CISCO Engage | Tech Day Twin Cities

Cisco ZTNA/SASE

Matt Hendrickson
Solutions Engineer - Security

Ben Craig
Solutions Engineer – SD-WAN

April 16, 2026

Introductions – Matt Hendrickson

- Nearly 12-years at Cisco
- Focusing on Security
- 28+ years in Security
- Robotics Coach – 2 teams
- Specializations in Identity Services Engine, Secure Access, Secure Firewall, and SNA.

Introductions – Ben Craig

- 4 years at Cisco
- Focusing on SD-WAN

Agenda

1. What is UZTNA
2. Secure Access Components
3. Secure Internet Access
4. Demo AI Access and SGT in Secure Access
5. Secure Private Access
6. Demo
7. Experience Insights
8. User Trust Scores

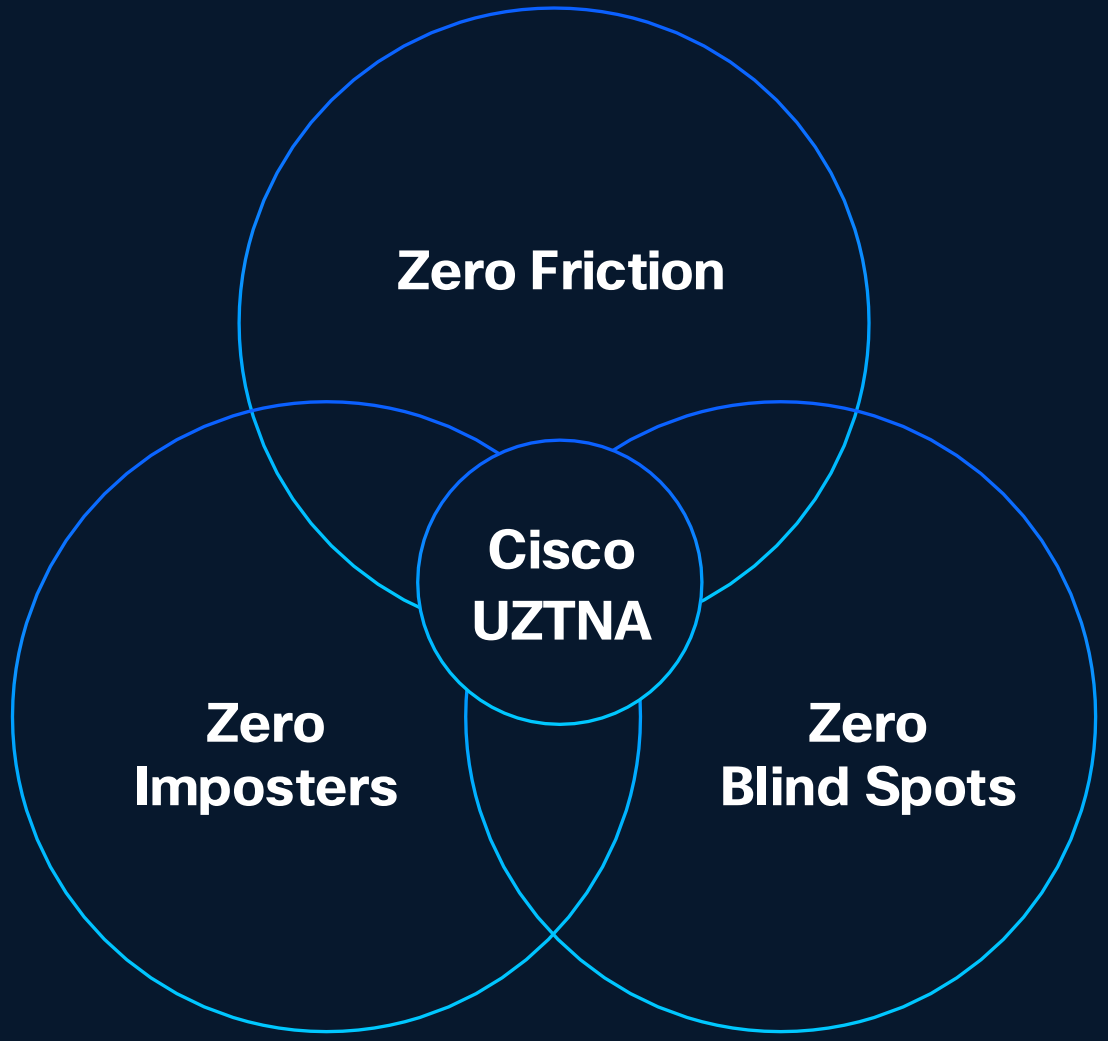
What is UZTNA?

What is UZTNA?

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 is built on 3 core *differentiators*

- **Zero Friction** – Seamless access for users and integrated operations for admins.
- **Zero Imposters** – Continuous identity and trust verification that stops Identity attacks.
- **Zero Blind Spots** – Complete visibility and protection across users, devices, apps, and *now AI*.



Cisco Universal ZTNA

Takes ZTNA to users and **devices**

Security Cloud Control

Secure SD-WAN + Secure Services Edge + **Continuous Trusted Identity for Everything**

Single vendor SASE

Digital Experience (ThousandEyes)”
“Threat Detection & Response (Talos, XDR, Splunk)”

cisco

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...

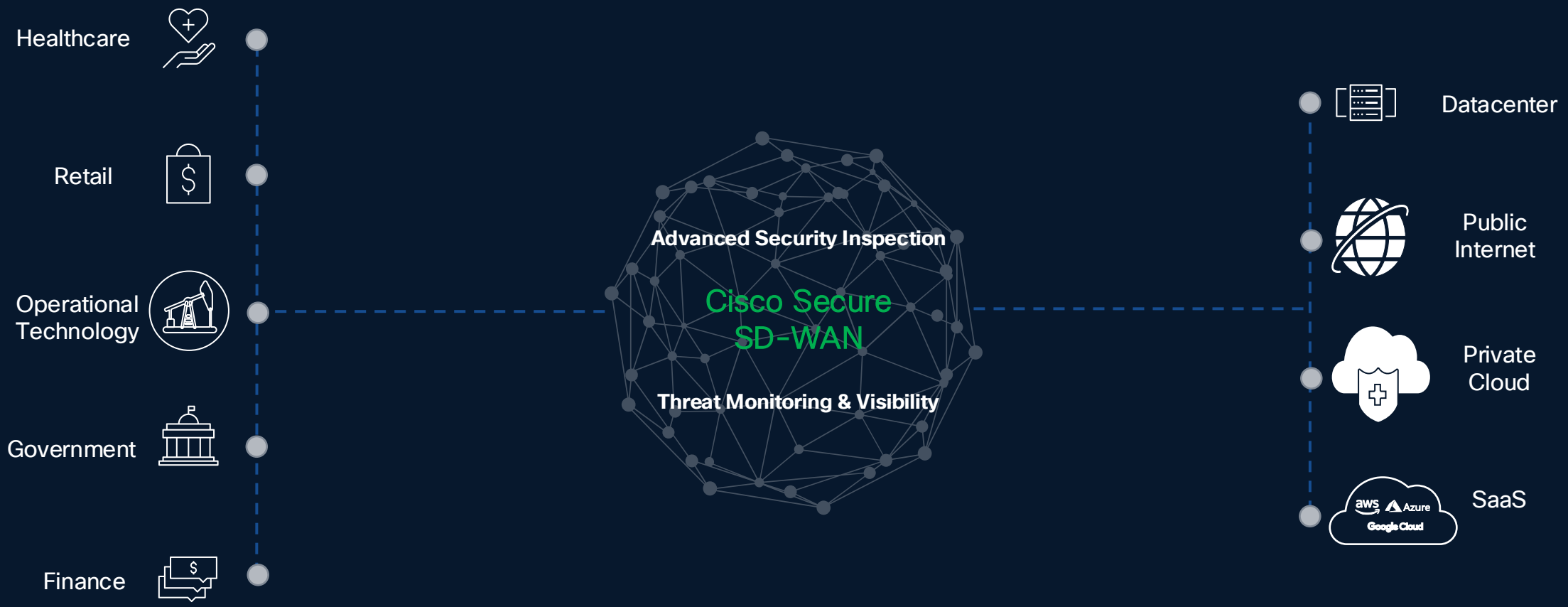
- DNS Security
- Multimode DLP
- Advanced Malware protection
- Sandbox
- Talos Threat Intelligence
- VPN as a Service
- Digital Experience Monitoring*
- Remote Browser Isolation*

Add-on solutions

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

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

Across Markets, One Security Solution, Catalyst SD-WAN



All Market Segments

Complete Security Portfolio

Any Destination

Cisco Secure WAN – Cloud Security

Policies

Manager

Controller

ISE

Security Cloud Control

Secure Service Edge (SSE)

