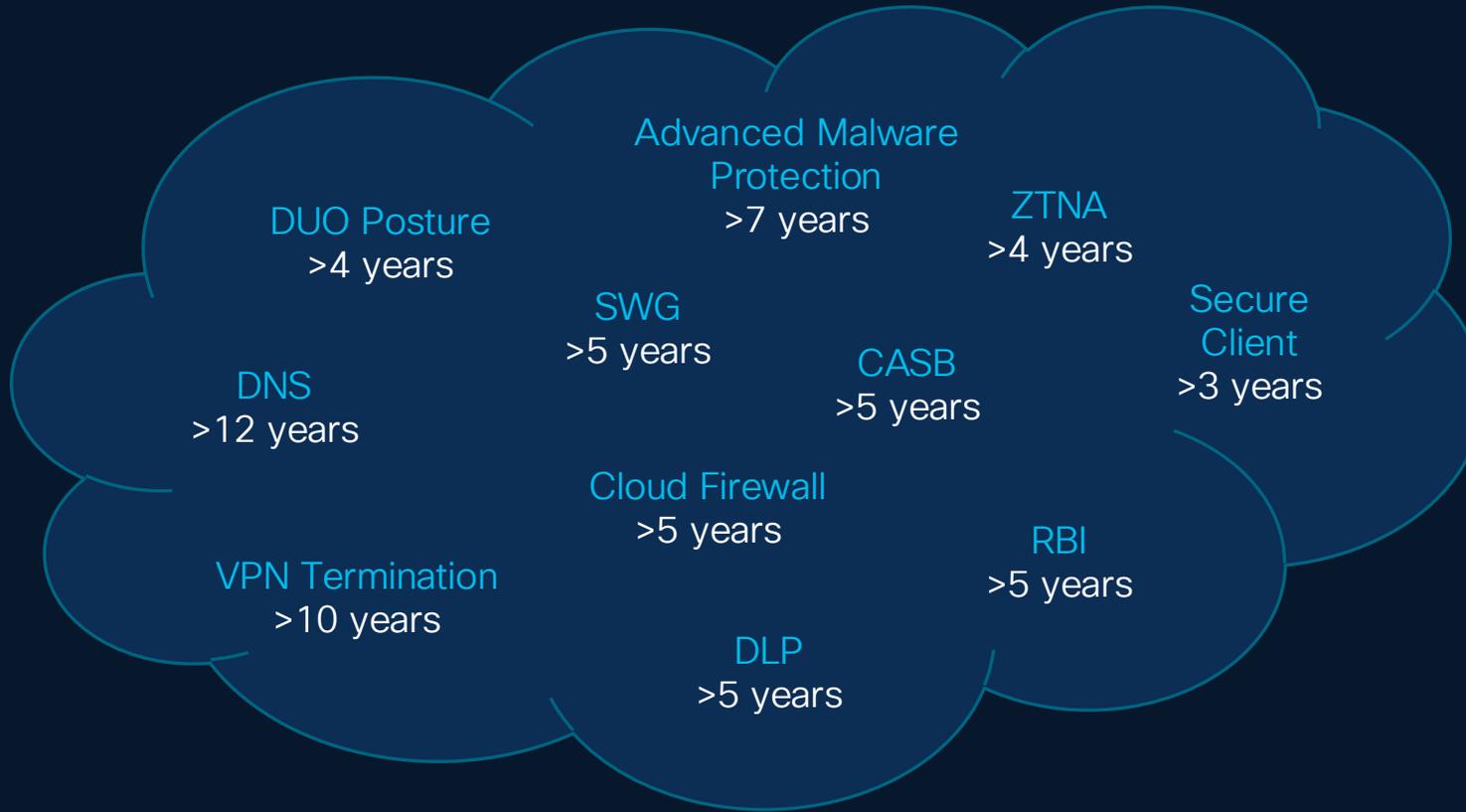
Cisco Secure Access

Extended SSE security grounded in “Identity first” zero trust



Cisco Secure Access

Proven cloud-native security converged into one service



Protecting 30,000+ customers | More than 220M endpoints

- Single Console
- Single Client
- Unified Policies

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



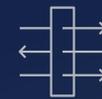
Secure Web Gateway (SWG)



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*

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

Add-on solutions



SD-WAN



XDR



DUO MFA/
SSO



CSPM

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

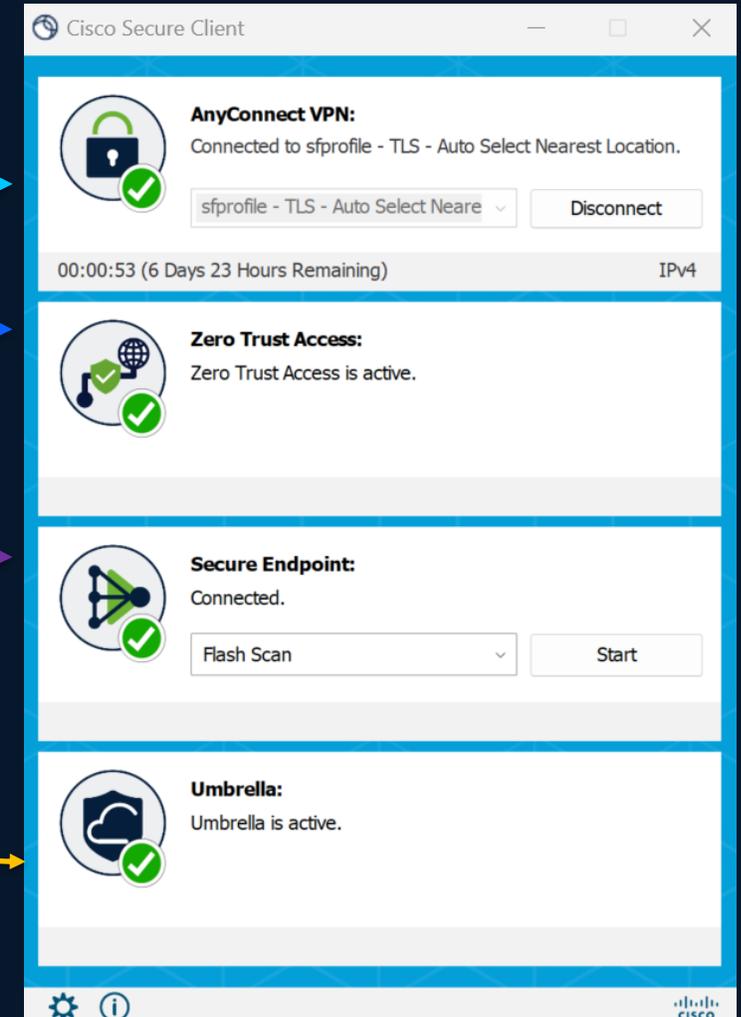
Secure Endpoint (AMP)

Roaming Module

Thousand Eyes (No UI)

Cloud Management Module (No UI)

