

Transforming Secure Connectivity for the AI-Ready Enterprise



Mike McPhee
Principal Solutions Engineer, Security

CCIEx2 | CCDE | GSE #339
Americas

What We'll Discuss Today

1. Introduction to Cisco Universal Zero Trust Network Access
2. Seamless Access
3. Identity Intelligence
4. Zero Downtime

About me

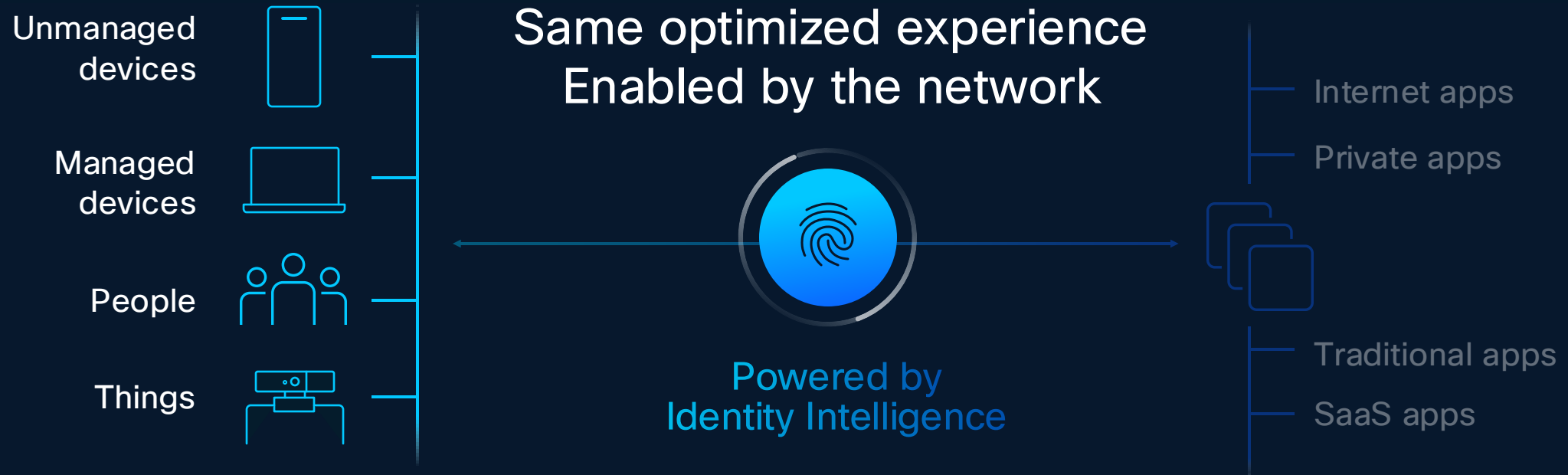
- Rochester NY (Photography, Garbage Plates, Civil Rights, and Kristen Wiig!!!)
- 13 years with Cisco
- 12+ years designing C2 systems
- 6 years in US Navy – “Bubblehead”
- GSE #339 & SANS MSISE
- 13-year CCIE 41663 (R&S, Sec) & CCDE 20180018
- Homebrewer, woodworker, astronomy buff, traveler, history hobbyist



Traditional ZTNA Was Designed for A Different Time and Different Needs



Universal ZTNA from Cisco



Remote

Campus

Branch

Airplane Remote Oil rig

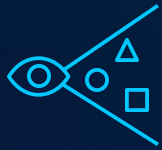
Stadium

Field

...