Cisco Secure Access

SecOps Ecosystem

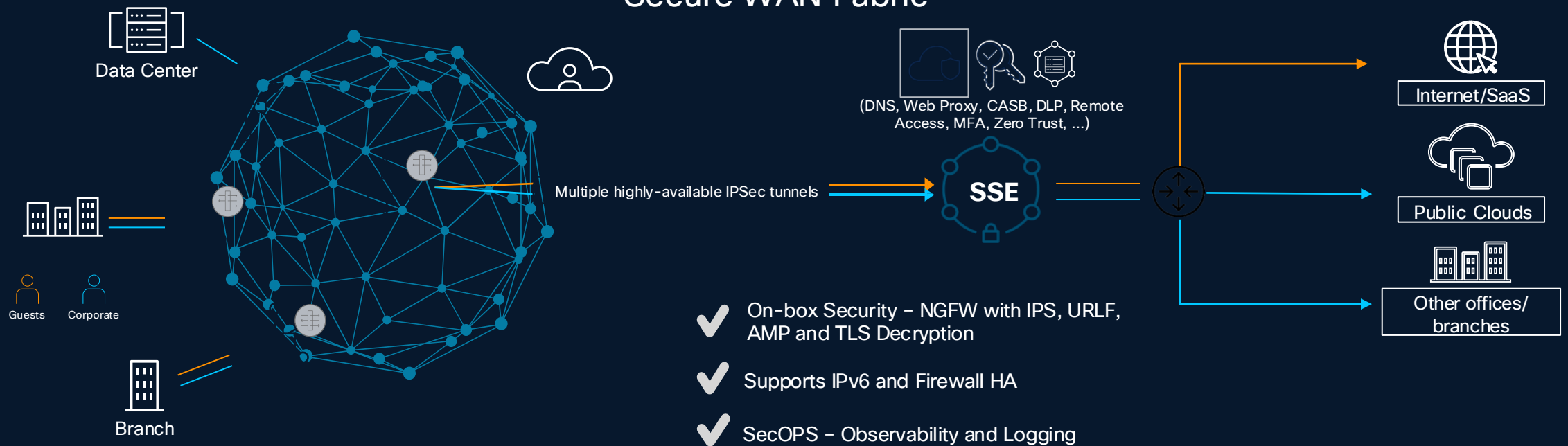
Manager

AI Ops

Splunk

SAL

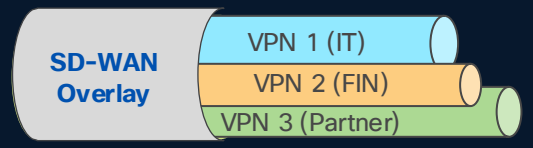
Secure WAN Fabric



- On-box Security – NGFW with IPS, URLF, AMP and TLS Decryption
- Supports IPv6 and Firewall HA
- SecOPS – Observability and Logging

Cisco Secure WAN – Granular End-to-End Segmentation

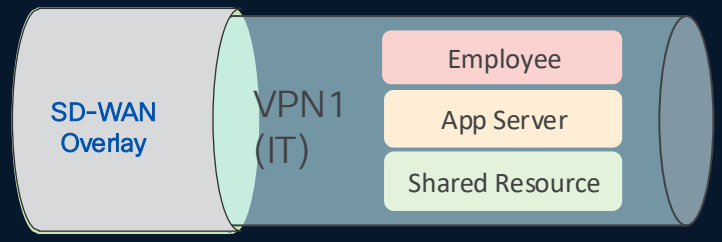
Macro Segmentation



VPN Level Segmentation

- IT VPN
- Finance VPN
- Partner VPN

Micro Segmentation

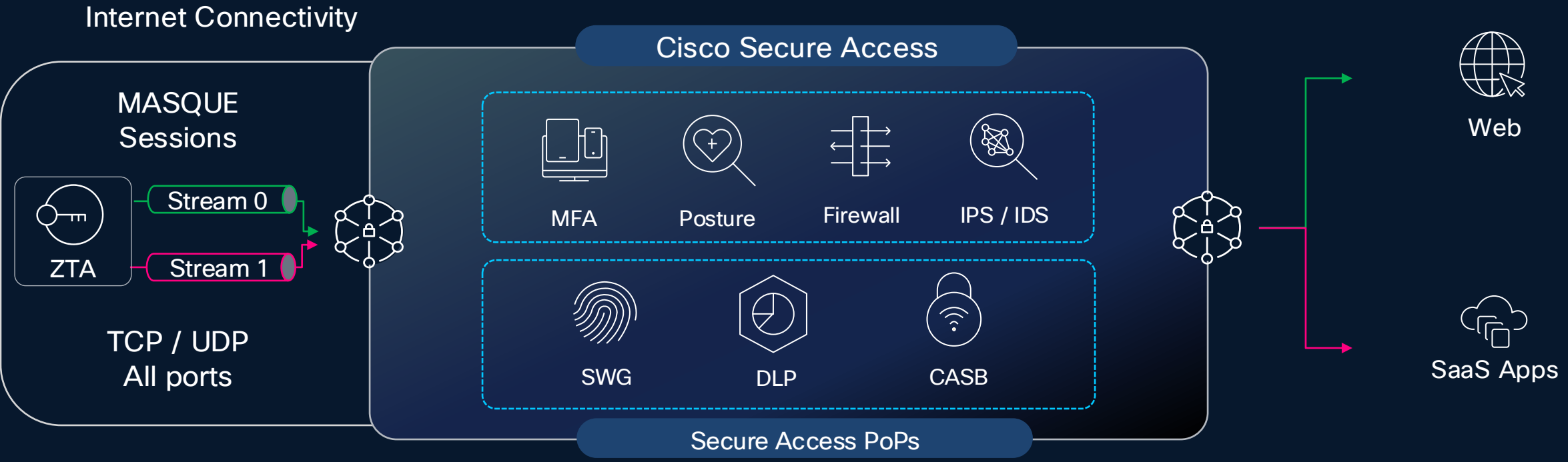


Group Level Segmentation
Example: IT VPN

- Employee
- App Servers
- Printers

Secure Internet Access

Client-based Zero Trust Access



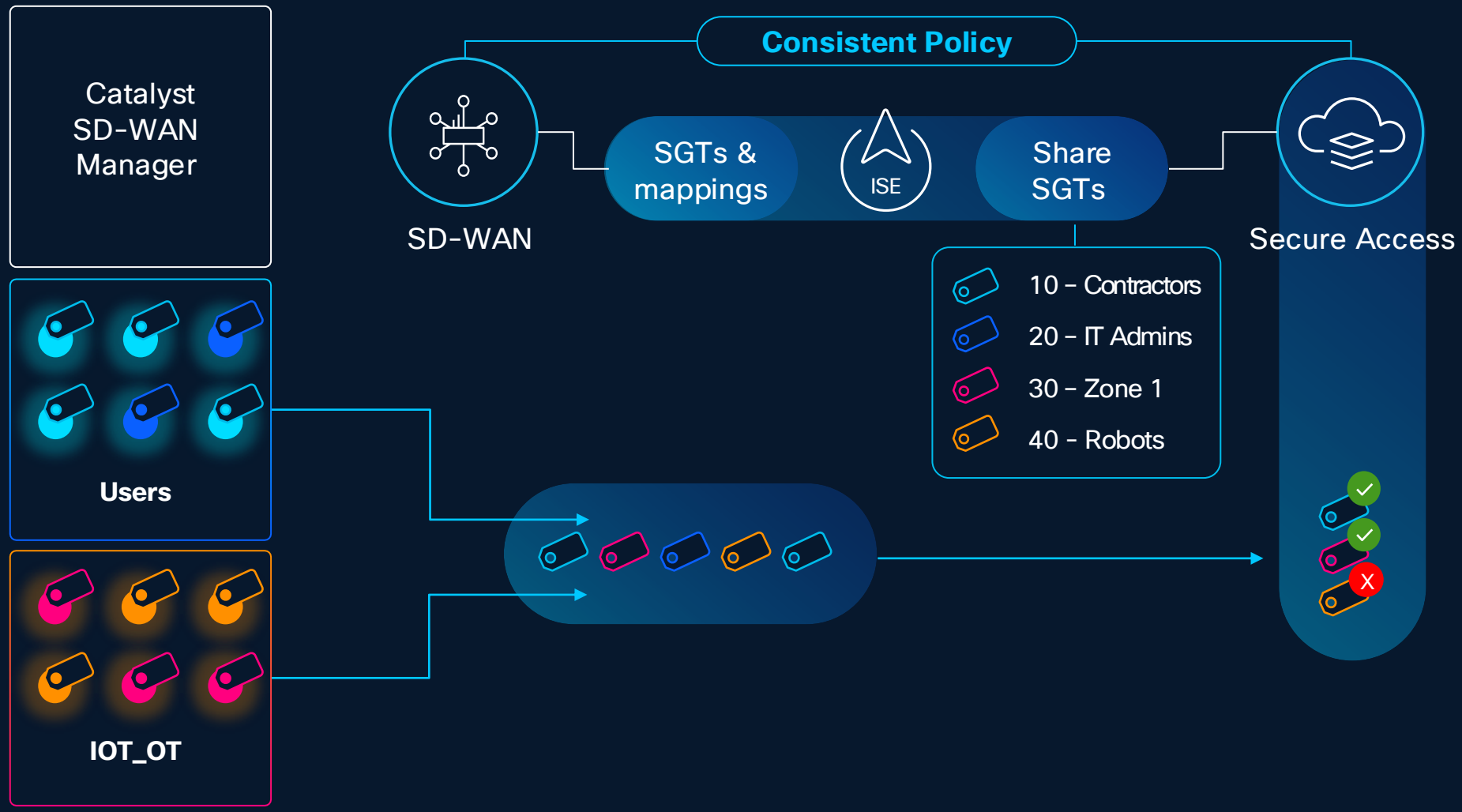
- Transparent user experience
- Trusted Network Detection
- Service managed client certificates with TPM-protected key storage

- Session-based security
- No VPN tunnels
- User and group-packet steering
- User and group-based policy

Identity Services Engine (ISE)