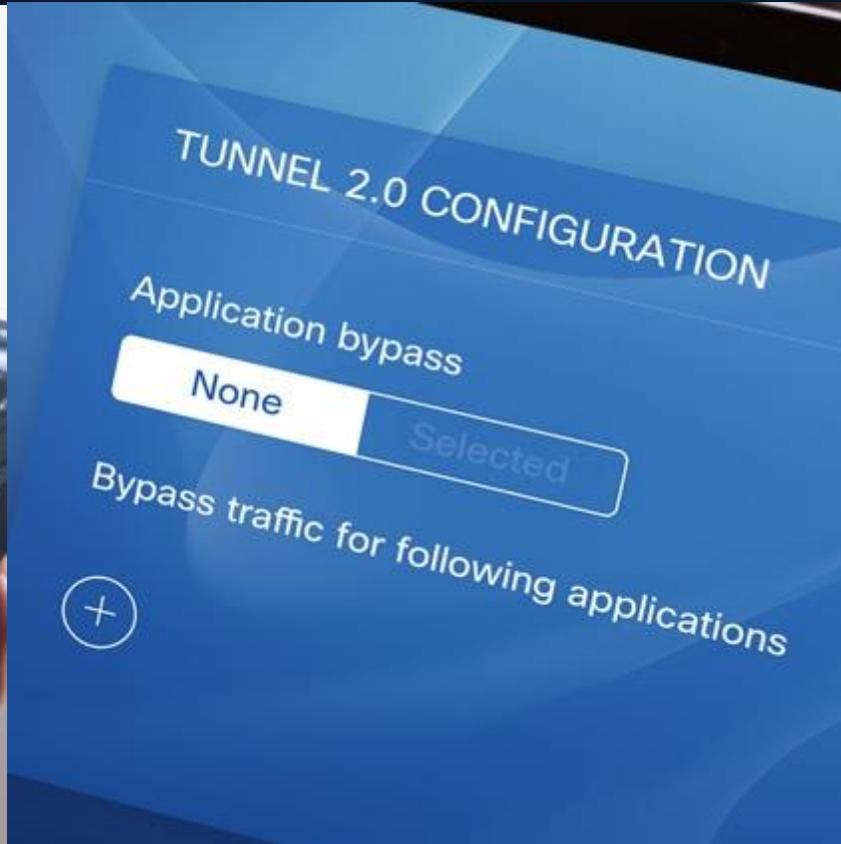
Diagnostic and Reporting (DART)