Cisco AI Access

Securing the use of AI



Visibility



Leakage prevention



Compliant use

1200+ AI applications

SASE: Secure Access Integrated With Cisco SD-WAN

Your security strategy for a hyper-distributed world

SASE

Secure
SD-WAN

Converged set of cloud networking

+

Security
Service Edge

Converged set of cloud security

End-to-end Assurance with ThousandEyes

Cisco Universal ZTNA

SD-WAN

+

Security
Service Edge

+

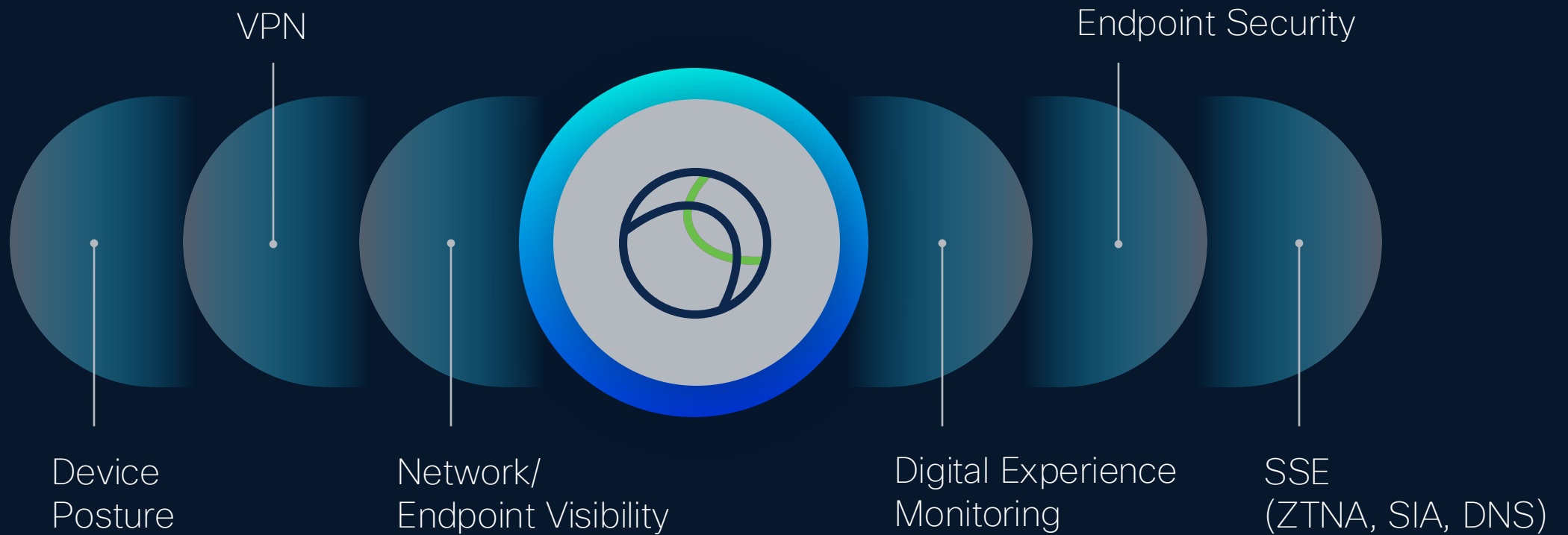
Identity
Trust

Cisco SASE

End-to-end Assurance with ThousandEyes

Seamless Access for All Applications

One Client, Multiple Functions



Flexible Journey to Universal 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

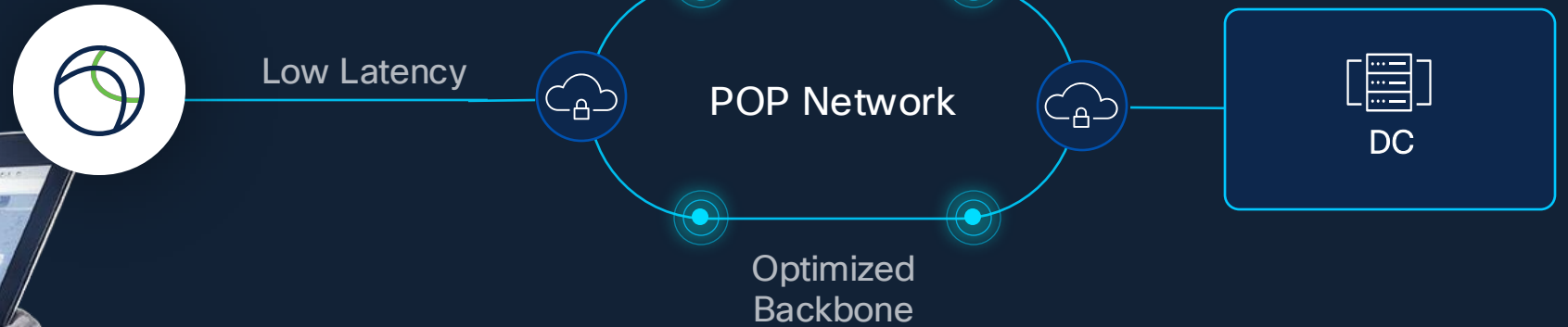
Enable remote users to securely connect with least privilege access to any private app.

Universal ZTNA

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

Cisco's Modern PoP Architecture

Leverages MASQUE/QUIC, Vector Packet Processing (VPP), and a global peering



Cisco SD-WAN Your Way

Flexibility to choose the SD-WAN fabric that fits best for your business



Cisco Catalyst SD-WAN

Future-ready, secure networking built for resilient enterprises



Cisco Meraki SD-WAN

Simple, cloud-managed networking and security made easy



Cisco Secure Firewall Threat Defense

Advanced threat protection for a secure network

Integrated SASE platform with Cisco Secure Access powers all for unified policy enforcement