Leverage SGTs for granular access control

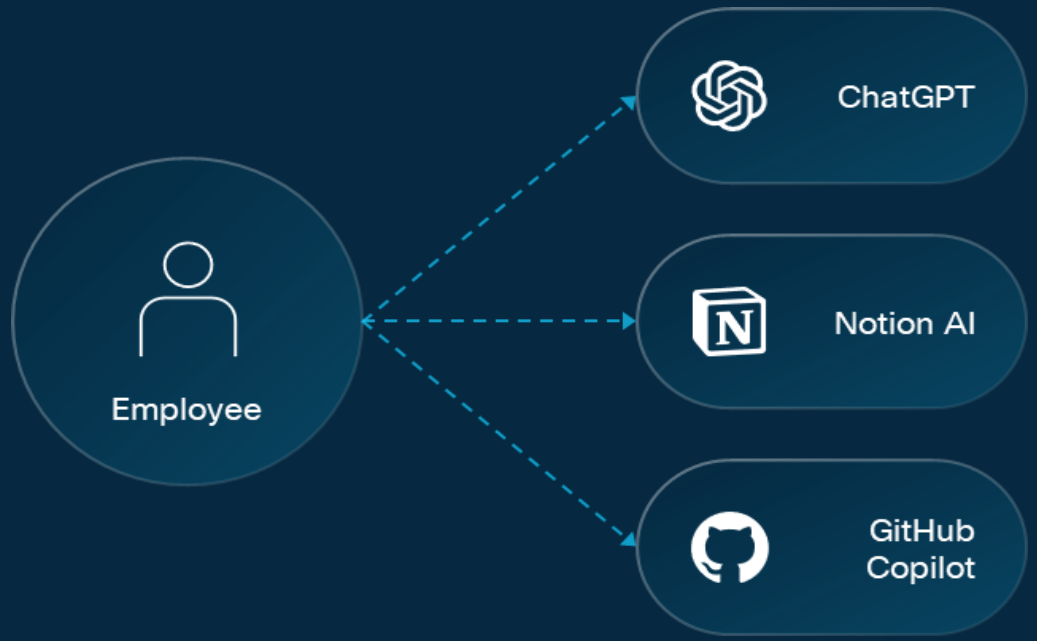
- SGT Based Policy across network & Cloud
- Maintain micro segmentation through Secure Access
- Uniquely identify devices and traffic based on context from ISE
- Apply policy to SGT Based identity



Two distinct areas of AI risk

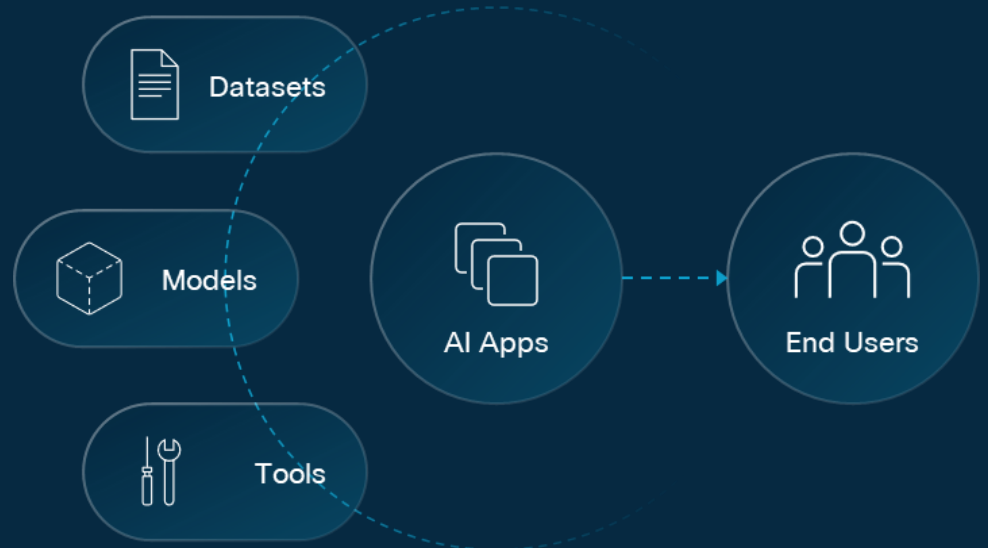
Third-Party AI Tools – AI Access with Secure Access

Manage employee use of **third-party AI tools**, preventing data leakage and other business risks, with Cisco Secure Access.



First-Party AI Applications – AI Defense* (Available as a separate product)

Enable end-to-end secure development of **first-party AI applications** across your business with Cisco AI Defense.



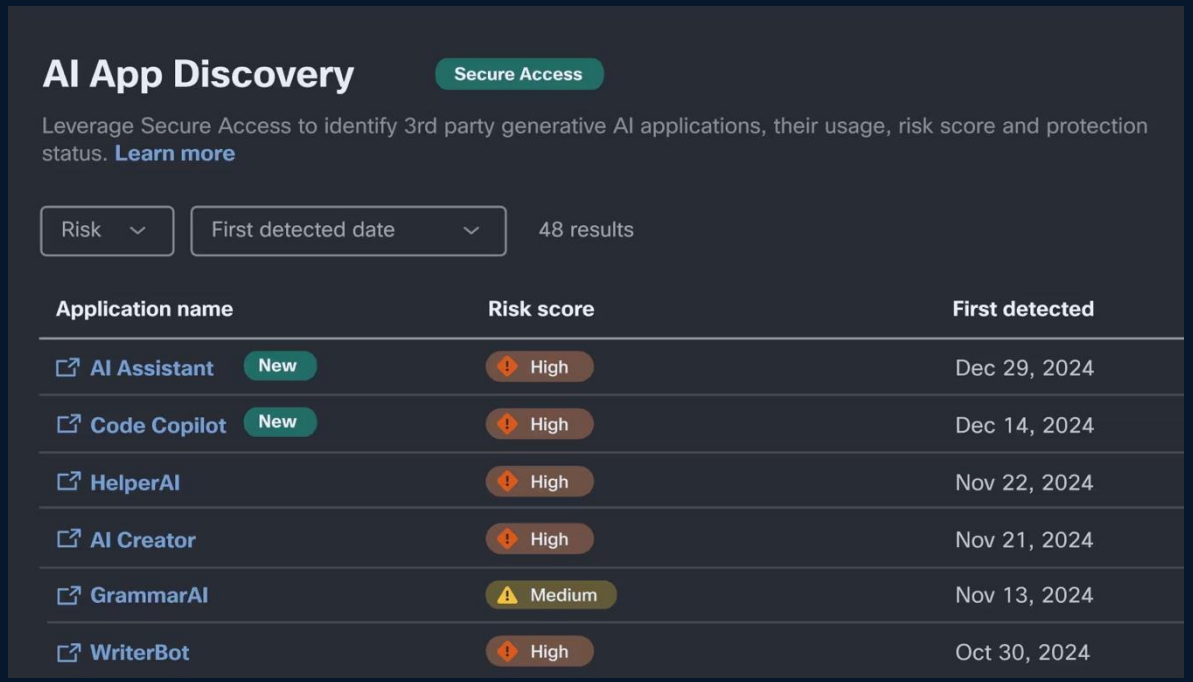
AI Access – Control Sanctioned and Unsanctioned GenAI apps

Superior visibility & control

- Discover Shadow GenAI apps – Allow, block and monitor
- Granular control for 1200+ GenAI apps
  - Sensitive documents
  - Source code
- Machine learning pretraining finds unstructured data and documents
  - Patent applications
  - M&A
  - Financial statements and more

Zero-Friction Security

- Built into Secure Access, no extra license
- Single unified policy framework
- Start fast with pre-built ML identifiers for classifying documents + AI guardrail protection