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

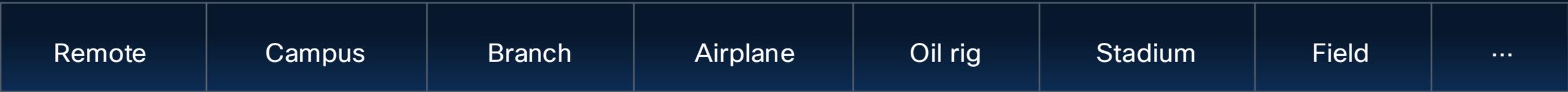


Zero Trust Access

The Complexity of a Distributed Edge



The Distributed Edge Complicates Zero Trust



The Power of a Unified Platform

Tight integrations across Cisco portfolio

High performance



Identity-driven security



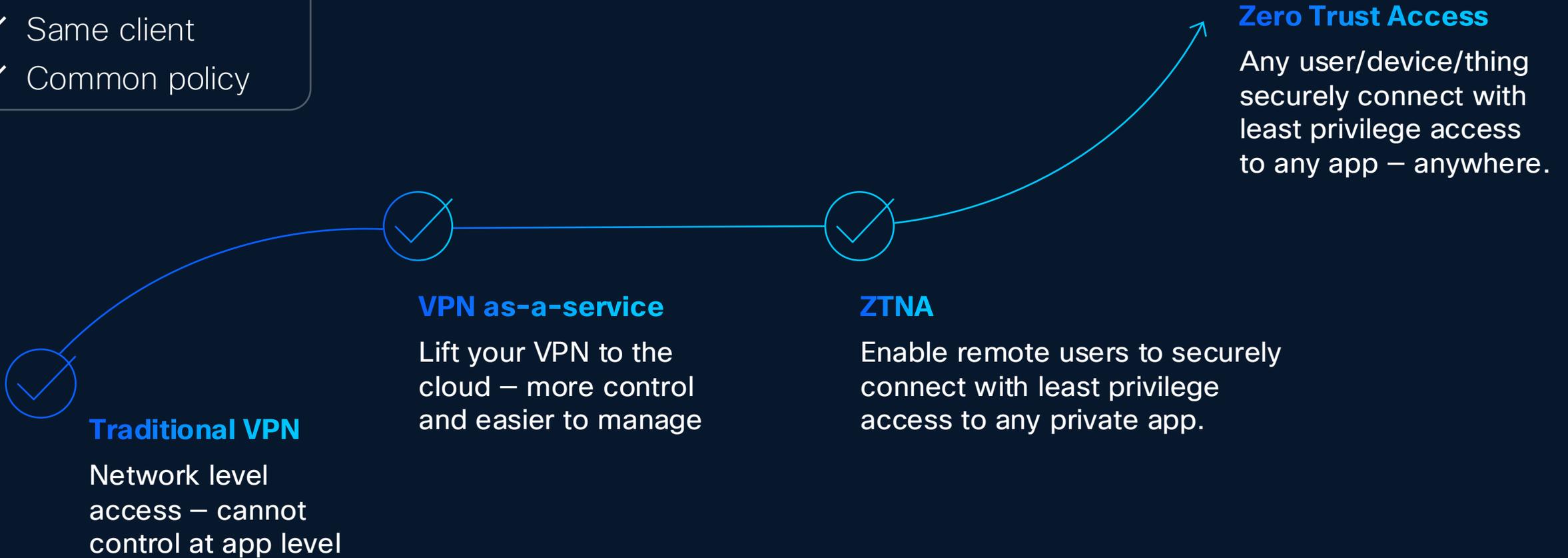
Resilience



AI-powered, highly optimized operations

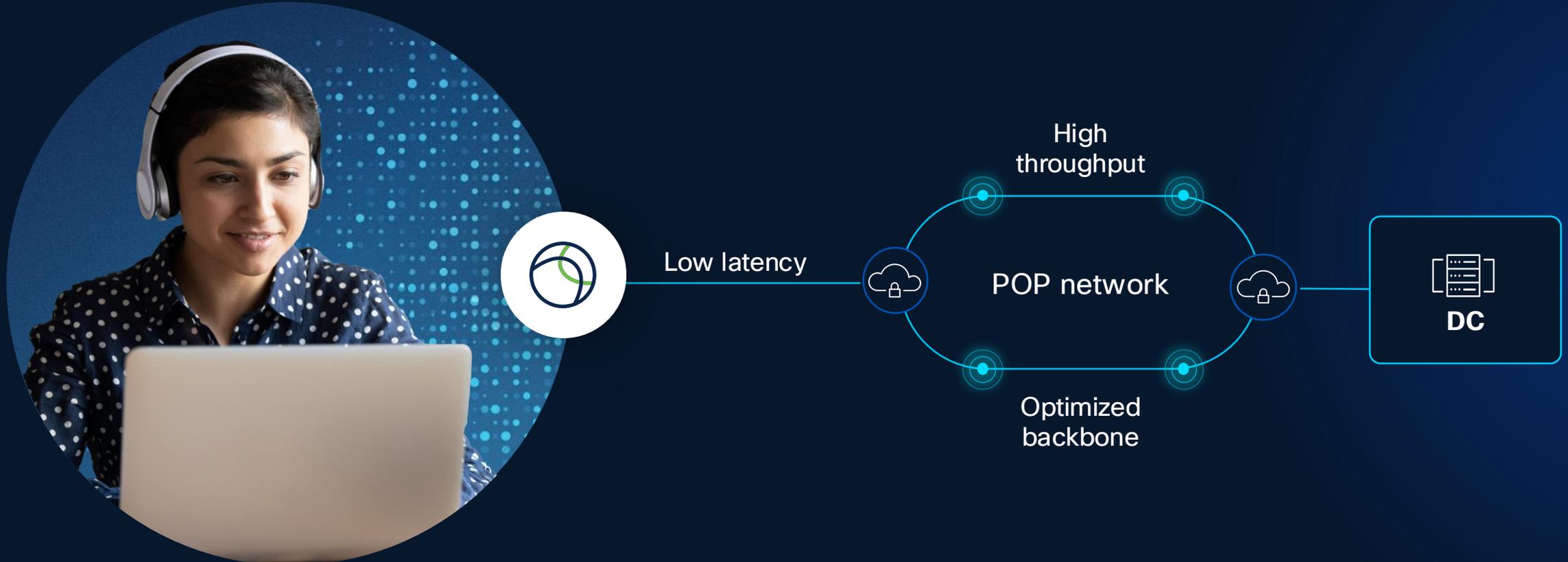
Flexible Journey to Zero Trust Access

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



Cisco's Modern PoP Architecture Optimizes User Experience

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





CAMPUS



HOME



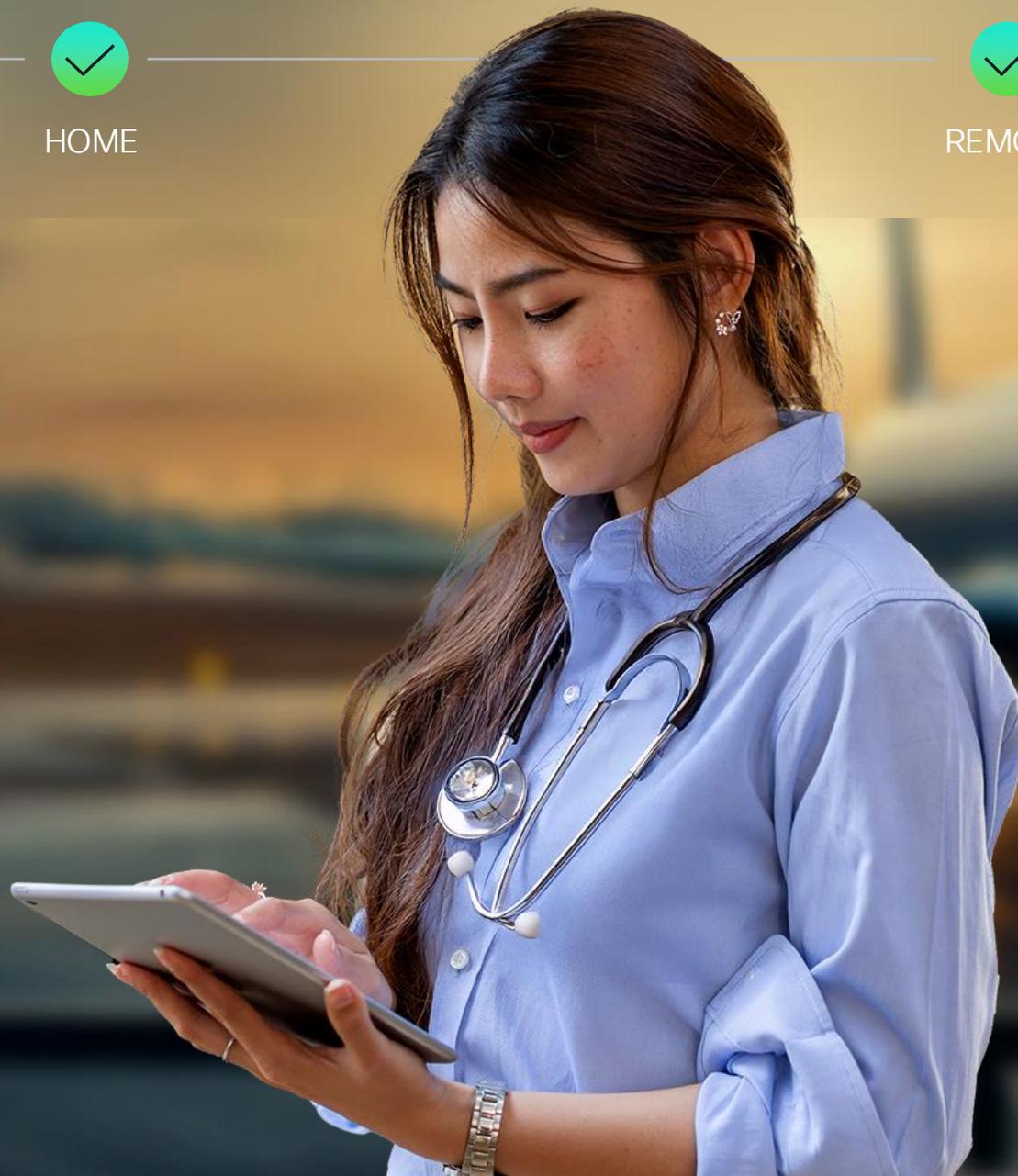
REMOTE

Hybrid Private Access

Same user experience in office and remote

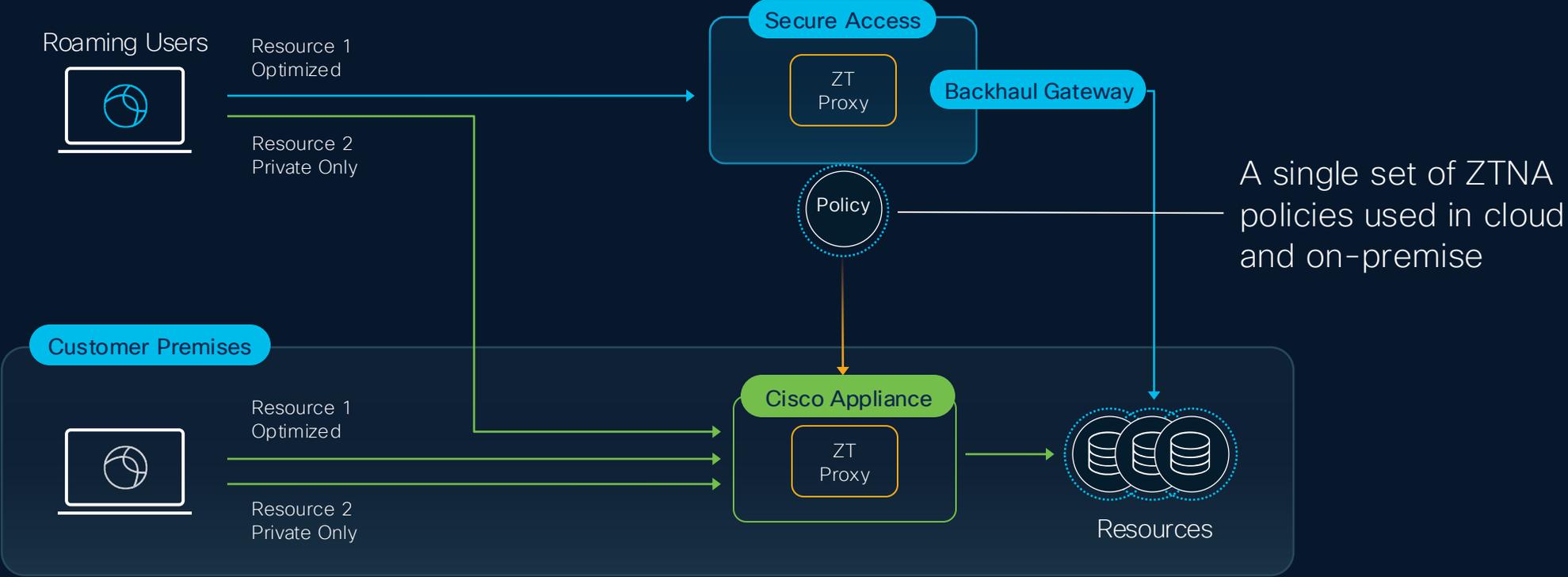
Cloud or local enforcement options by app

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

The screenshot displays the Cisco Security Cloud Control interface for configuring a policy. The main header is "Security Cloud Control" with the Cisco logo. A navigation menu on the left includes "Objects", "Security Devices", and "Secure Connections".

The main content area is titled "1 Specify Access" and includes a "Help" link. It features two action options: "Allow" (with a green checkmark icon) and "Block" (with a red slash icon). Below these are fields for "From" (sources) and "To" (destinations). The "From" field contains "Neil Patel (neipatel@ssep.onmicrosoft.com)" and the "To" field contains "Excalidraw".

Under "Endpoint Requirements", there is a section for "Zero-Trust Client-based Posture Profile" (Custom) with "Profile: Open" and "Requirements: None". It also lists "Private Resources: Excalidraw, SpeedTest-firewall".

A diagram at the bottom illustrates the connection flow: a user icon connects "via local network" to a server icon, which is then connected to another server icon. A green circle with a refresh icon highlights the server icon.

Overlaid on the top right is a callout box with the following text:

- Zero-trust connections**
Allow endpoints to connect to this resource from outside your network without requiring a VPN connection. [Help](#)
- Client-based connection**
Allow connections from endpoints that have the Secure Client installed. Enable this option for maximum control over endpoint security requirements (posture).