CAMPUS



HOME



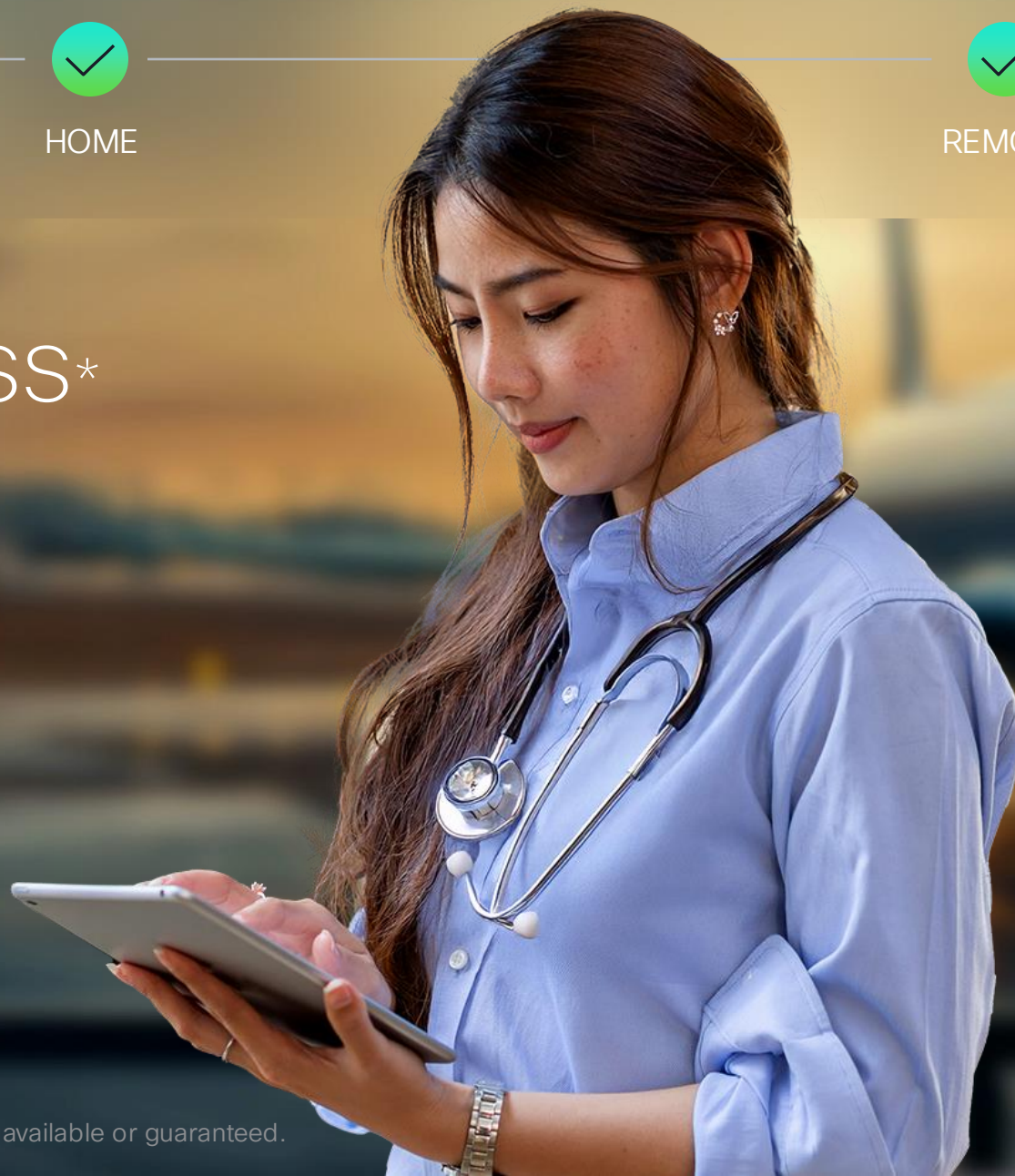
REMOTE

Hybrid Private Access*

Same experience in office
and remote

Resilience with fail-over to
on-prem firewall

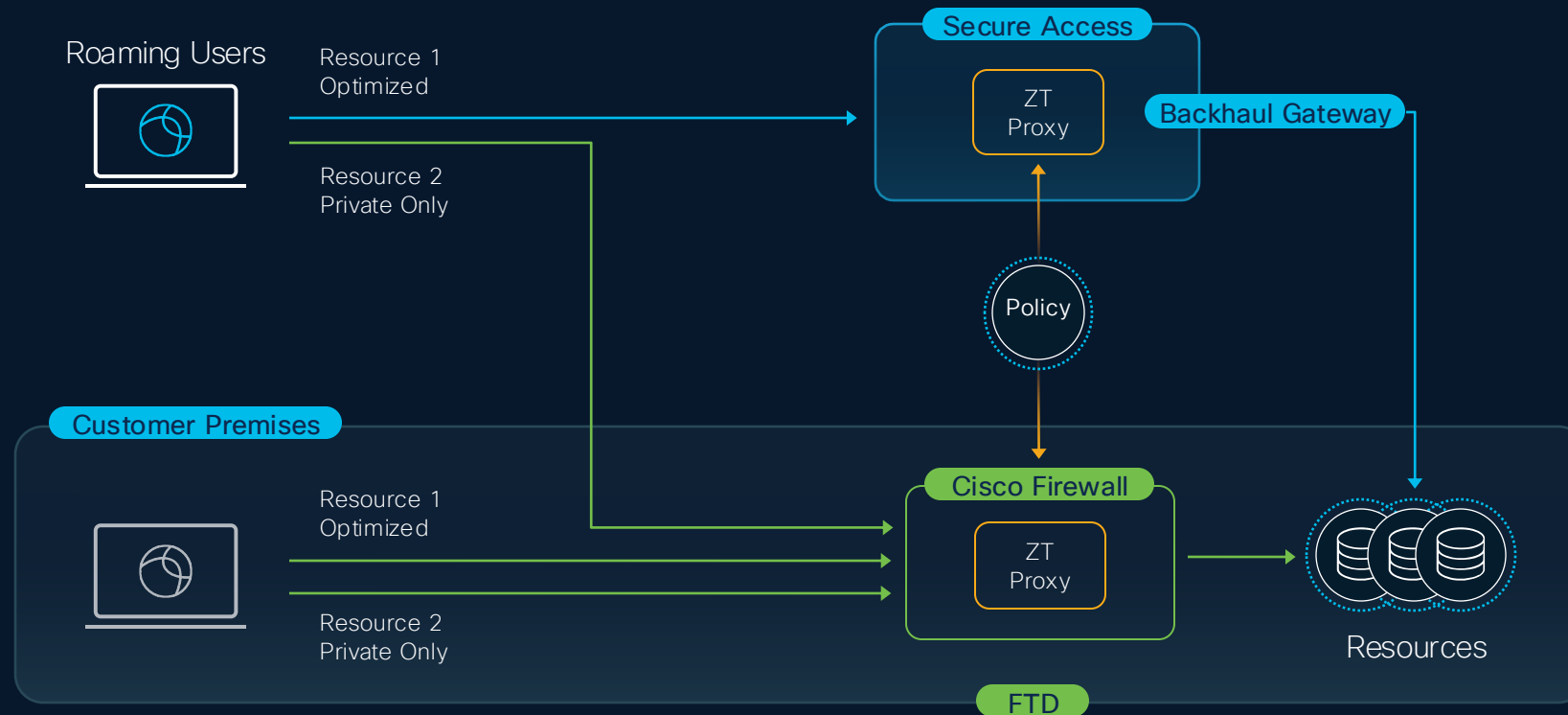
No traffic to sensitive apps
flows through Cisco cloud