1200+ Apps
Visibility & Control

15+ Top Apps
Advanced Guardrails

1
Unified Security Framework

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

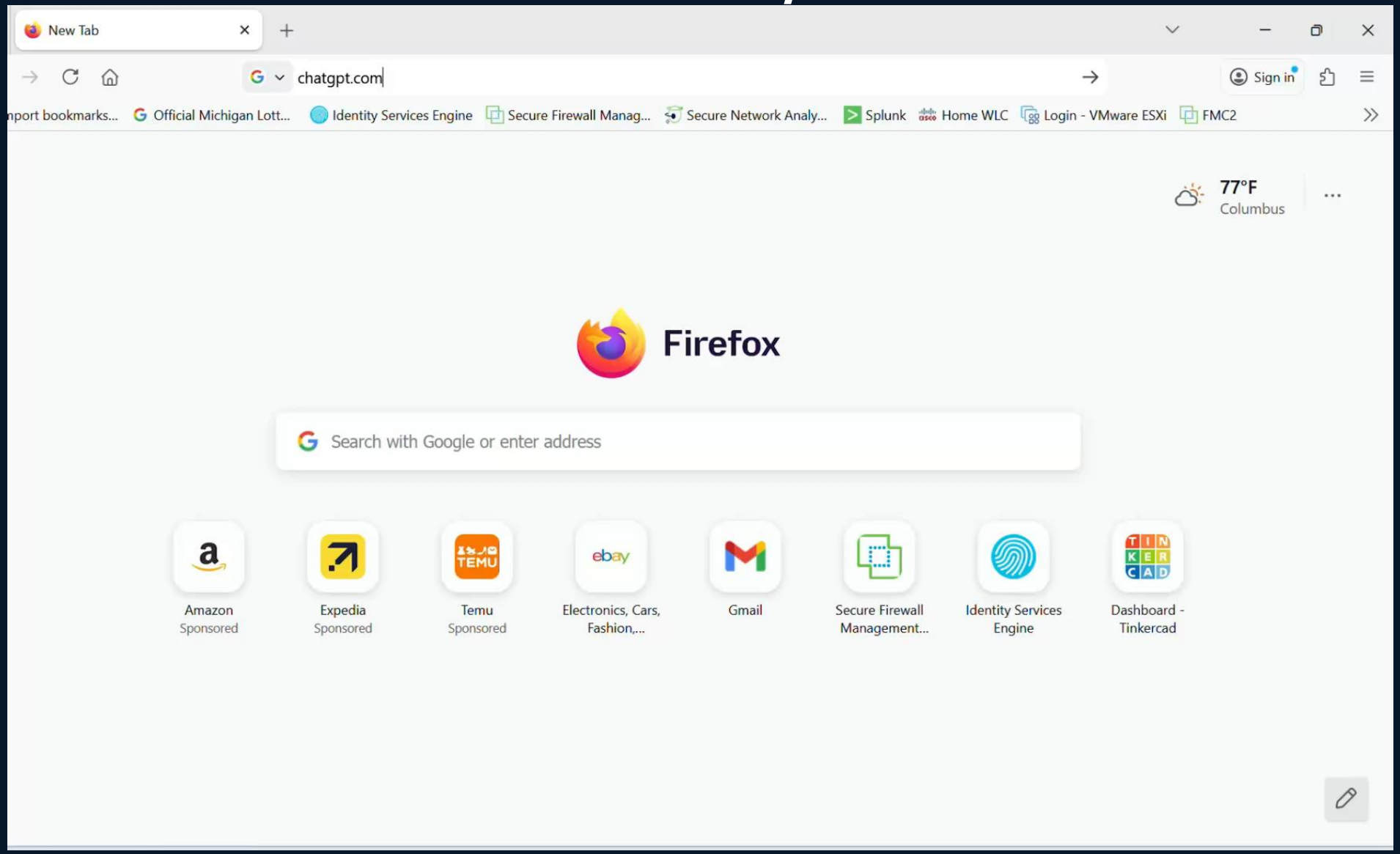
Safety

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

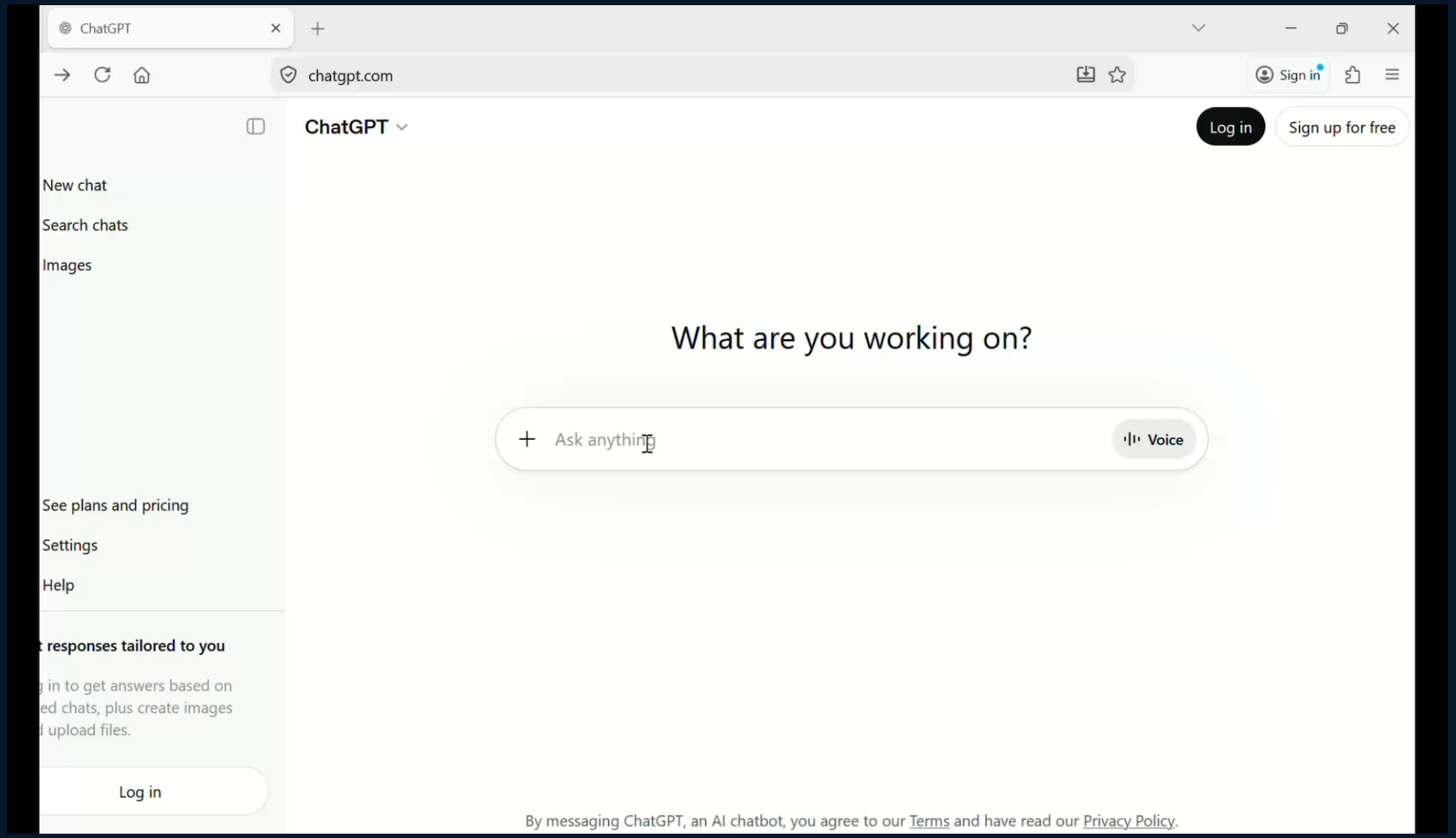
Map guardrails to standards and frameworks like: OWASP MITRE ATLAS