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

Secure Access with Enterprise Browser

Zero Trust Access to Private Apps and Internet Apps

Enterprise Browser



Unmanaged and Managed Endpoints

- 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

Cisco Secure Access

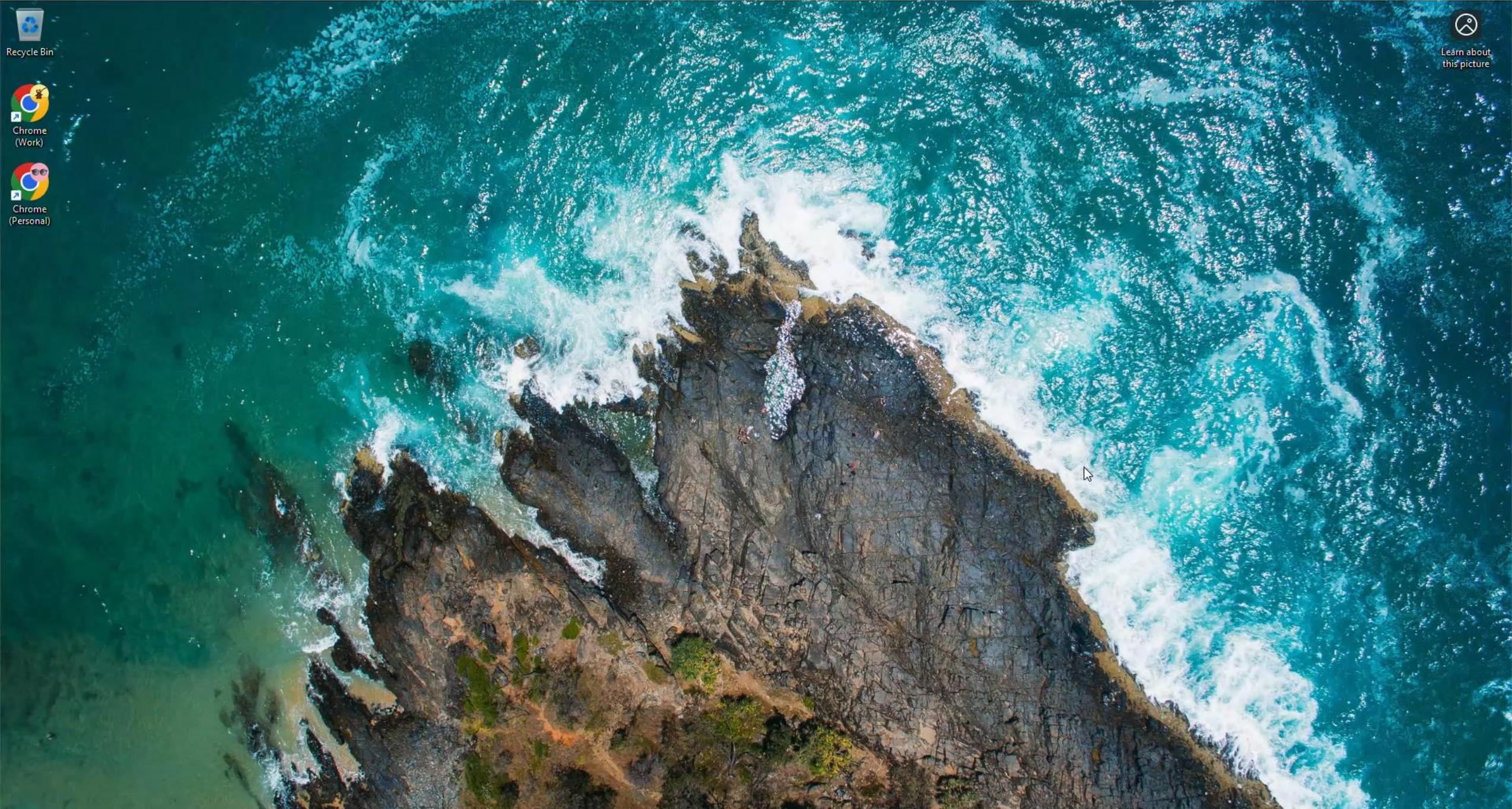


Secure Service Edge (SSE)

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



Private Applications



Learn about this picture

Recycle Bin

Chrome (Work)

Chrome (Personal)



Search



ENG
CMK



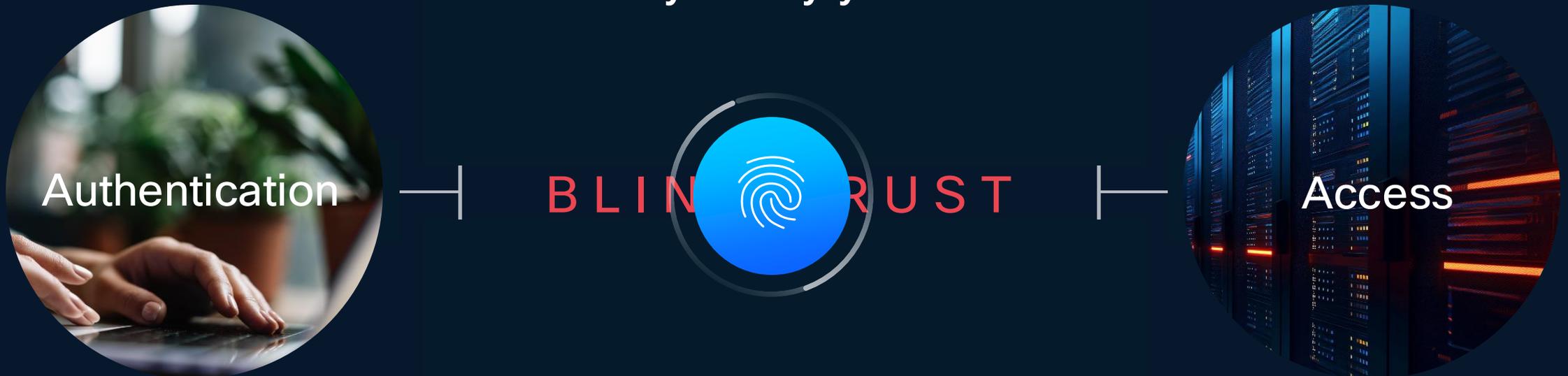
11:35 AM
12/13/2024



Identity Intelligence

Identity Intelligence

Continuously assess you are
who you say you are



Works with existing IDPs



Cisco
Duo IAM

Cisco
Secure
Access

Cisco
Secure
Firewall

User Trust Level



TRUSTED

NEUTRAL

UNTRUSTED

- 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

<h4>Users ⓘ</h4> <div style="display: flex; justify-content: space-around; margin-top: 10px;"> <div style="text-align: center;"> <p style="font-size: 24px; color: red;">22</p> <p>Untrusted users</p> </div> <div style="text-align: center;"> <p style="font-size: 24px;">4253</p> <p>Neutral users</p> </div> <div style="text-align: center;"> <p style="font-size: 24px;">43</p> <p>Trusted users</p> </div> </div>	<h4>MFA Status ⓘ</h4> <table border="1" style="width: 100%; border-collapse: collapse; margin-top: 10px;"> <tr> <td style="text-align: center;">159 No MFA</td> <td style="text-align: center;">21 No strong MFA</td> <td style="text-align: center;">22 Weak MFA</td> </tr> <tr> <td style="text-align: center;">1 MFA Flood</td> <td style="text-align: center;">1 Telecom MFA Limit Reac</td> <td style="text-align: center;">3 Admins with Weak MFA</td> </tr> </table>	159 No MFA	21 No strong MFA	22 Weak MFA	1 MFA Flood	1 Telecom MFA Limit Reac	3 Admins with Weak MFA	<h4>Security Event Trends ⓘ</h4> <p style="margin-top: 10px;">30 ↗ 1% Weak MFA, used to successfully sign in</p> <p>20 ↗ 15% Unused application for a user</p>
159 No MFA	21 No strong MFA	22 Weak MFA						
1 MFA Flood	1 Telecom MFA Limit Reac	3 Admins with Weak MFA						

Usage monitoring Last 24 Hours

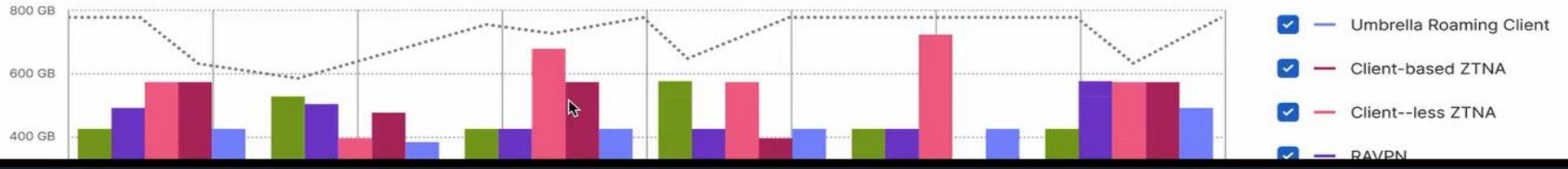
Total usage
Usage data - delayed up to 30 min.