* Capabilities are planned but not yet available or guaranteed.

Hybrid Private Access for Flexible Enforcement*

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



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).

1 Specify Access
Specify which users and endpoints can access which resources. [Help](#)

Action

Allow
Allow specified traffic if security requirements are met.

Block
Block specified traffic.

From

Specify one or more sources.

Neil Patel (neipatel@ssep.onmicrosoft.com) x

To

Specify one or more destinations.

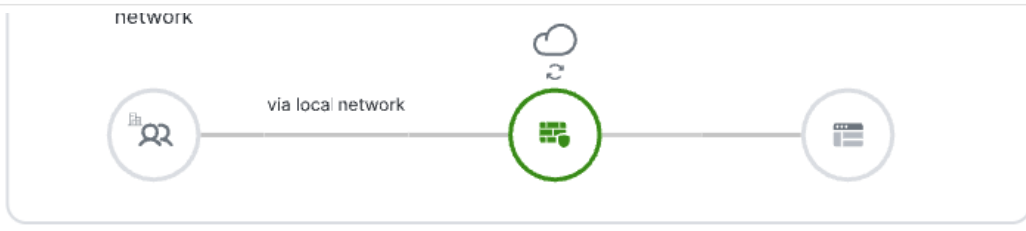
Excalidraw x +1

Endpoint Requirements

For zero-trust connections, if endpoints do not meet the specified requirements, this rule will not match the traffic. [Help](#)

Zero-Trust Client-based Posture Profile Custom
Requirements for end-user devices on which the Cisco Secure Client is installed.
Profile: **Open** | Requirements: **None**
Private Resources: **Excalidraw, SpeedTest-firewall**

- Objects
- Security Devices
- Secure Connecti



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.





Developers are users too

Stop Risky Models Before They Start



Malicious code



IP compliance

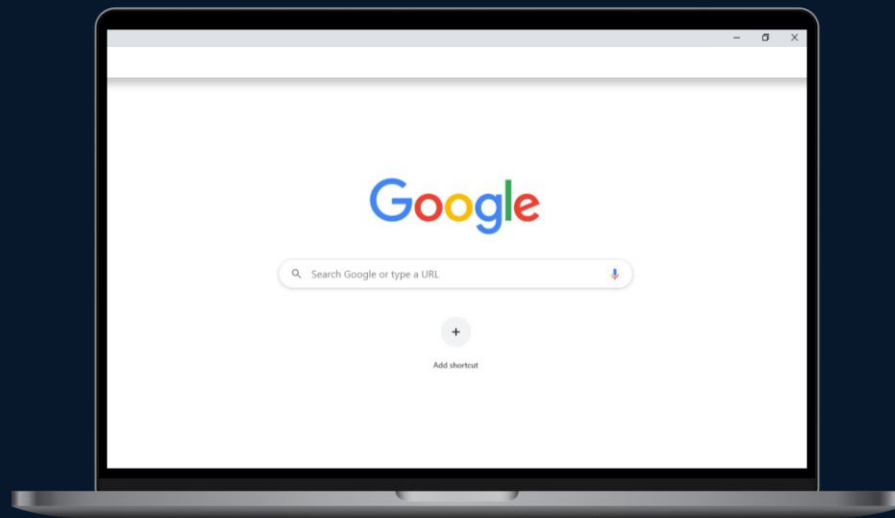


Origin compliance

Pre-use enforcement

Device Support

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



Chrome Enterprise Browser



Native OS Integration





 Learn about this picture

 Recycle Bin

 Chrome (Work)

 Chrome (Personal)

 Search 

ENG CMK  11:35 AM 12/13/2024 

Identity Intelligence



60
percent

of breaches
leveraged identity
as a key component

Cisco Talos Incident Response | Year in Review 2024

Attackers Expect You to Have MFA

Brute-force or password spray



Enrollment

MFA bypass



OS login



App login

Stolen session cookies



Mid-Session



Helpdesk

Physical access to device

Fallback to less secure MFA method

Deepfake social engineering at help desk

INTRODUCING

Duo Identity & Access Management (IAM)



