

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

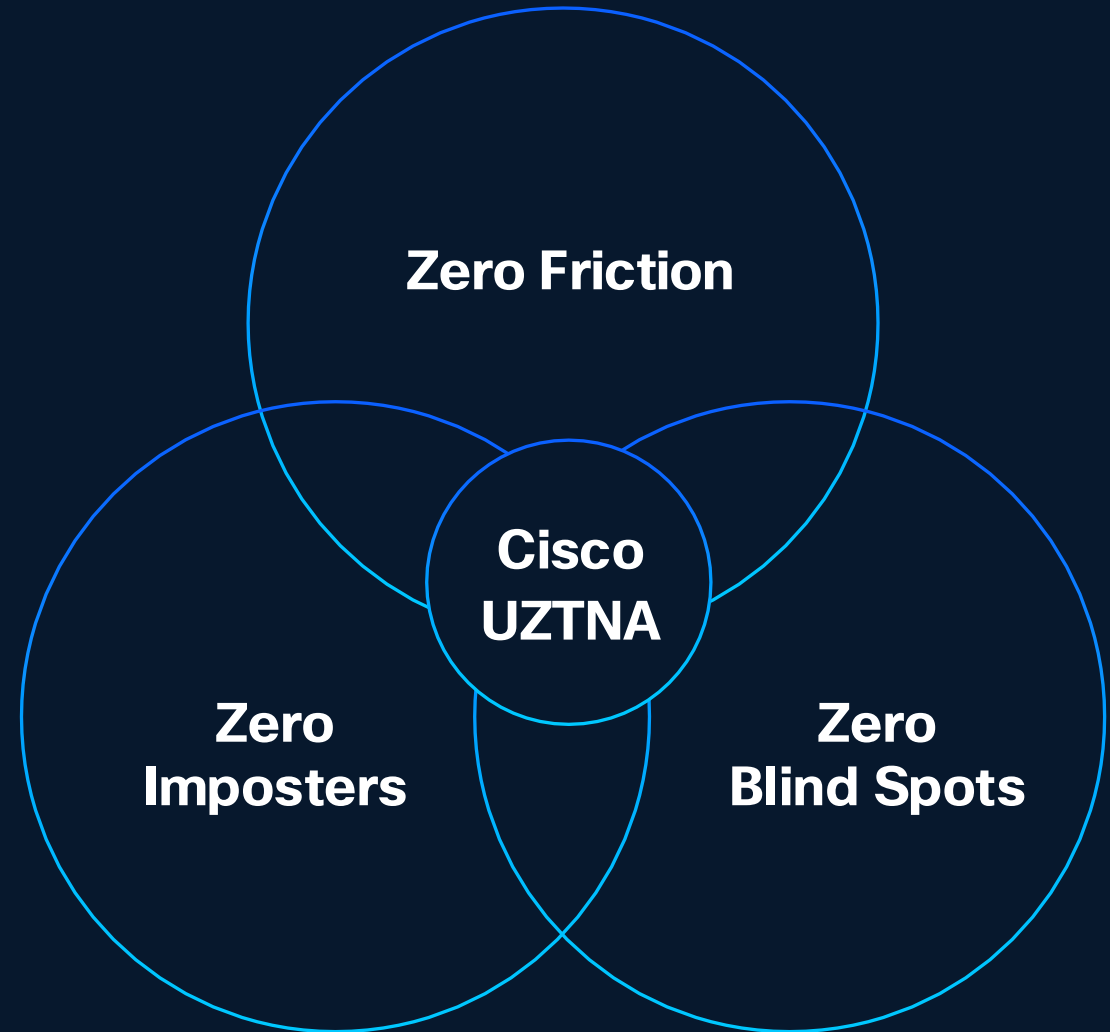
What is UZTNA?

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 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