765.59 GB Total traffic

390 GB ↘ More than last month

265.59 GB Sent

390 GB ↗ More than last month



AI Security

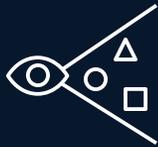
Show of Hands...

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

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:



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.

Copy.ai

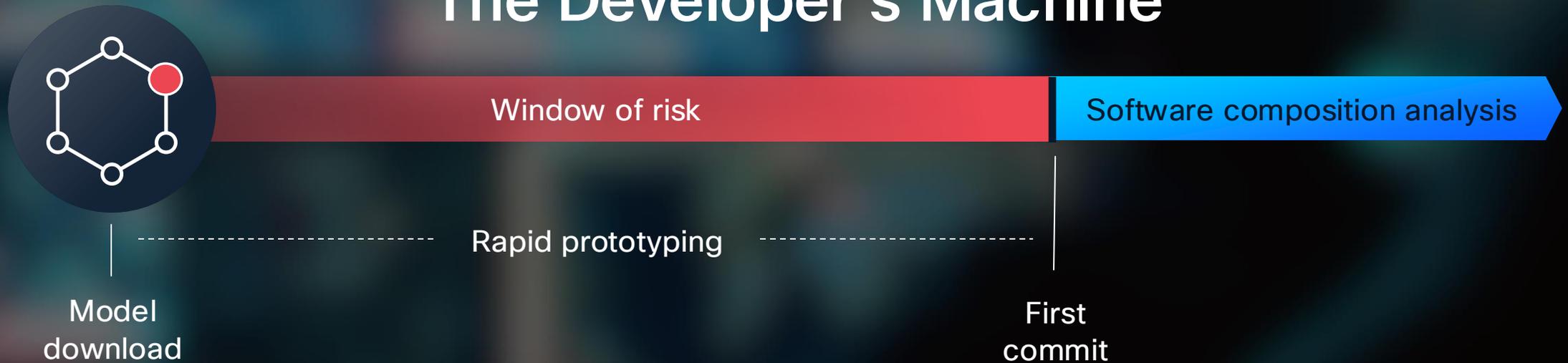
Copilot

OpenAI

Gemini

Using AI apps

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



Stop Risky Models Before They Start



Malicious code



IP compliance



Origin compliance

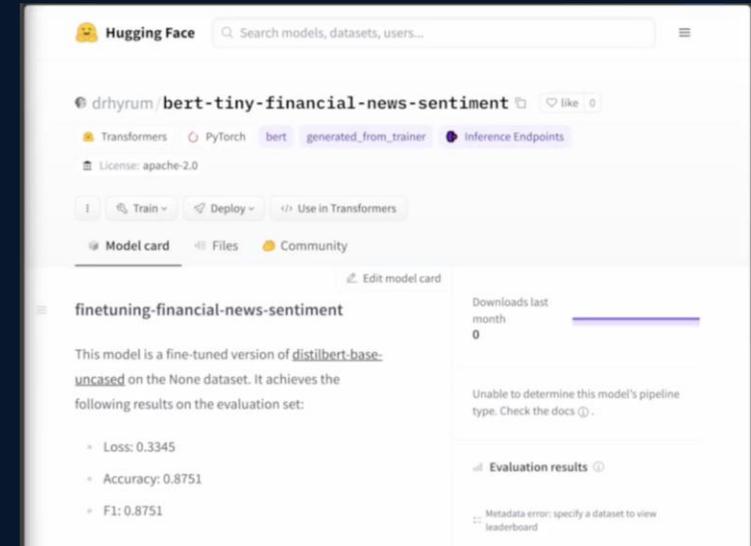
Pre-use enforcement

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 Model Risk & Compliance Analysis

Model Name	Downloads	Risk Categories	Status
yolo-world-mirror	5	Copy Left License	Blocked
layoutlm3-base	5	Copy Left License	Blocked
bert-tiny-torch-picklebomb	6	Code Execution	Blocked
DeepSeek-V3-0324	12	Prohibited Suppliers	Blocked

AI Guardrails Demo

Organization
ABM Finance Co. - North America

Home

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

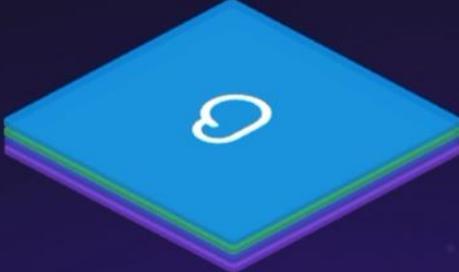
- Platform services
- Favorites
 - Security Devices
 - Shared Objects
 - Platform Management

Demo Flows

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](#)

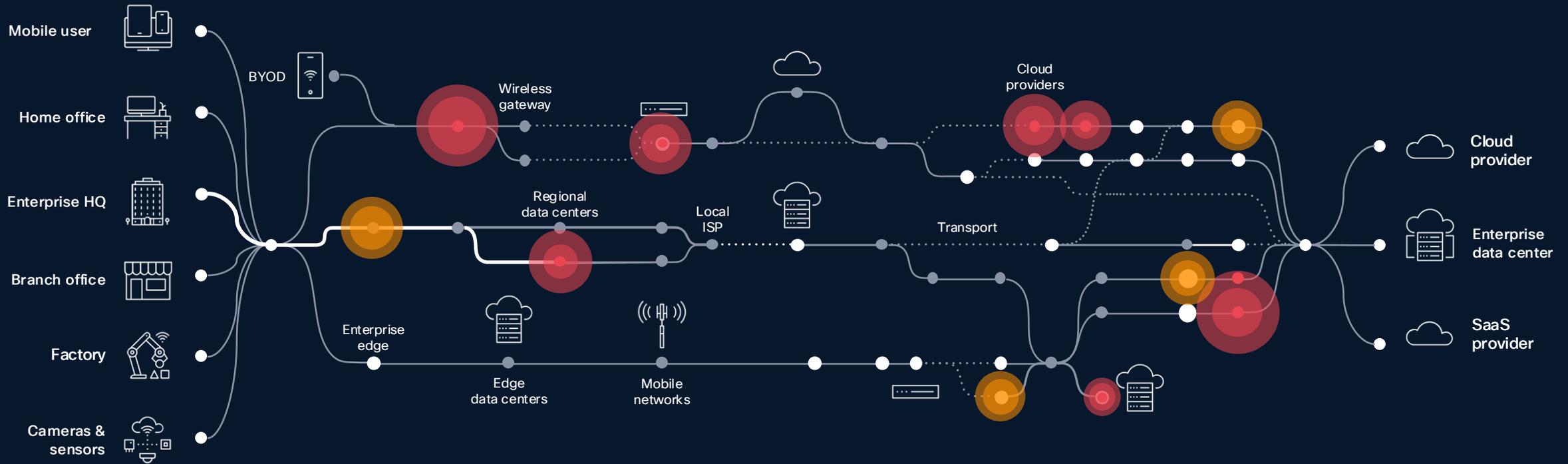
ASSIGN ROLES ...