Duo IAM

Security-First
Identity

End-to-End
Phishing Resistance

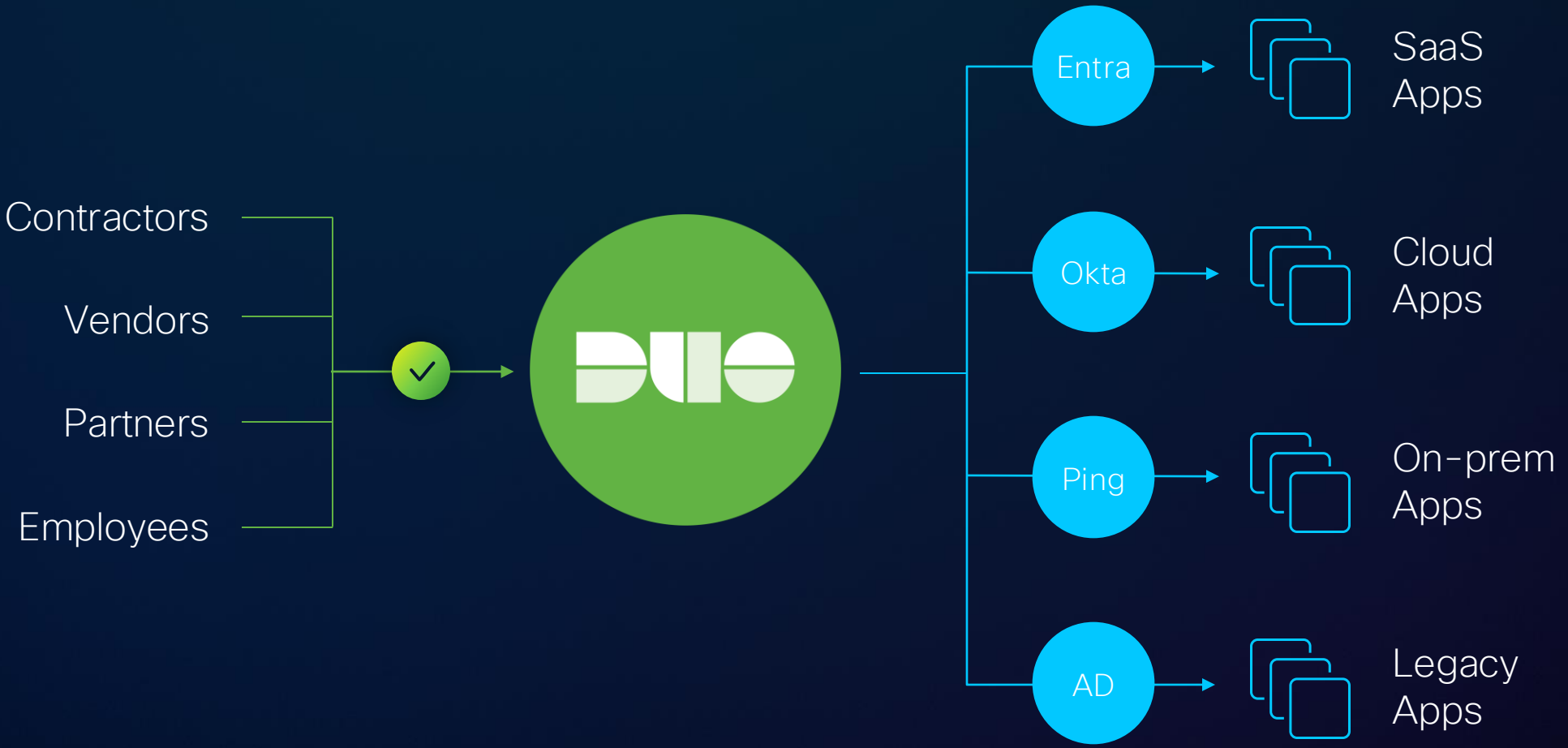
Unified Identity
intelligence

World-Class User Experience

Standalone IAM
when required

Identity broker
for existing IAM

Alternate directory for
third-party users



Duo IAM

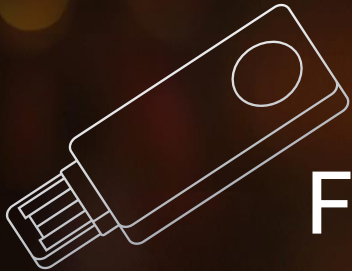
Security-First
Identity

End-to-End
Phishing Resistance

Unified Identity
intelligence

World-Class User Experience

End-to-End Phishing Resistance



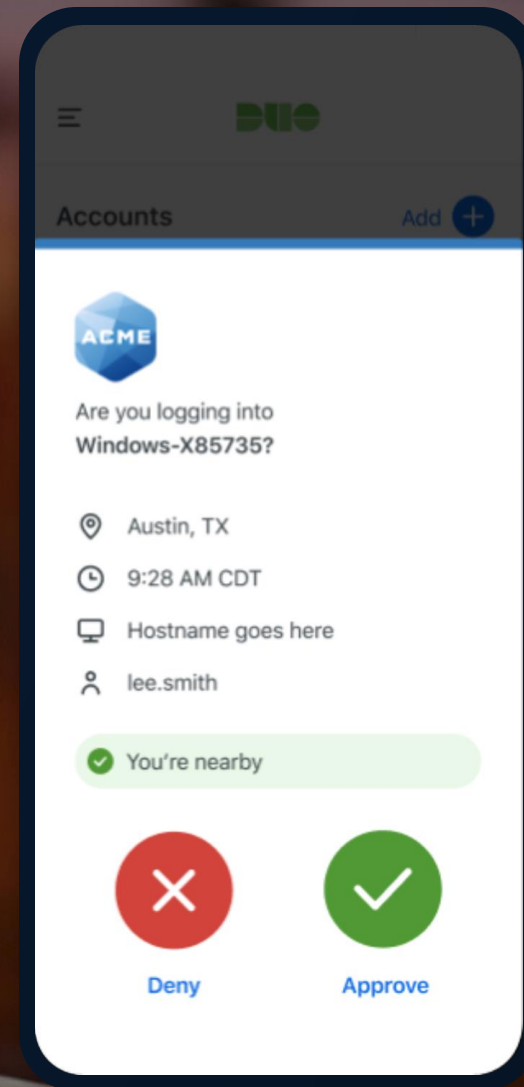
FIDO2, Hardware
Tokens

End-to-End Phishing Resistance

Proximity Verification



Bluetooth Low Energy (BLE)