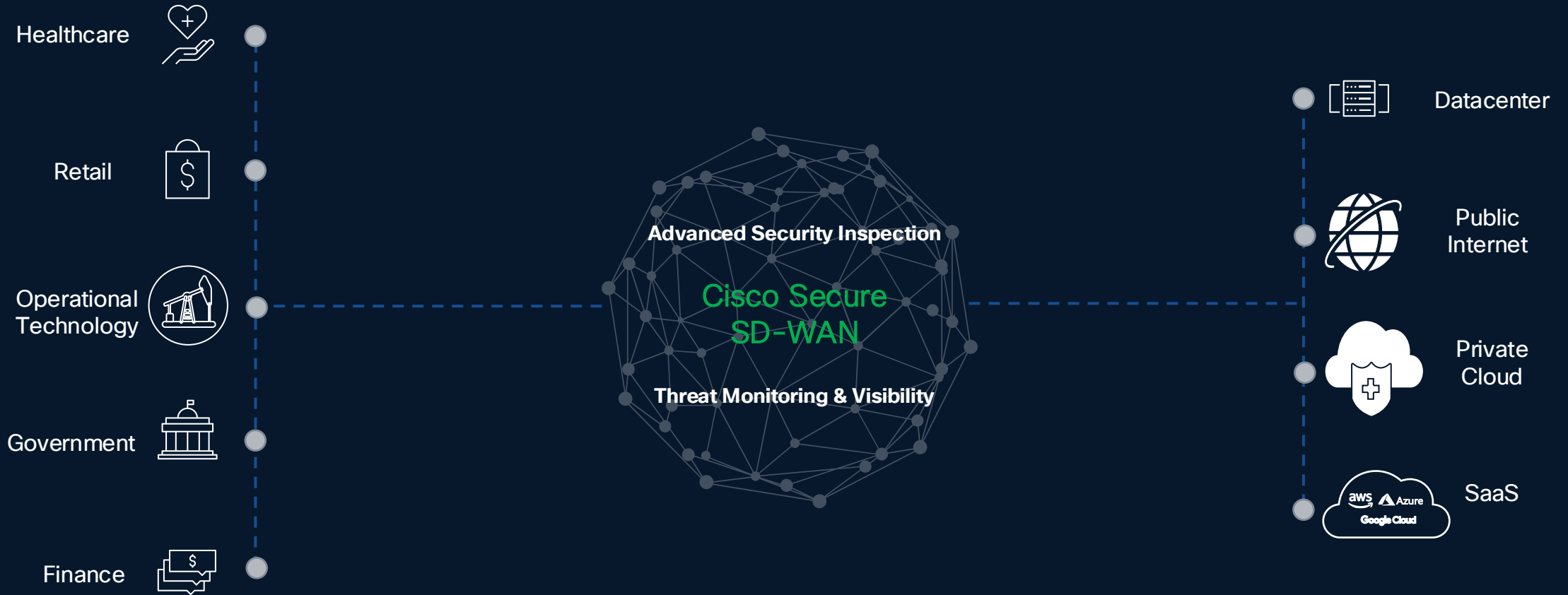


DUO MFA/SSO



CSPM

Across Markets, One Security Solution, Catalyst SD-WAN

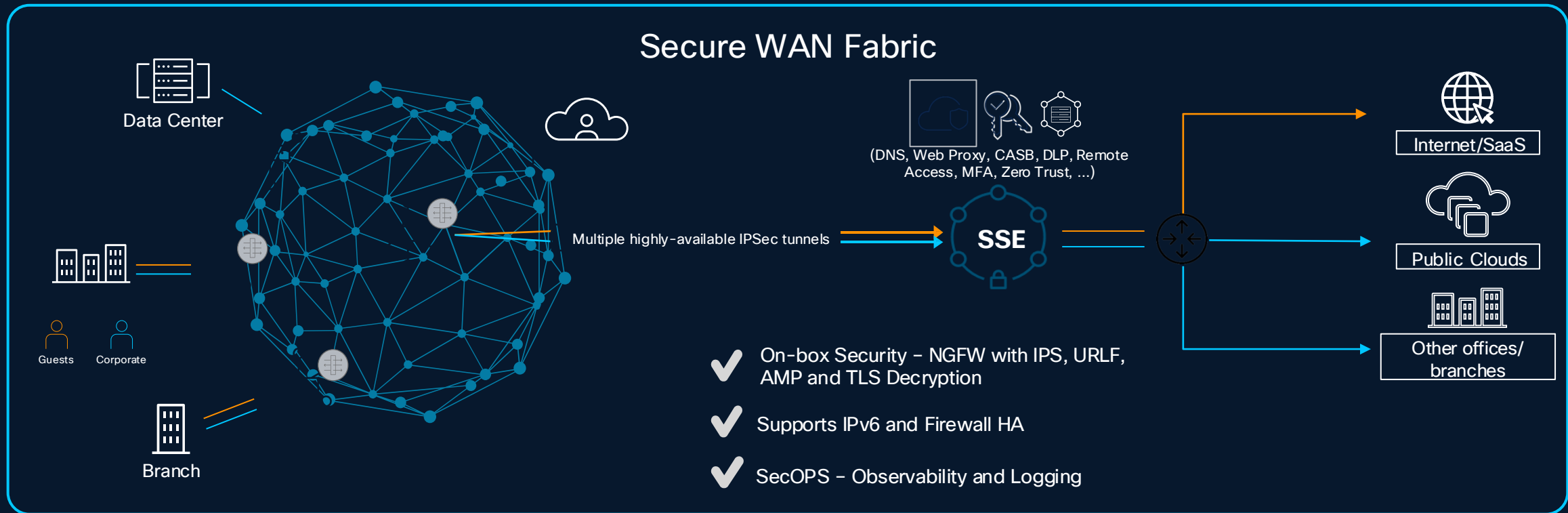


All Market Segments

Complete Security Portfolio

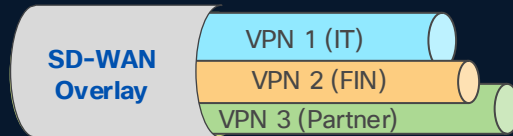
Any Destination

Cisco Secure WAN – Cloud Security



Cisco Secure WAN – Granular End-to-End Segmentation