Create organization users and assign roles to control access.

[Assign](#)

Digital Experience Monitoring

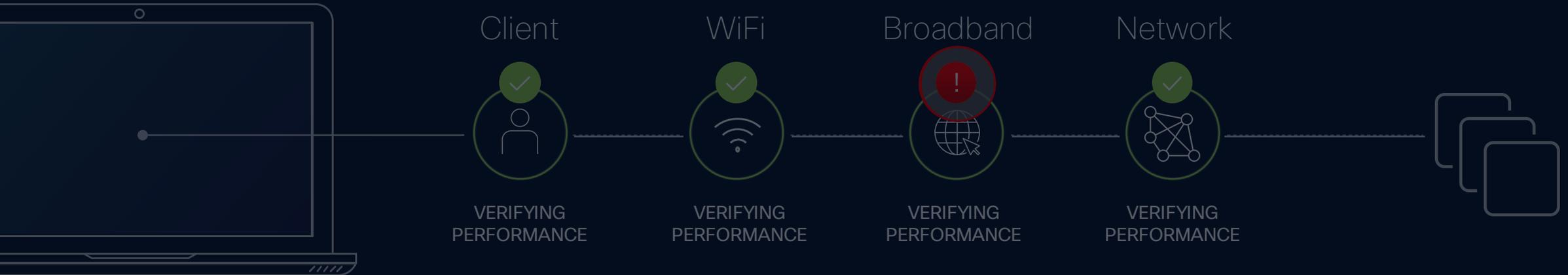
Complexity Compromises Resilience



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



Digital Experience Monitoring Demo

Simplify Troubleshooting

The screenshot shows the Cisco Secure Access Experience Insights dashboard. The browser address bar displays the URL: `dashboard.sse.cisco.com/org/8255584/insights/insightsmanagement`. The user is logged in as Daniel Smith. The dashboard is titled "Experience Insights" and is powered by ThousandEyes. It provides a holistic view of user experience for public and private resources.

SaaS Applications in US (Pacific Northwest) (20 total)

View the performance status of the common SaaS applications that are used by today's enterprises (based on research by Cisco) to gain greater awareness and control of the end-user experience

Application	Status	Response Time
AWS	Reachable	71ms
Azure	Reachable	216ms
Bing	Reachable	132ms
Box	Reachable	99ms
Confluence	Reachable	73ms

[View all SaaS applications](#)

Endpoints summary

Number of endpoints: 16 registered / — total

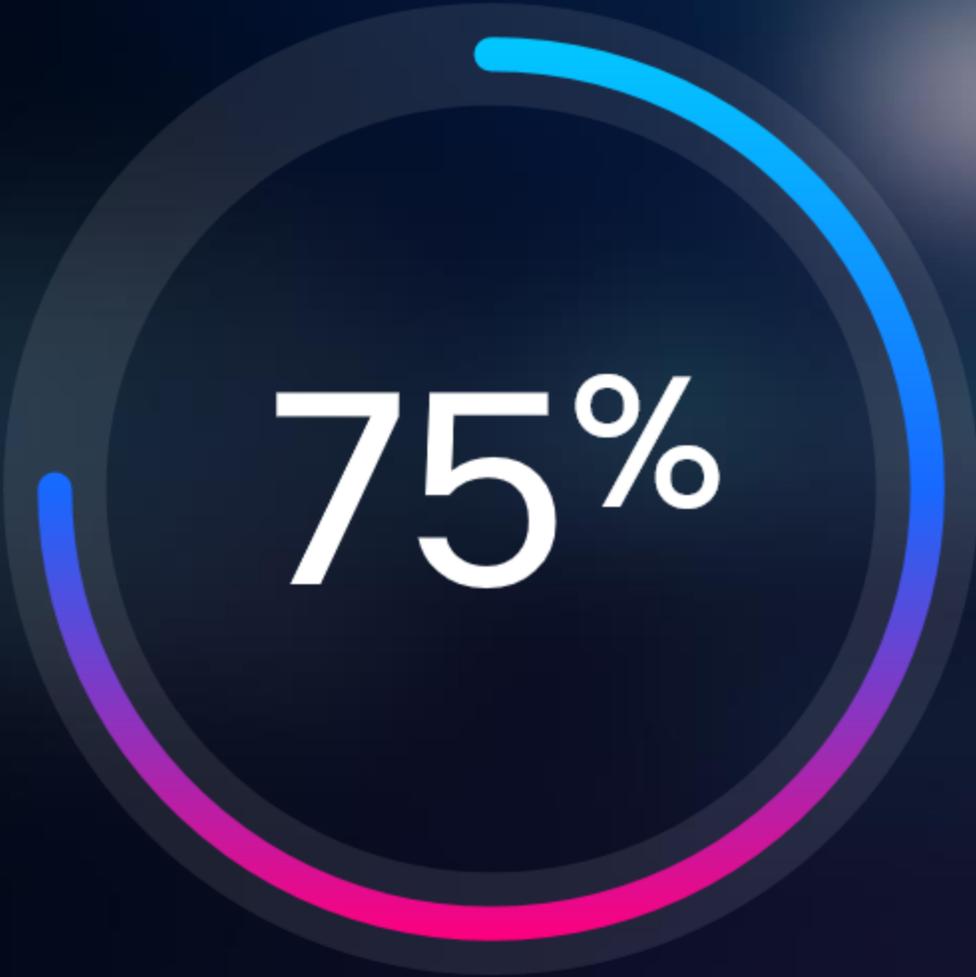
- 1 Connected to Secure Access

Health status:

- 0 Unhealthy
- 1 At Risk
- 15 Undetermined
- 0 Healthy

Endpoint map

View the geographic distribution and real-time health status of endpoints. Drill down to pinpoint endpoint regions that are reporting poor performance.