cisco

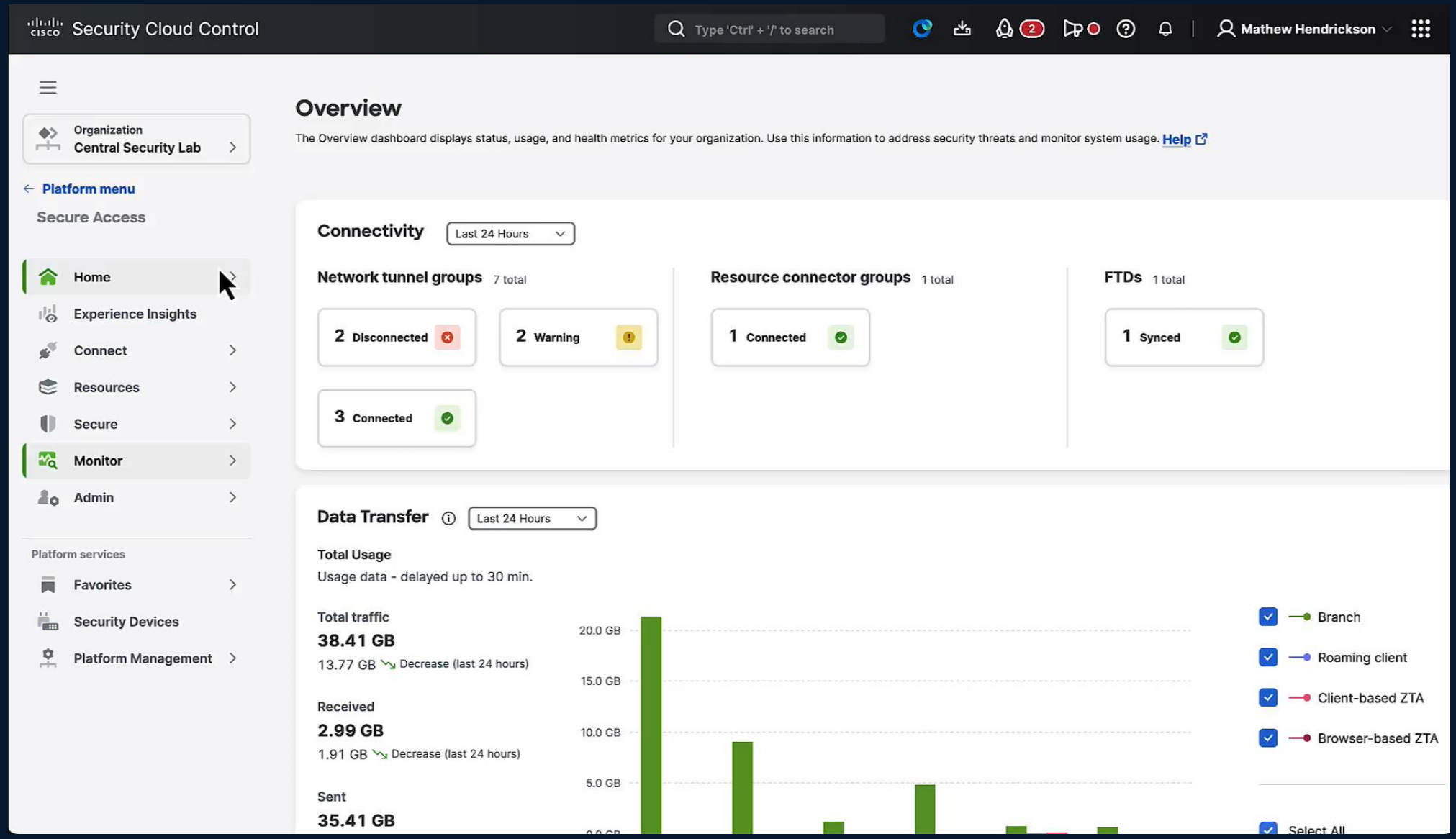
Demo – SIA AI Access/DLP CC



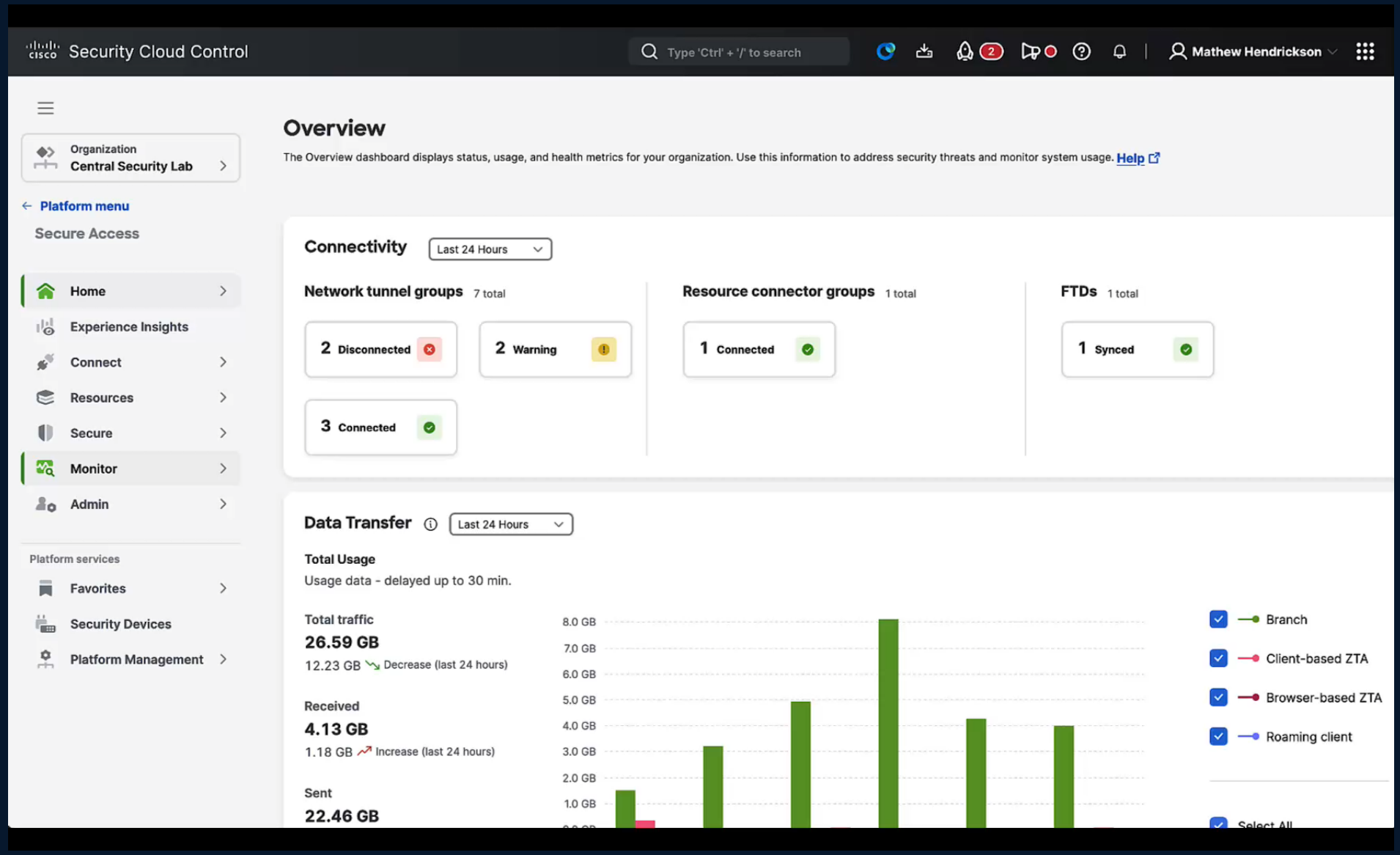
Demo AI Access Guardrails



Demo AI Access Reporting

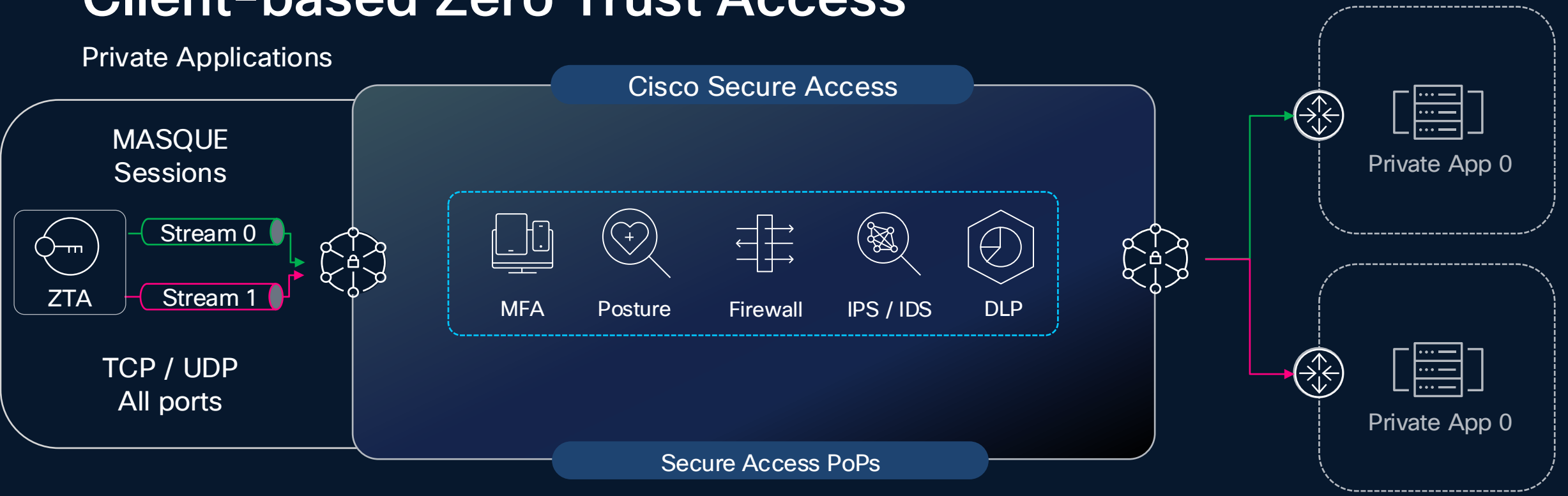


Demo SGTs in Secure Access



Zero Trust Access (SPA)

Client-based Zero Trust Access

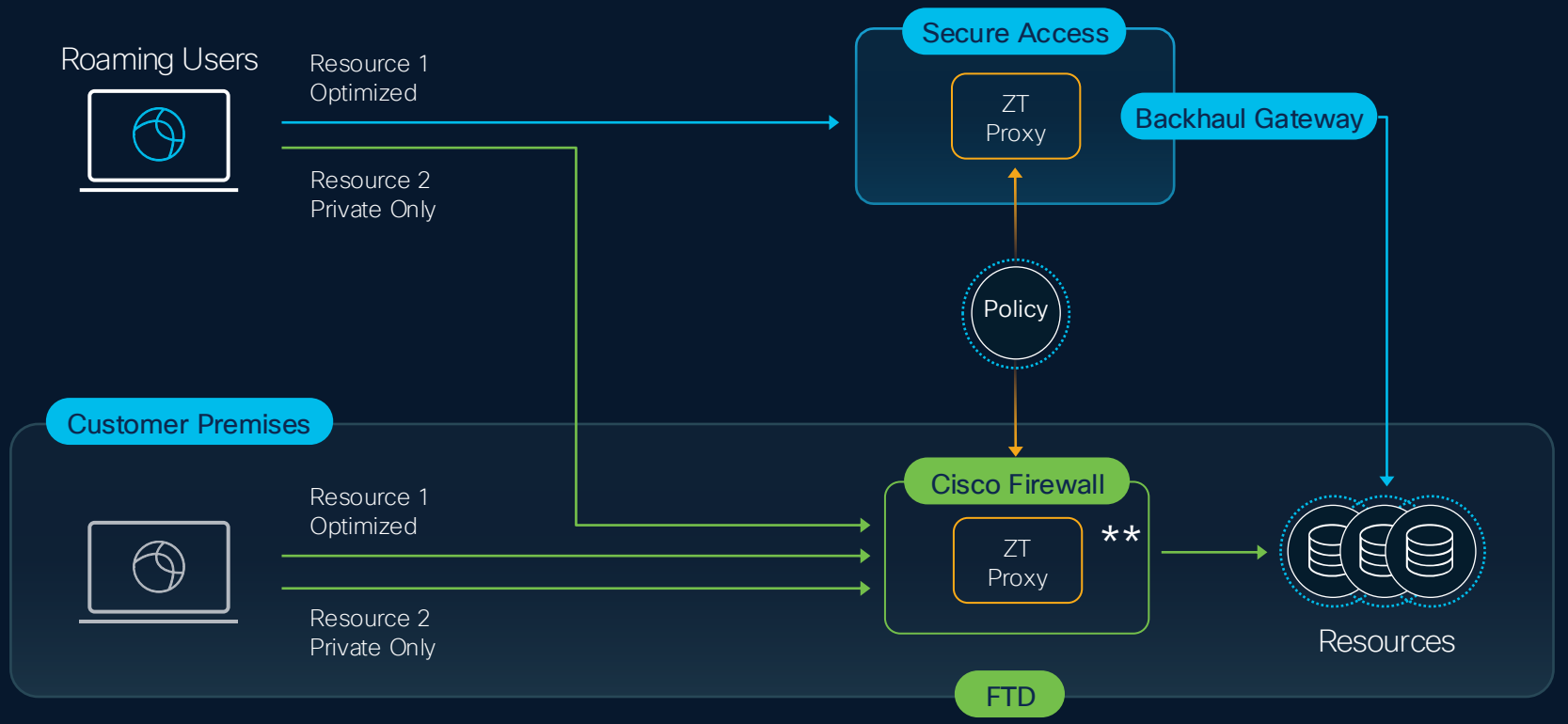


- Transparent user experience
- Forward proxied resource access with coarse or fine-grained access control
- Service managed client certificates with TPM-protected key storage