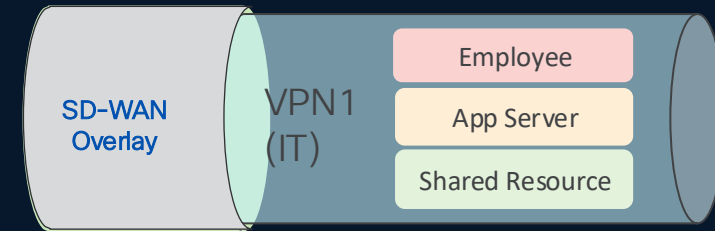
Macro Segmentation



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

Internet Connectivity



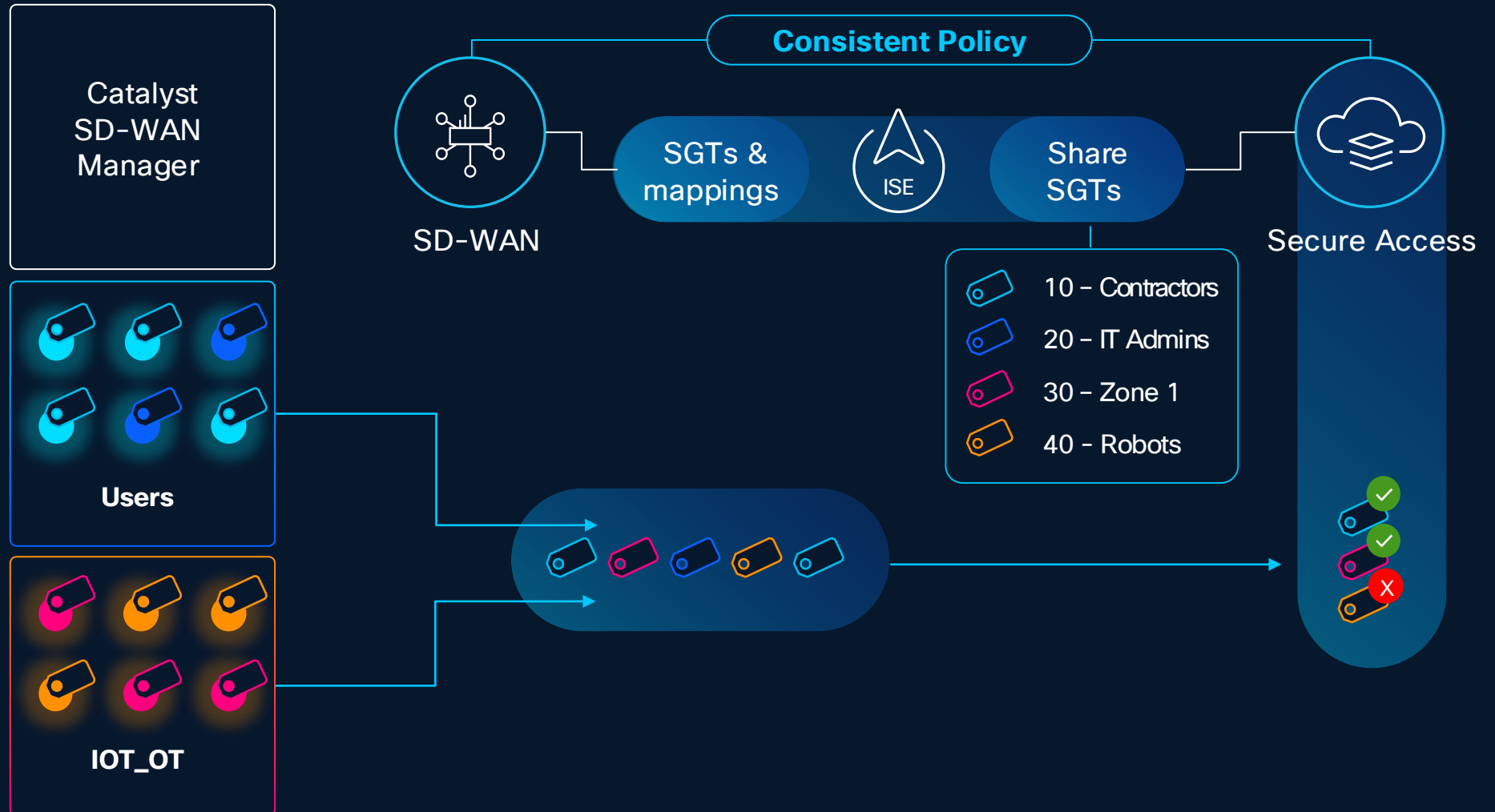
- Transparent user experience
- Trusted Network Detection
- Service managed client certificates with TPM-protected key storage