Cisco Secure Access Use Case

Duo IAM

Security-First
Identity

End-to-End
Phishing Resistance

Unified Identity
Intelligence

World-Class User Experience

SailPoint

Dragos

Crowdstrike

Salesforce

Okta

PingIdentity

Cisco ISE

Auth0

Cyberark

Microsoft

Google

Amazon

Cisco Identity Intelligence



USERS



MACHINES



SERVICES



HRIS



DATA



APPS



PLATFORMS



SailPoint

Dragos

Crowdstrike

Salesforce

Cisco ISE

Okta

PingIdentity

Auth0

Microsoft

Google

Cyberark

Amazon

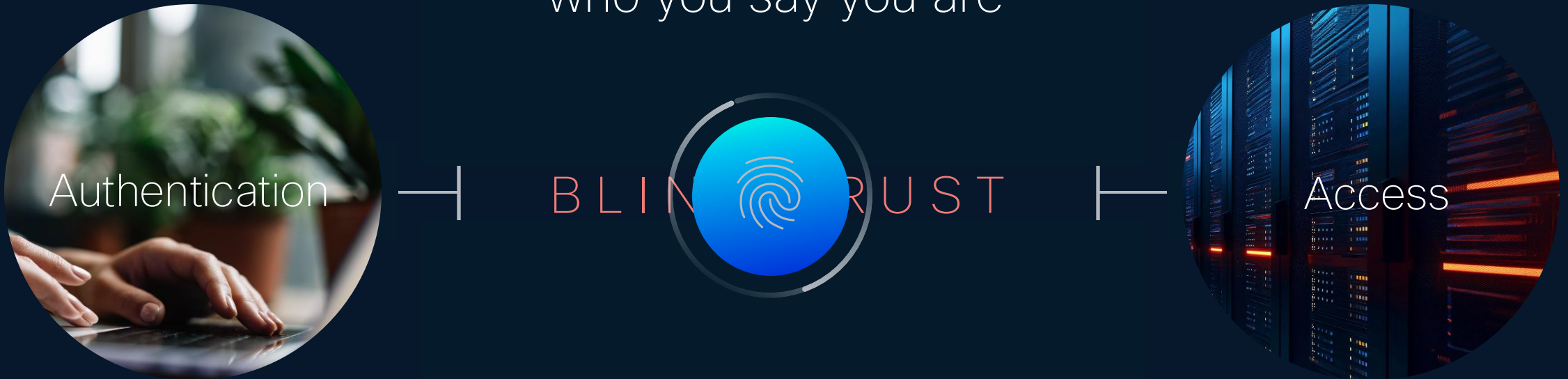




Cisco Identity Intelligence

Identity Intelligence

Continuously assess you are
who you say you are



Works with existing IDPs



Cisco
Duo IAM

Cisco
Secure
Access

Cisco
XDR

User Trust Level



TRUSTED

NEUTRAL

UNTRUSTED

* Capabilities are in private preview.

Cisco Secure Access Use Case

Duo IAM

Security-First
Identity

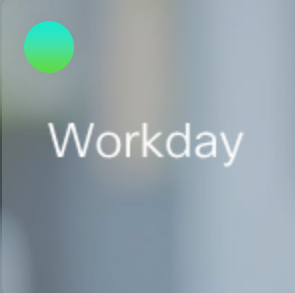
End-to-End
Phishing Resistance

Unified Identity
intelligence

World-Class User Experience



Authenticate once.