- Inside to out L4-7 tunnels from RCs
- No routing complexities
- Apps are hidden, supports overlapping subnets
- Easy to scale with high availability

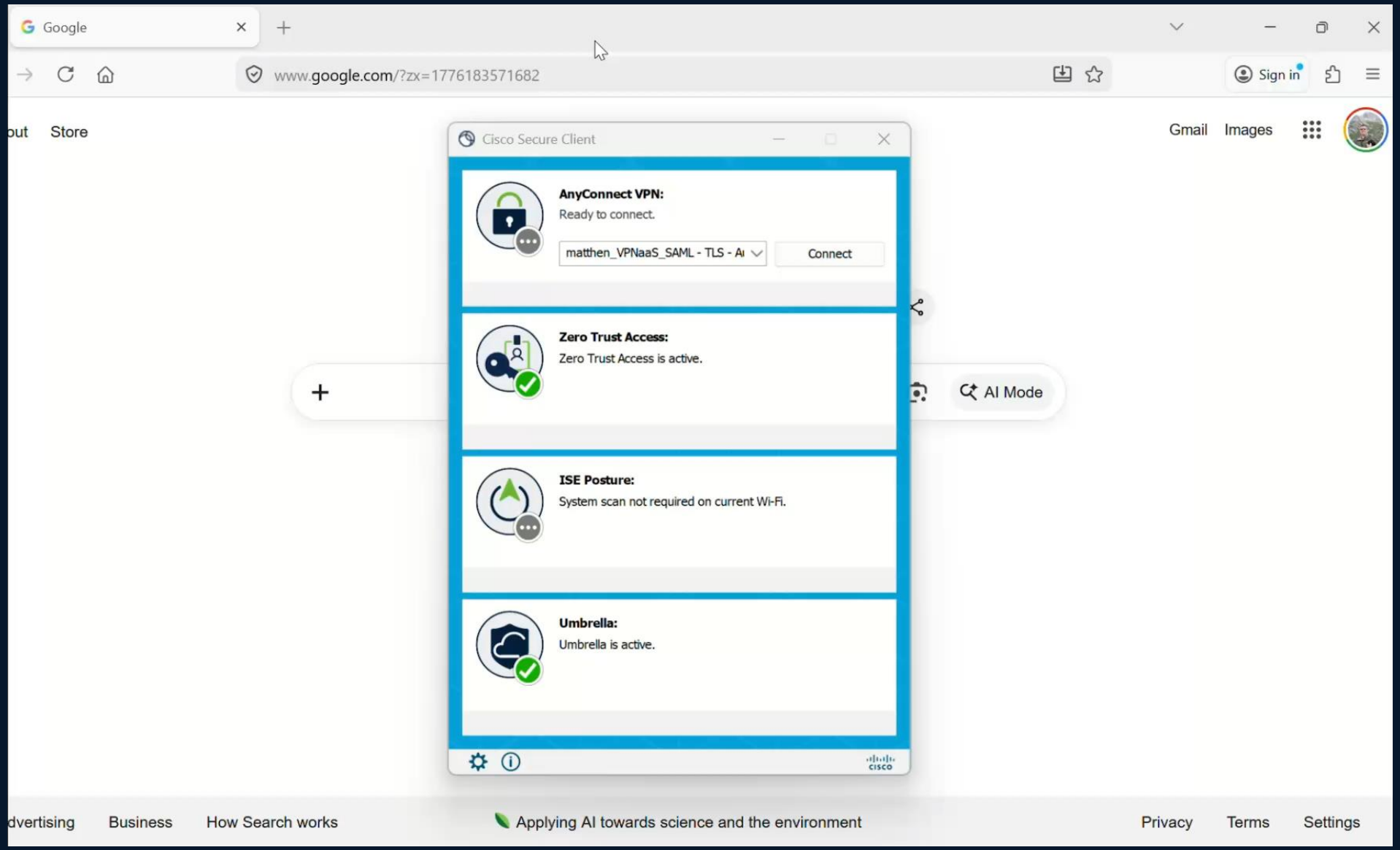
Hybrid Private Access for flexible enforcement