- 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

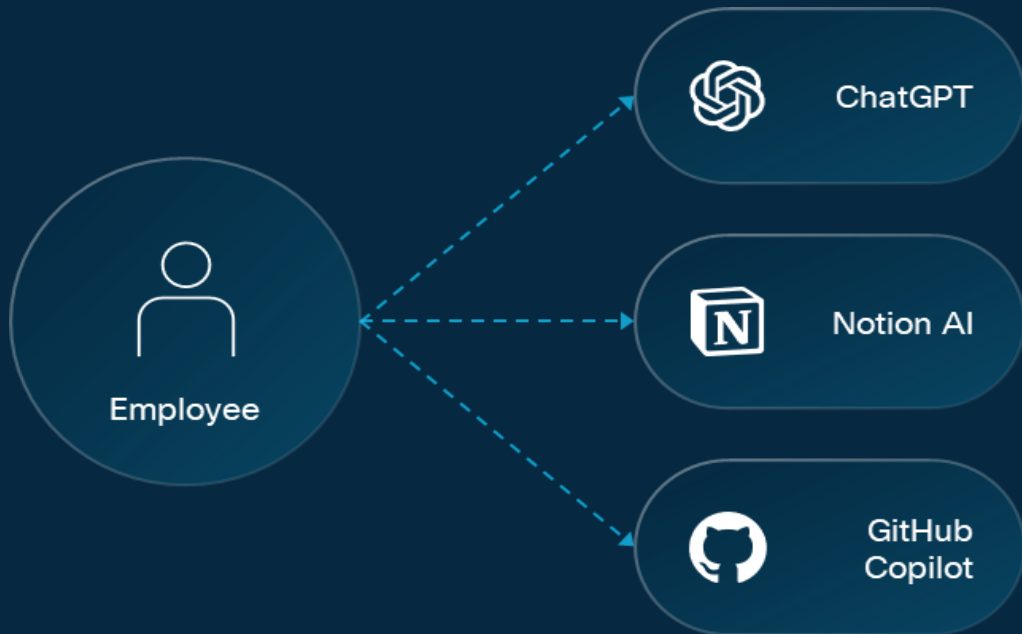
- SGT Based Policy across network & Cloud
- Maintain micro segmentation through Secure Access
- Uniquely identify devices and traffic based on context from ISE
- Apply policy to SGT Based identity