75%

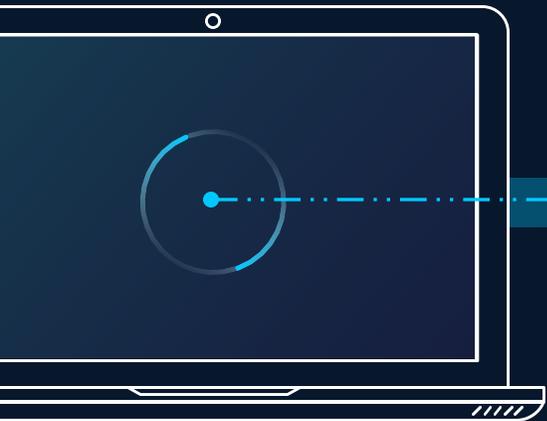
of outages are from
misconfigurations

Cisco AI Assistant & Policy Verification

Policy Verification Predicts the Impact of Changes

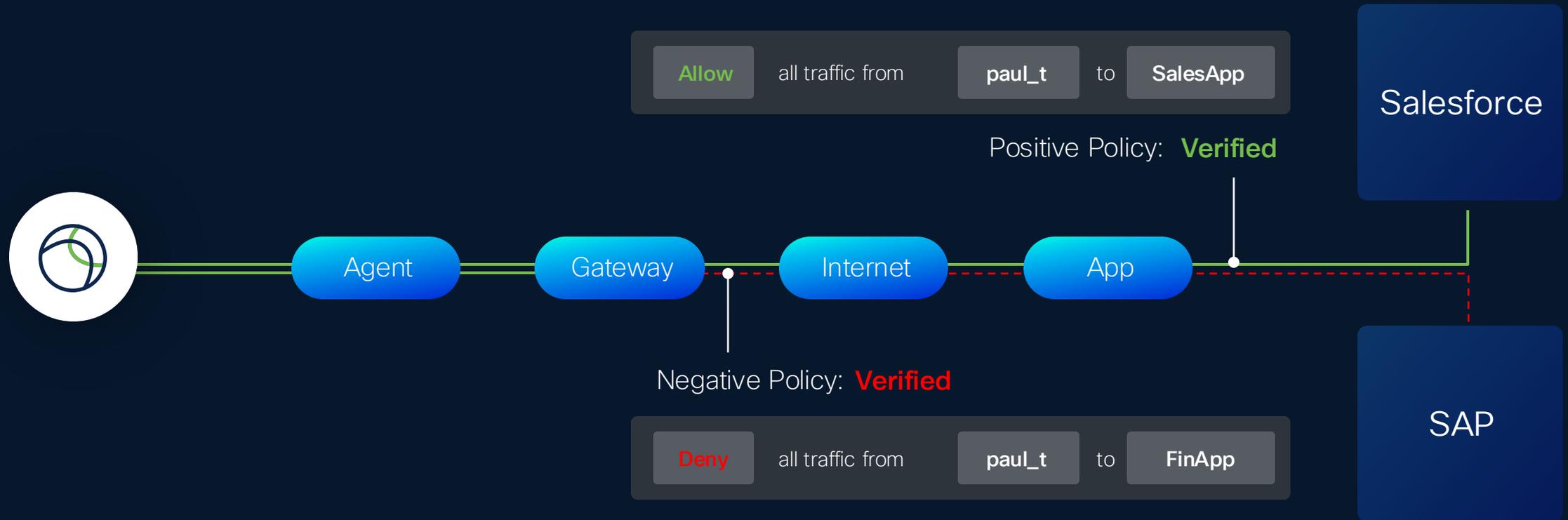
Positive Policy: **Verified**

Allow all traffic from **paul_t** to **SalesApp**

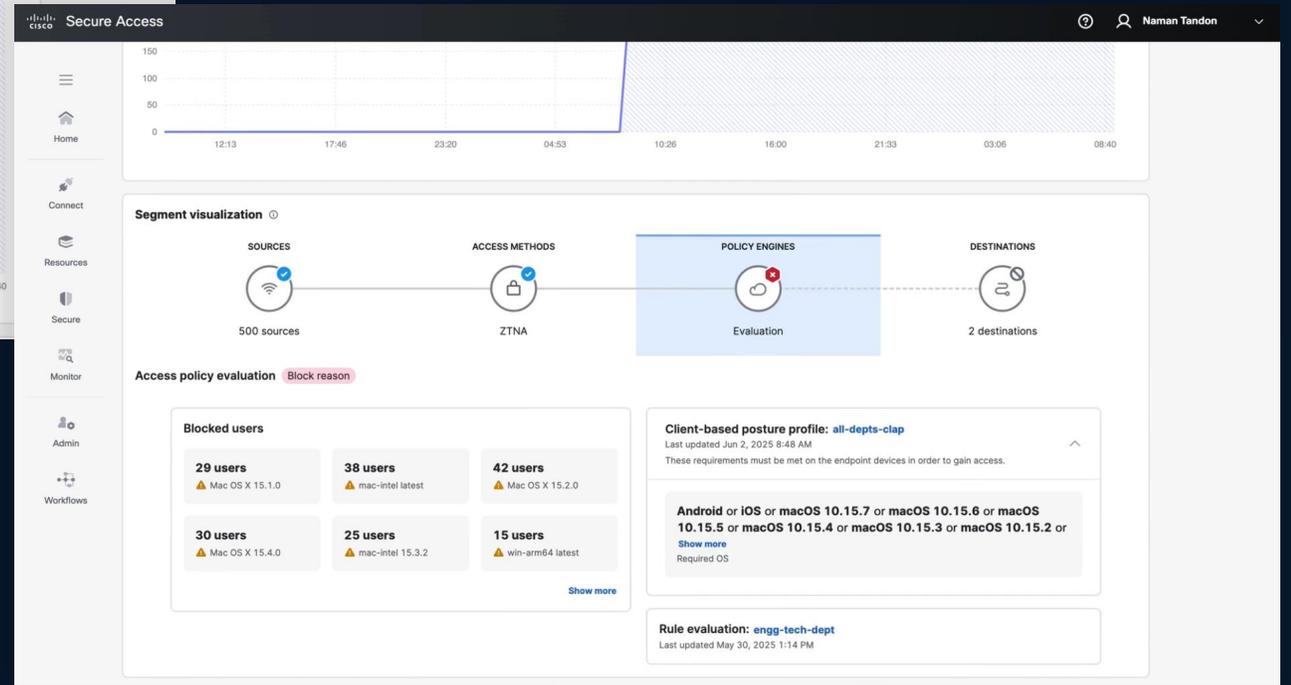
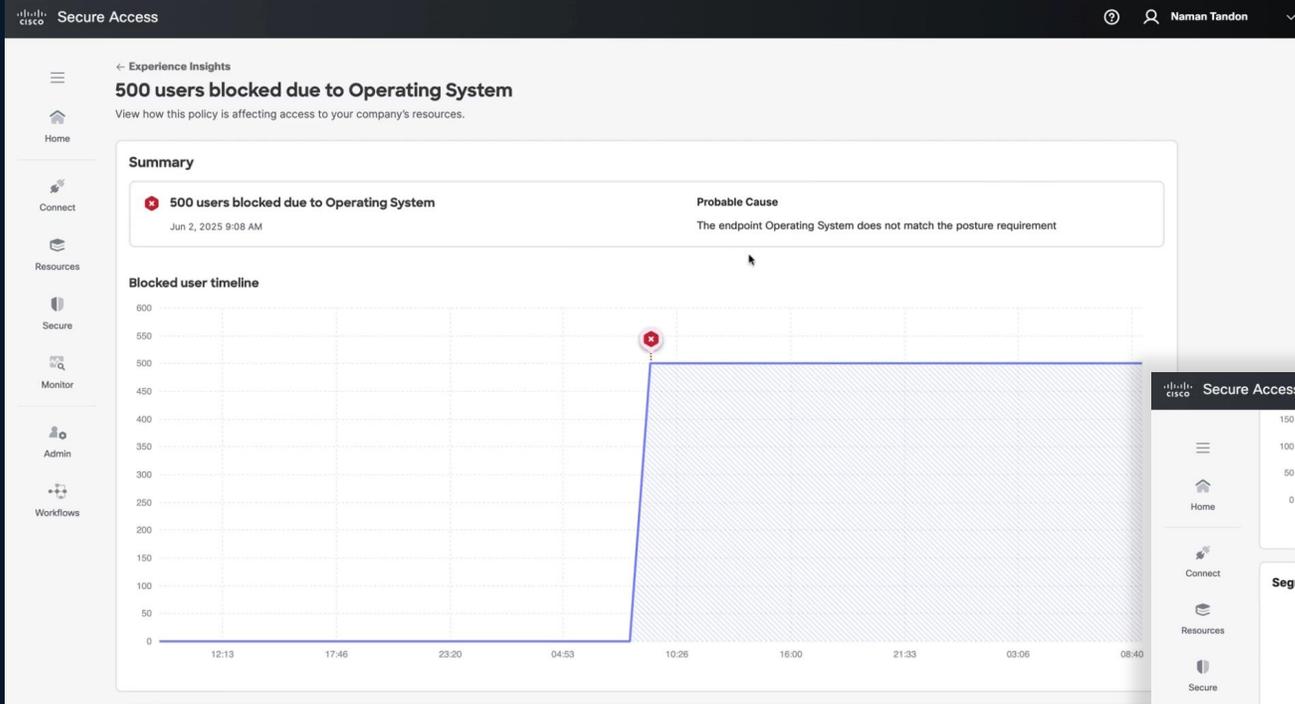


Depictions are examples only.