FIREWALL



Workday

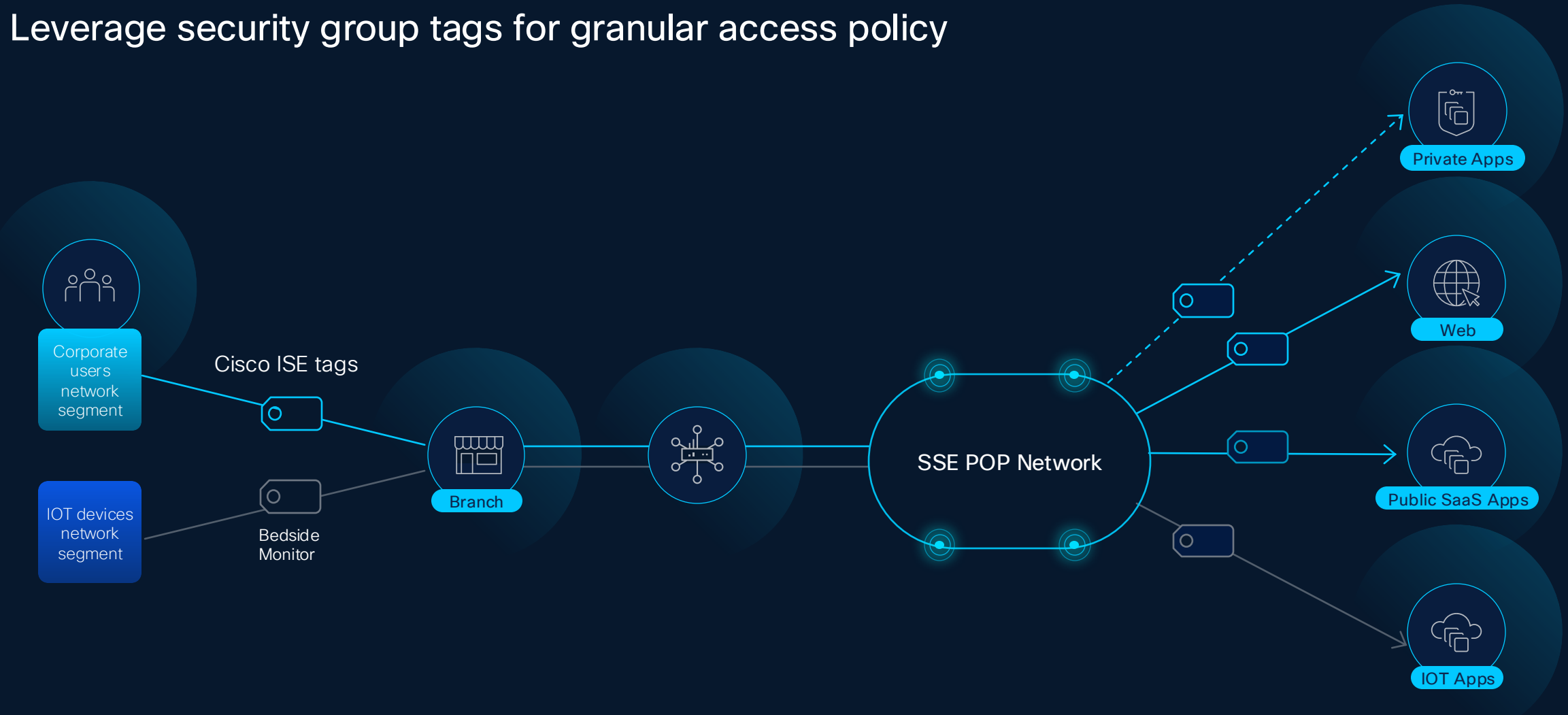


Frustrate attackers,
not users.

Things have identities.

Enforce Zero Trust Using Identity Context

Leverage security group tags for granular access policy



Security Group Tags (SGTs) Based Policy

1

The screenshot shows the Cisco Secure Access 'Integrations' page. A red circle highlights the 'Integrations' header. Below it, the 'Cisco Identity Services Engine' integration is visible. A second red circle highlights the 'Specify Access' step in the configuration process.

2

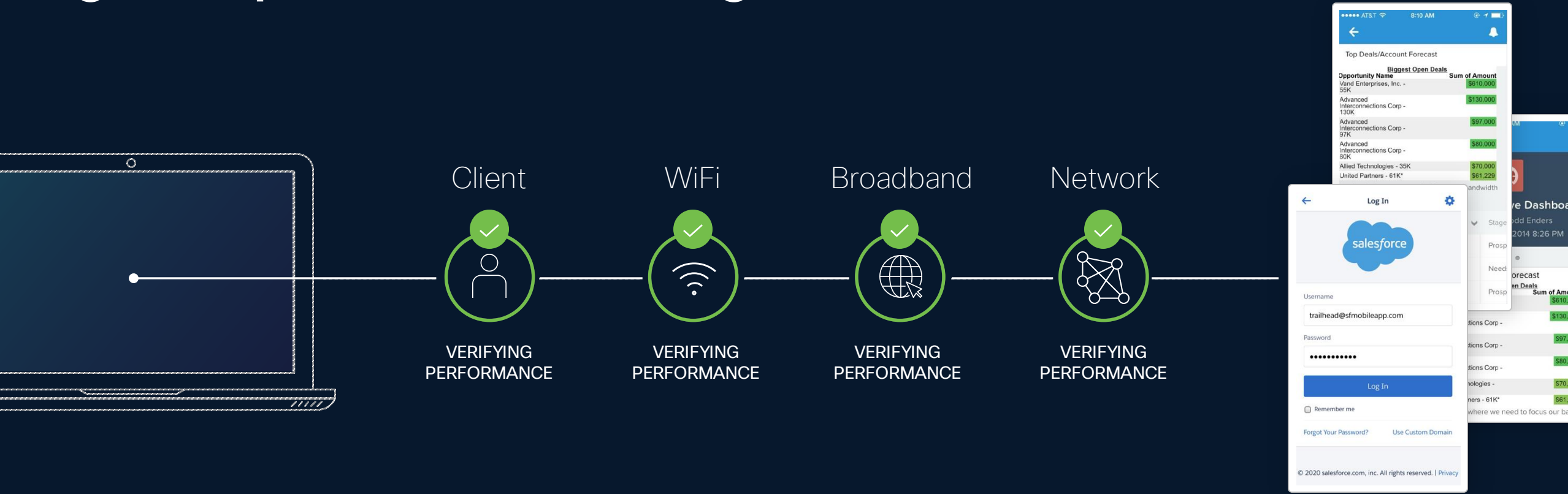
3

The screenshot shows the Cisco Secure Access 'Security Group Tags' page. A table lists various SGTs with their names and tag values. A red circle highlights the 'Rule name' field in the background configuration window, which is set to 'VideoEquipmentAccess'.