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

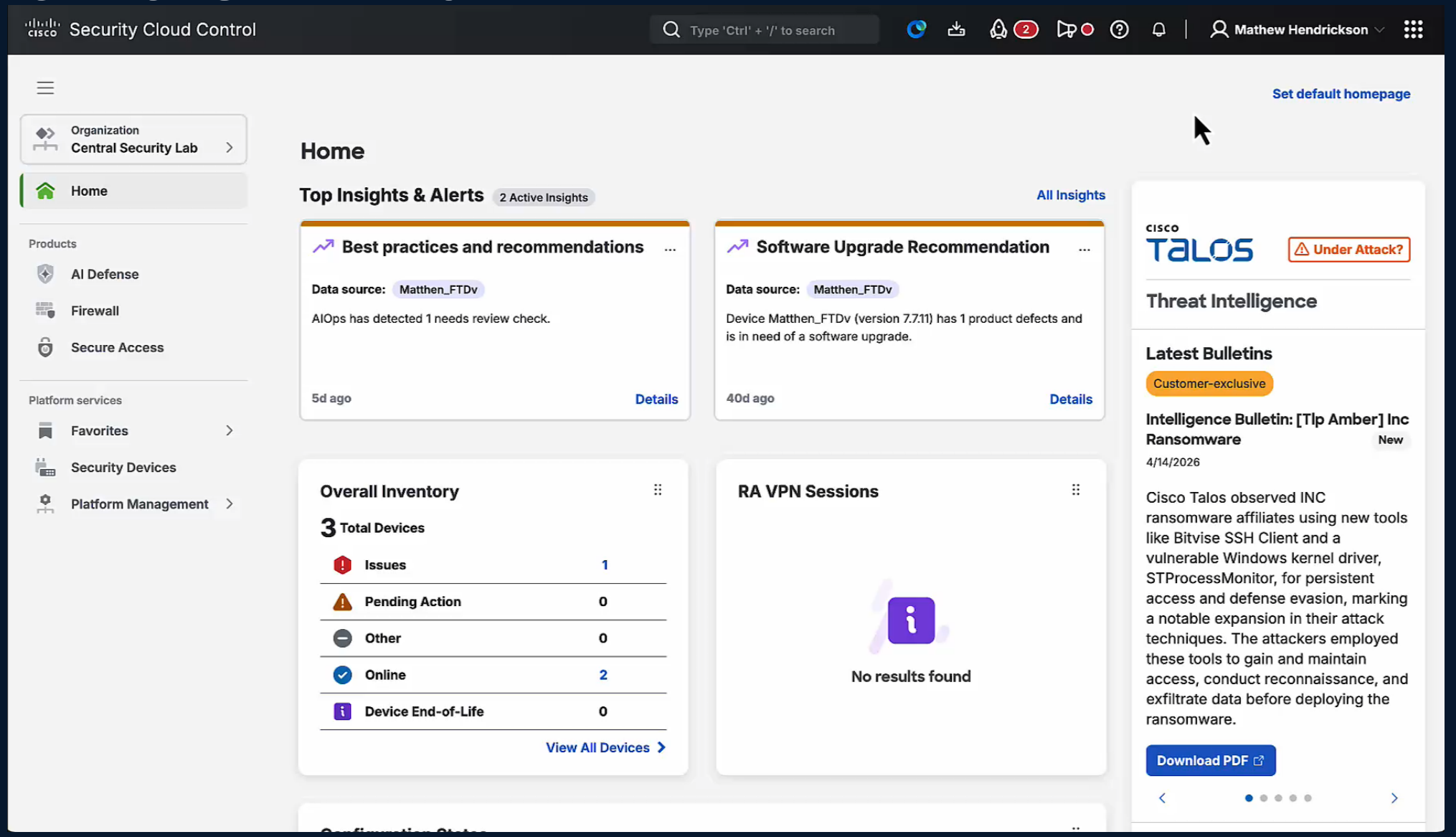


** Roadmap: policy enforcement on 8k routers

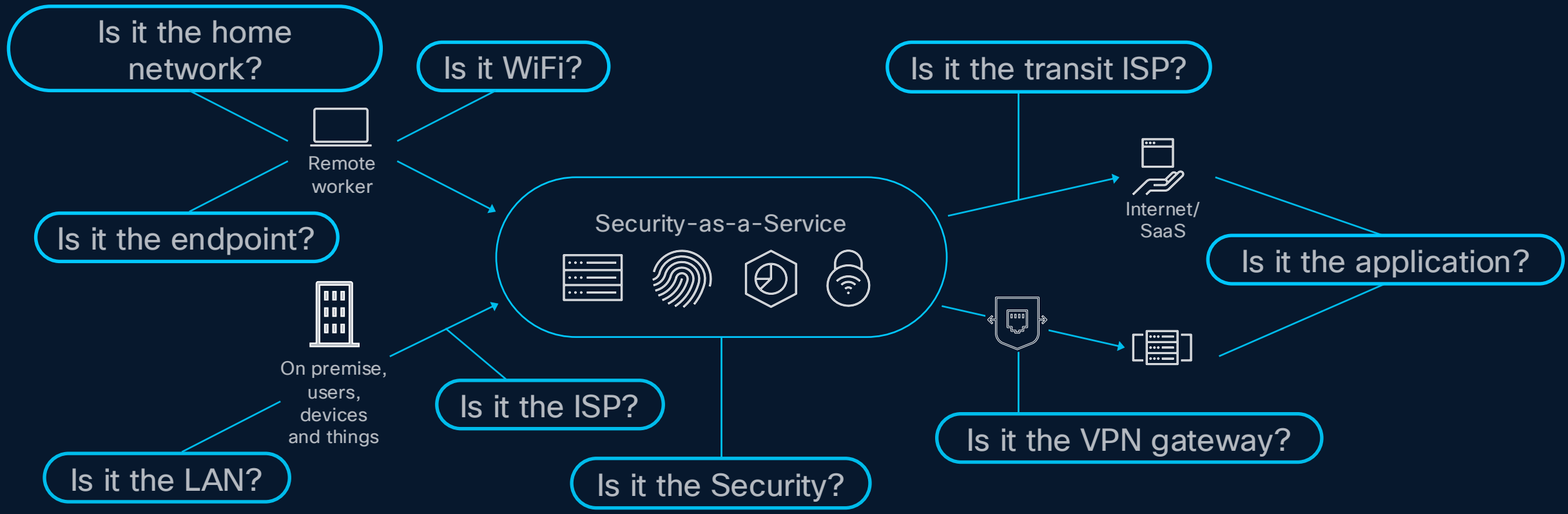
Demo Secure Private Access



Demo SPA Admin

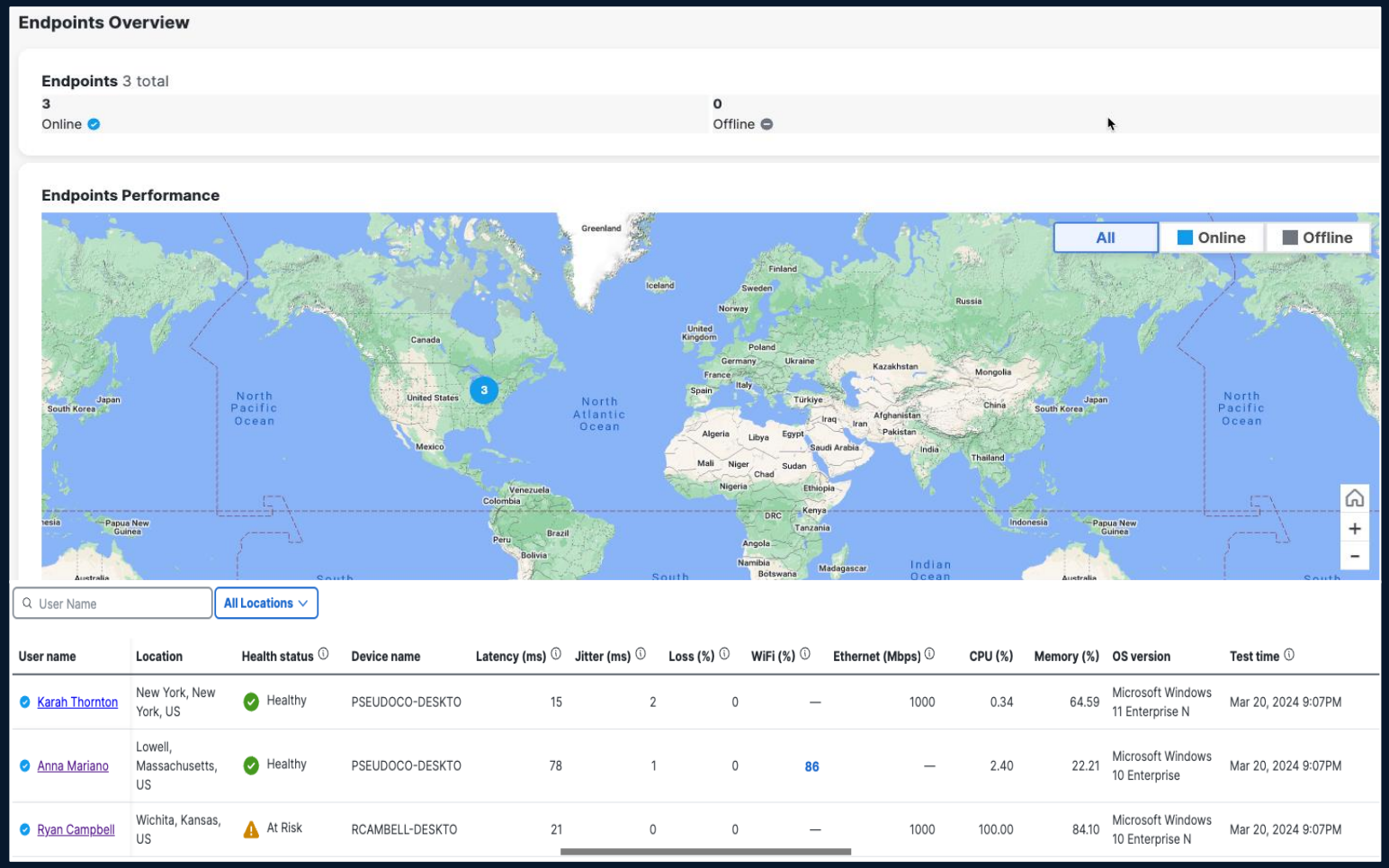


Troubleshooting the hybrid work experience



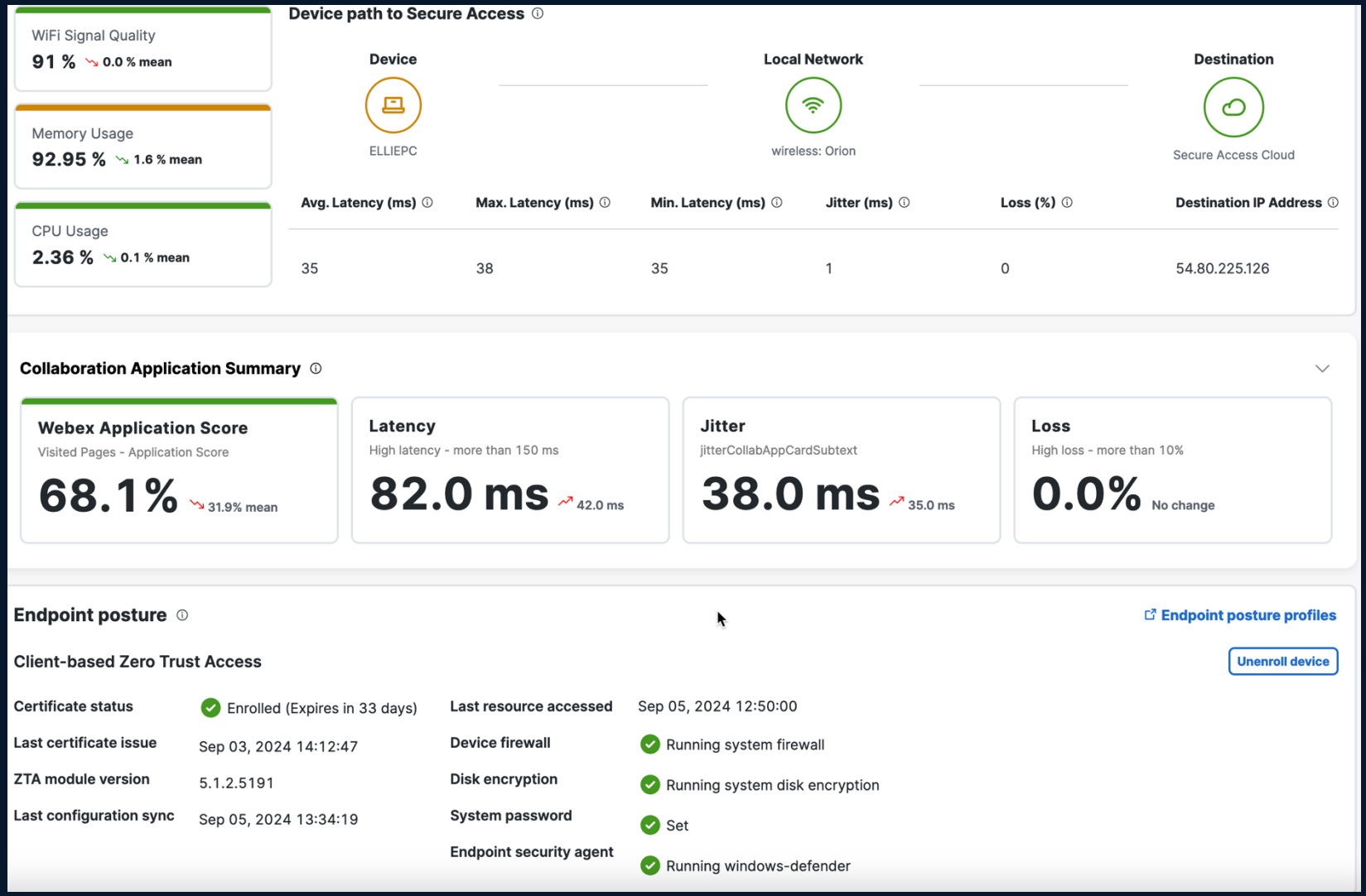
Secure Access Experience Insights

Monitor user digital experience without separate agents or management portals



- Global visibility of registered endpoint status
- Is part of the Cisco Secure Access dashboard
- Includes ThousandEyes Embedded Endpoint Agent(EPA) as a module in Cisco Secure Client