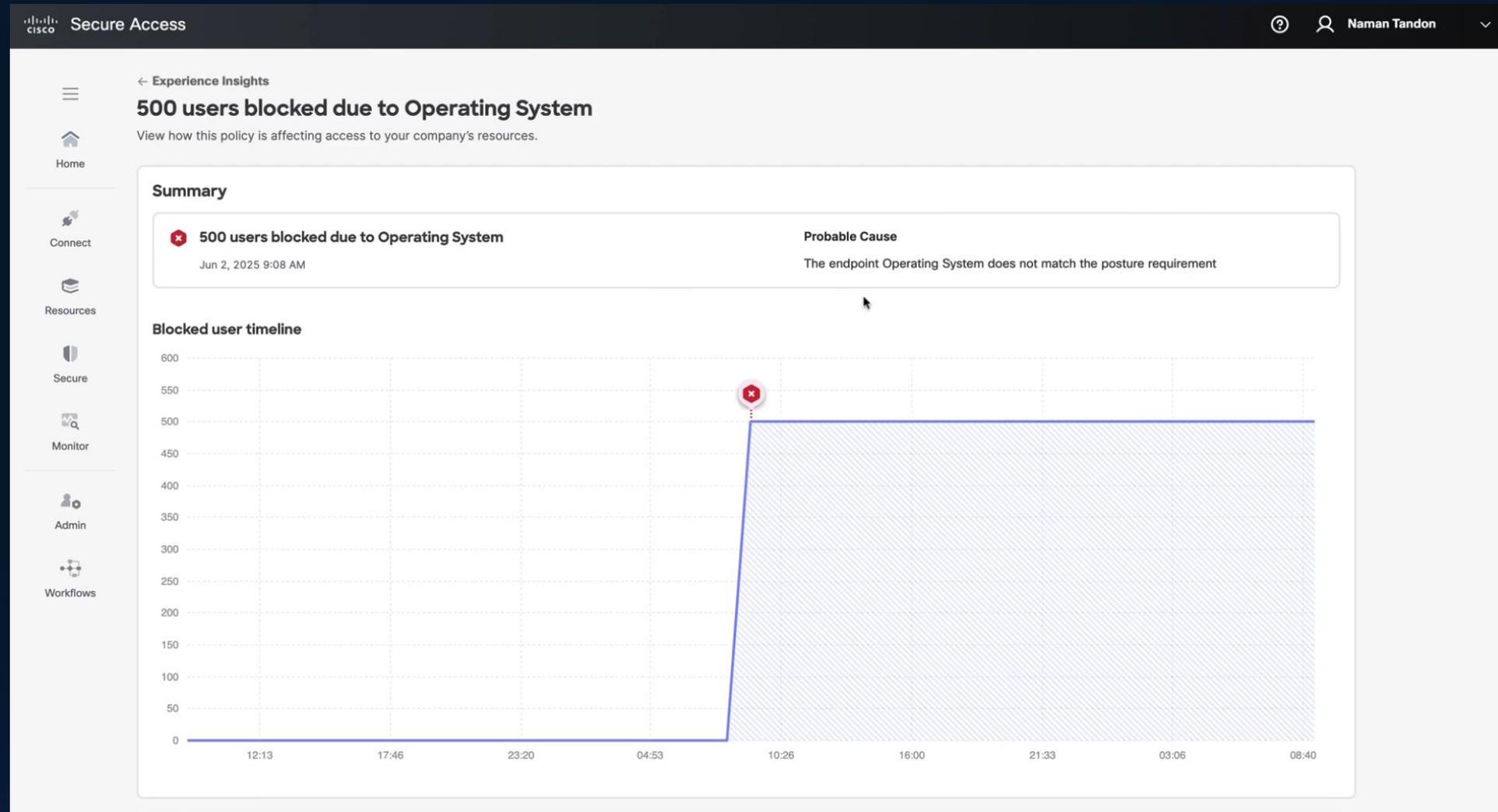
Policy Verification Shows the Impact of Changes



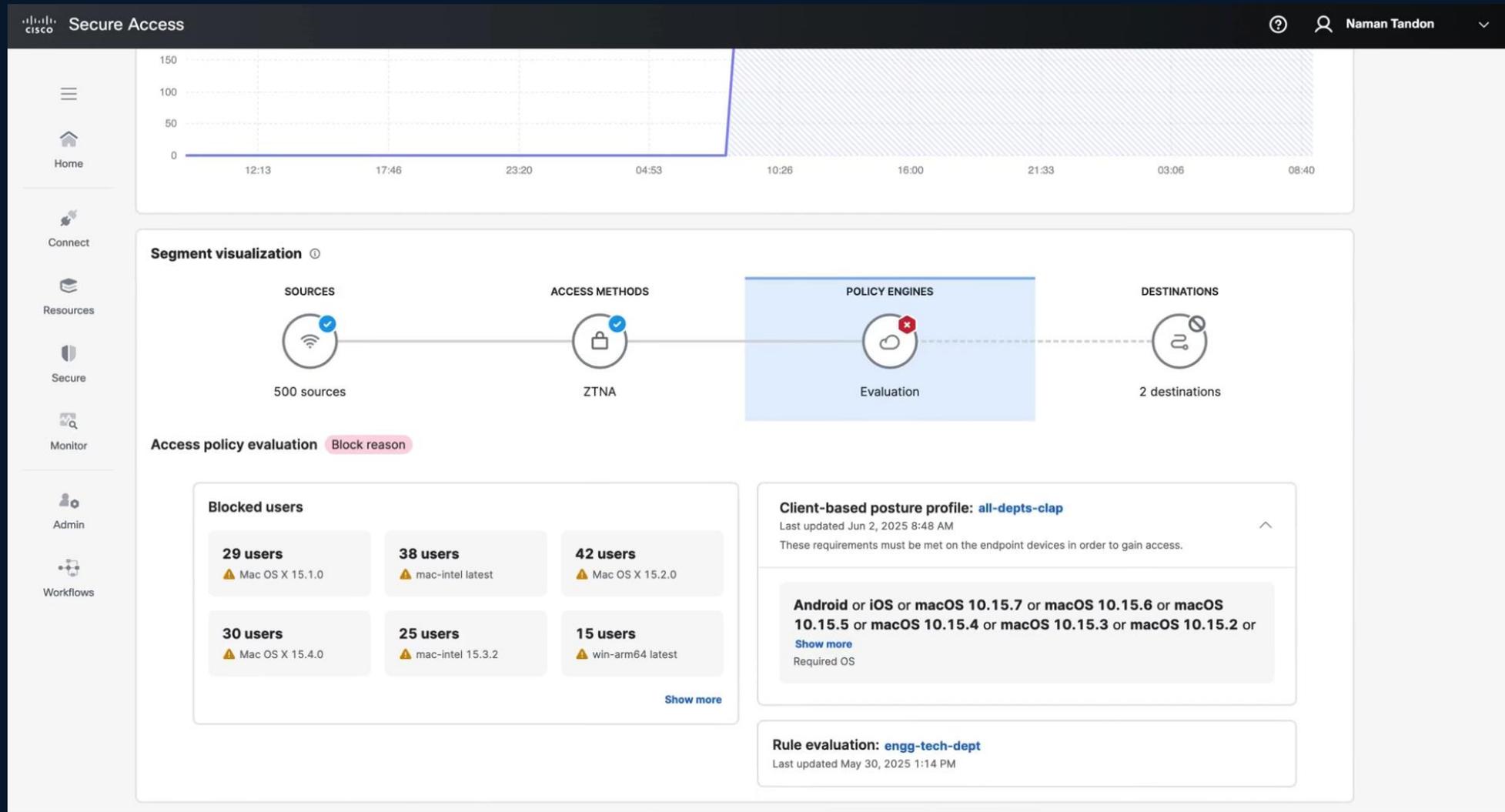
Policy Verification



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

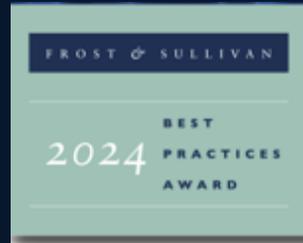
Recognized for SSE and ZTNA Leadership



Rated First in CASB, SWG,
DNS Internet Security

FORRESTER®

Rated as Strong
Performer in Forrester
2024 SSE Wave



Customer Value Leader
Global Security Services Edge

Gartner.
Peer Insights™

SSE Category 2025
4.8/5 Rating



ZTNA Overall Leader Award
KuppingerCole 2024

Thank you