Name	Tag
ANY	65535
AP_EMR_EPG	503
AP_Services_EPG	501
AP_Test_EPG	502
Auditors	9
BYOD	15
Cameras	24
Contractors	5
Developers	8
Development_Servers	12

Zero Downtime

End-to-End Visibility With Digital Experience Monitoring



Historical performance and recommendations

Simplify Troubleshooting

Consolidated view of network and security events to make troubleshooting easier

The screenshot displays the Cisco Secure Access Experience Insights dashboard. The page title is "Experience Insights" with a "read-only" indicator. Below the title, there is a brief description: "Experience Insights brings together employee digital experience data so you can understand their journey to Secure Access and corporate resources. Get a comprehensive view into their device and network behaviour to identify and resolve issues faster and make informed decisions on how to improve those interactions. Help".

The "Endpoints summary" section contains two summary cards:

- Number of endpoints 4 total**: 3 Online (blue dot icon)
- Health status**: 0 Unhealthy (red dot icon), 1 At Risk (yellow triangle icon), 1 Healthy (green checkmark icon)

A world map is displayed below the summary cards, with a legend for health status: All (blue), Unhealthy (red), At risk (yellow), and Healthy (green). Two blue circles with the number "1" are overlaid on the map, one over the United States and one over the United Kingdom.

Below the map, there are search filters: "Search by user name", "Select location", and "Select health status".

At the bottom, a table lists endpoint details:

User name	Location	Health status	Device name	Latency	Jitter	Loss	WiFi	Ethernet	CPU	Memory	OS	Test time
Carol Freeman	Wichita, Kansas, US	Healthy	PSEUDOCO-DESKTO	23 ms	0 ms	0.00%	—	1000 Mbps	0.39%	17.76%	Microsoft Windows 11	Sep 12, 2024 2:30PM

- Home
- Experience Insights
- Connect
- Resources
- Secure
- Monitor
- Admin
- Workflows

Experience Insights read-only

Powered by **ThousandEyes**

Experience Insights brings together employee digital experience data so you can understand their journey to Secure Access and corporate resources. Get a comprehensive view into their device and network behaviour to identify and resolve issues faster and make informed decisions on how to improve those interactions. [Help](#)

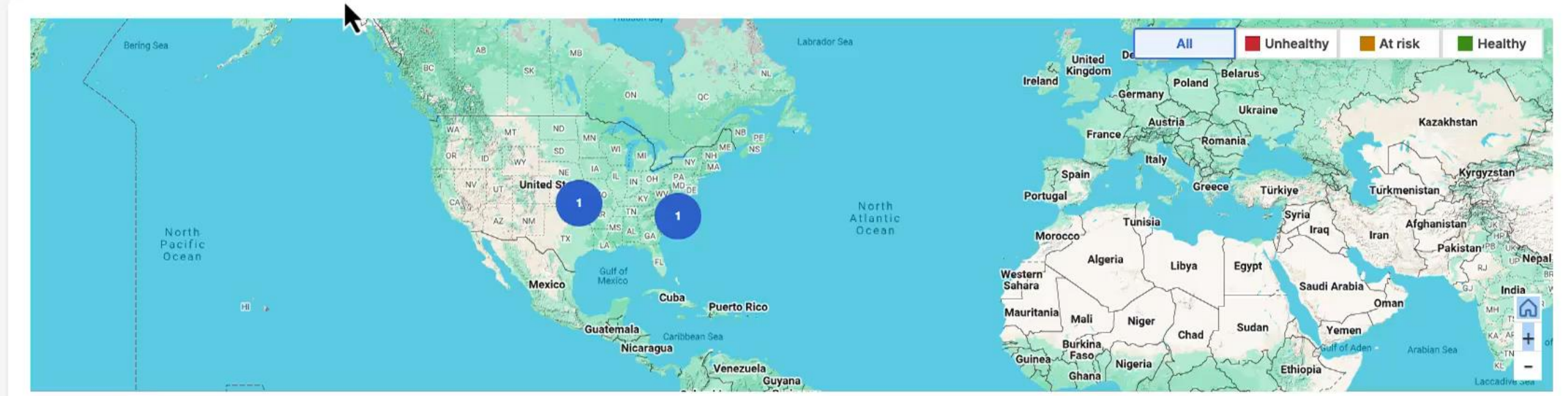
Endpoints summary

Number of endpoints 4 total

3 Online ✔

Health status

0 Unhealthy ❗ 1 At Risk ⚠ 1 Healthy ✔



User name	Location	Health status	Device name	Latency	Jitter	Loss	WiFi	Ethernet	CPU	Memory	OS	Test time
Carol Freeman	Wichita, Kansas, US	✔ Healthy	PSEUDOCO-DESKTO	23 ms	0 ms	0.00%	—	1000 Mbps	0.39%	17.76%	Microsoft Windows 11	Sep 12, 2024 2:28PM

Summary

Cisco Clears the Path to Zero Trust



Protect identities with identity intelligence



Control access across all users and things for tighter security



Build resilience with optimized infrastructure and simplified IT

CISCO Connect

Thank you