Secure Access Experience Insights



Cisco and Google Enhance Zero Trust Access

Google Chrome Enterprise

Browser-based security for web apps

+

Cisco Secure Access

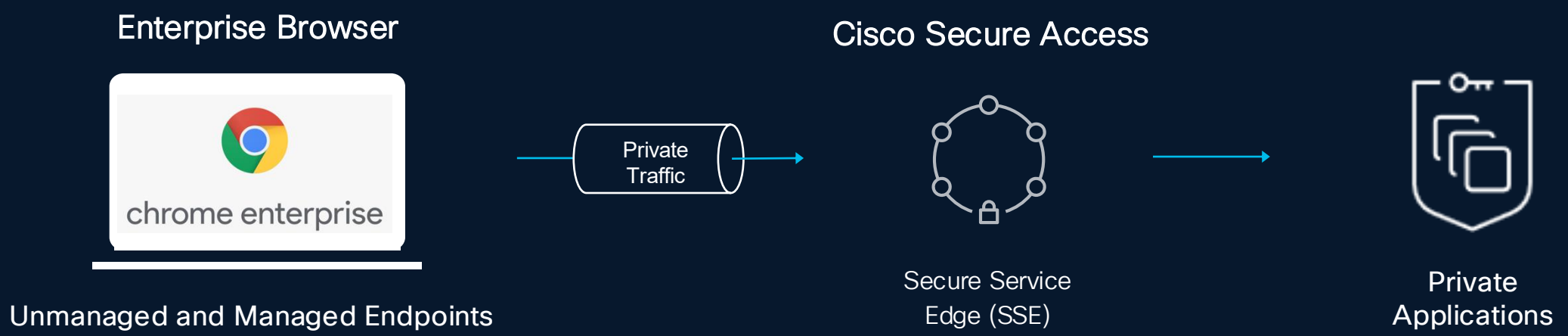
Cloud-based security for Private apps and more

DEVICE TRUST + SECURE ACCESS TO ALL APPS + EXPANSIVE TELEMETRY

cisco

Secure Access with Enterprise Browser

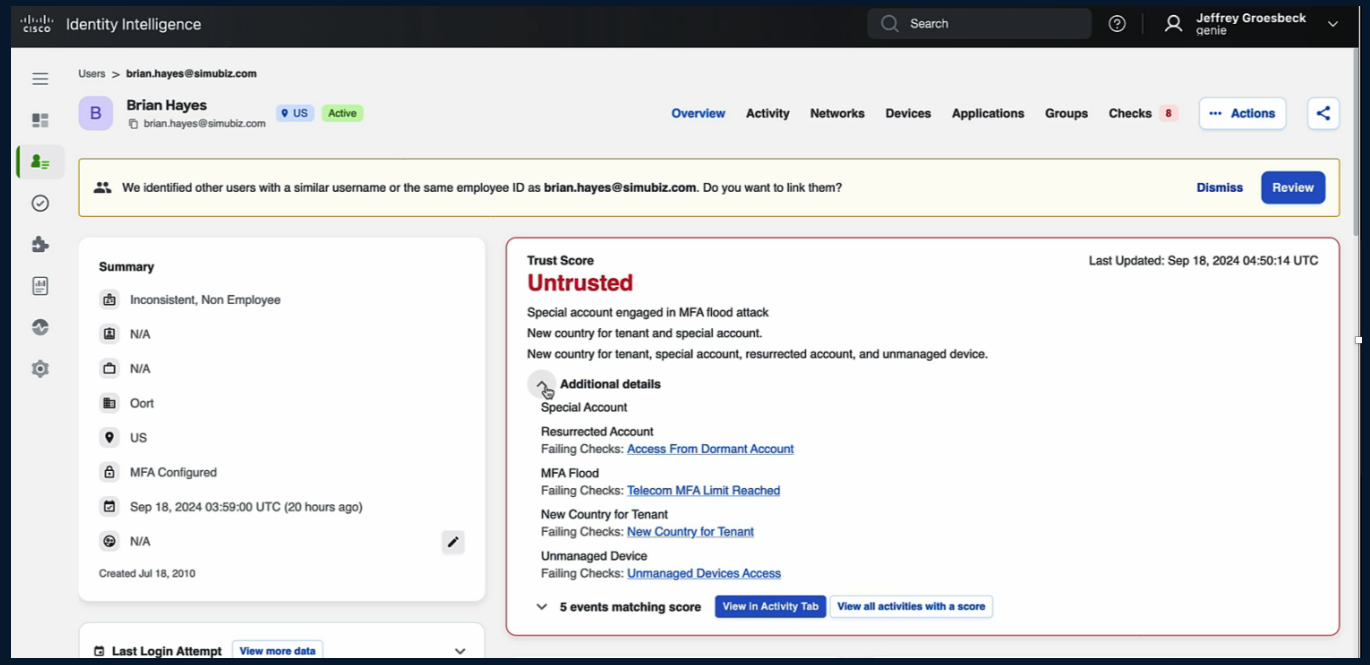
Zero Trust Access to Private Apps and Internet Apps



- 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

User Trust Score



User Trust Score

Identity Intelligence will be providing a user trust score for integrating solutions to leverage. Will be a single score, determined by a user's behaviors, actions and posture

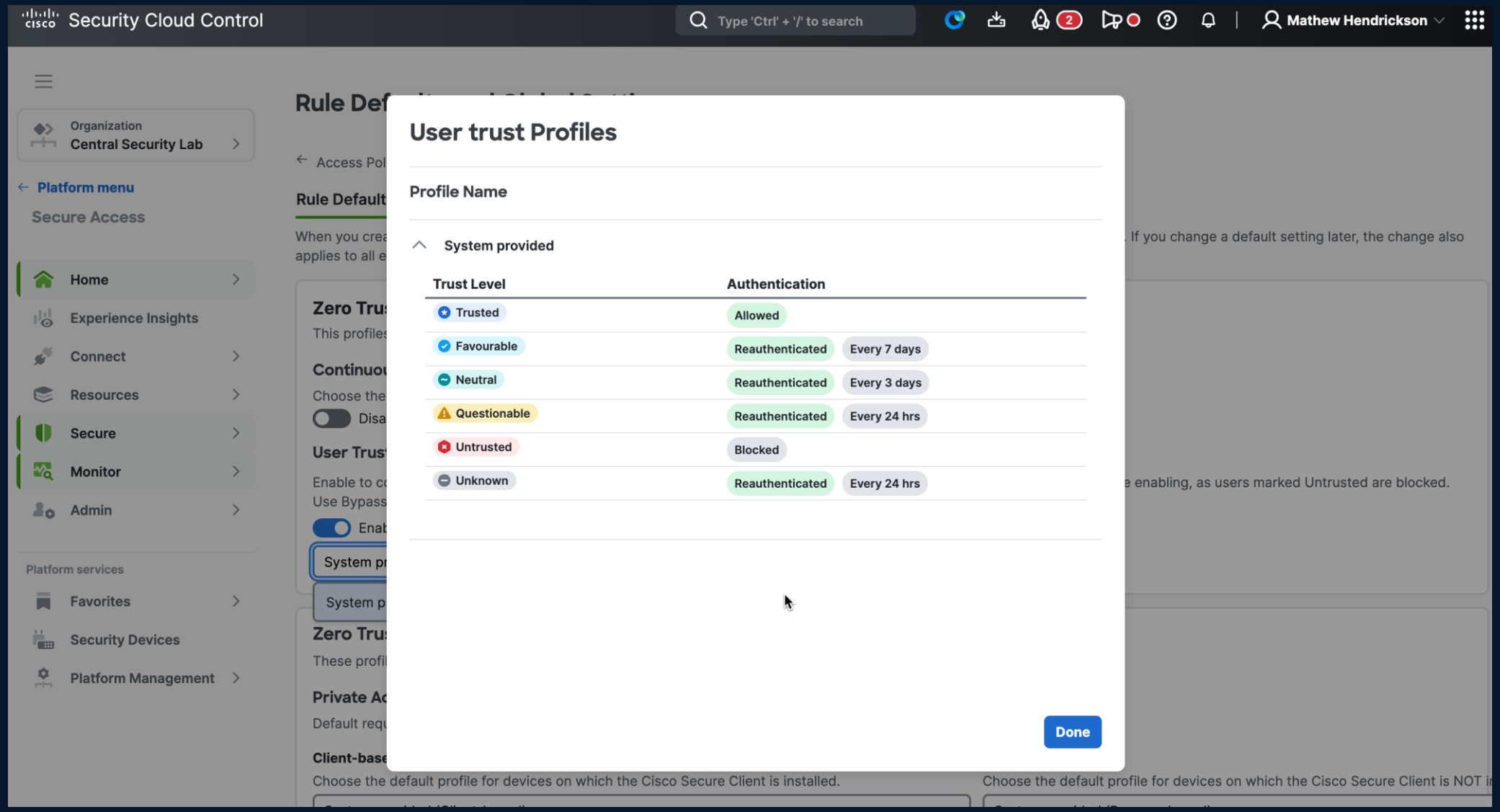
Easy Workflows

After assessment, seamlessly take response action from the console.

Key Scores

- Trusted
- Favorable
- Neutral
- Questionable
- Untrusted
- Unknown

User Trust Scores



Thank you


CISCO