Two distinct areas of AI risk

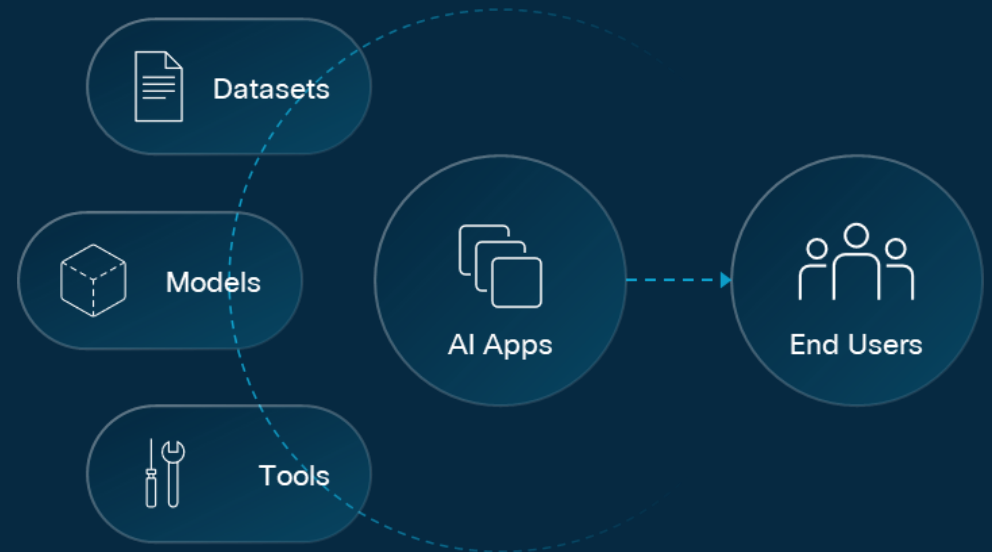
Third-Party AI Tools – AI Access with Secure Access

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.



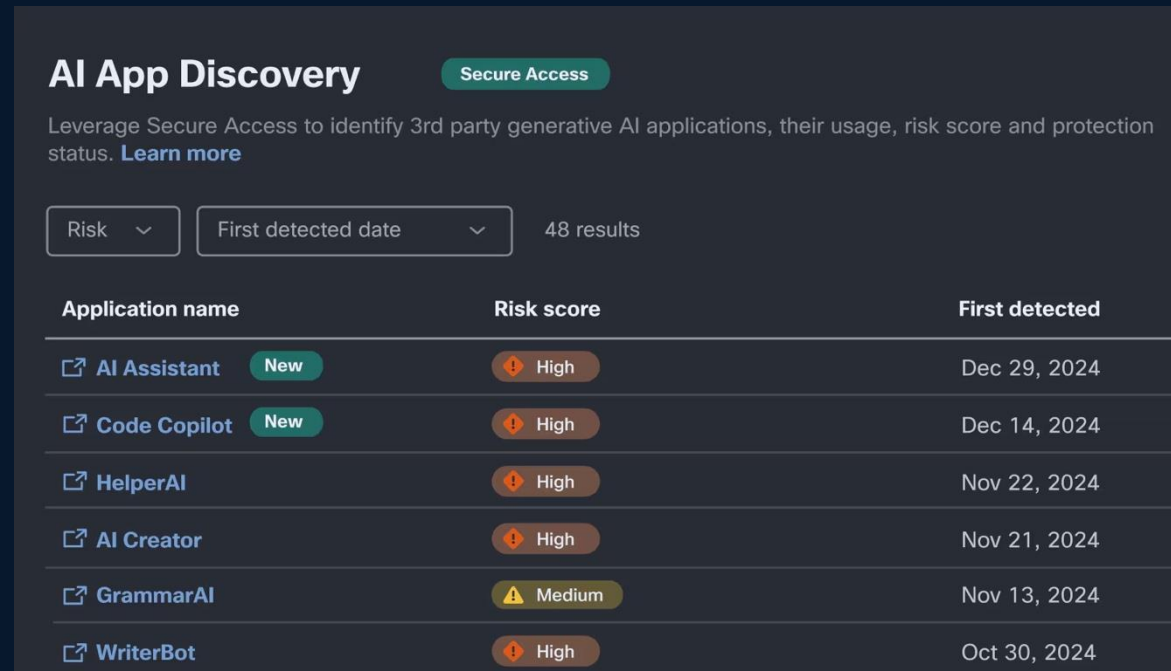
AI Access – Control Sanctioned and Unsanctioned GenAI apps

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



AI App Discovery Secure Access

Leverage Secure Access to identify 3rd party generative AI applications, their usage, risk score and protection status. [Learn more](#)

Risk First detected date 48 results

Application name	Risk score	First detected
AI Assistant New	High	Dec 29, 2024
Code Copilot New	High	Dec 14, 2024
HelperAI	High	Nov 22, 2024
AI Creator	High	Nov 21, 2024
GrammarAI	Medium	Nov 13, 2024
WriterBot	High	Oct 30, 2024

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

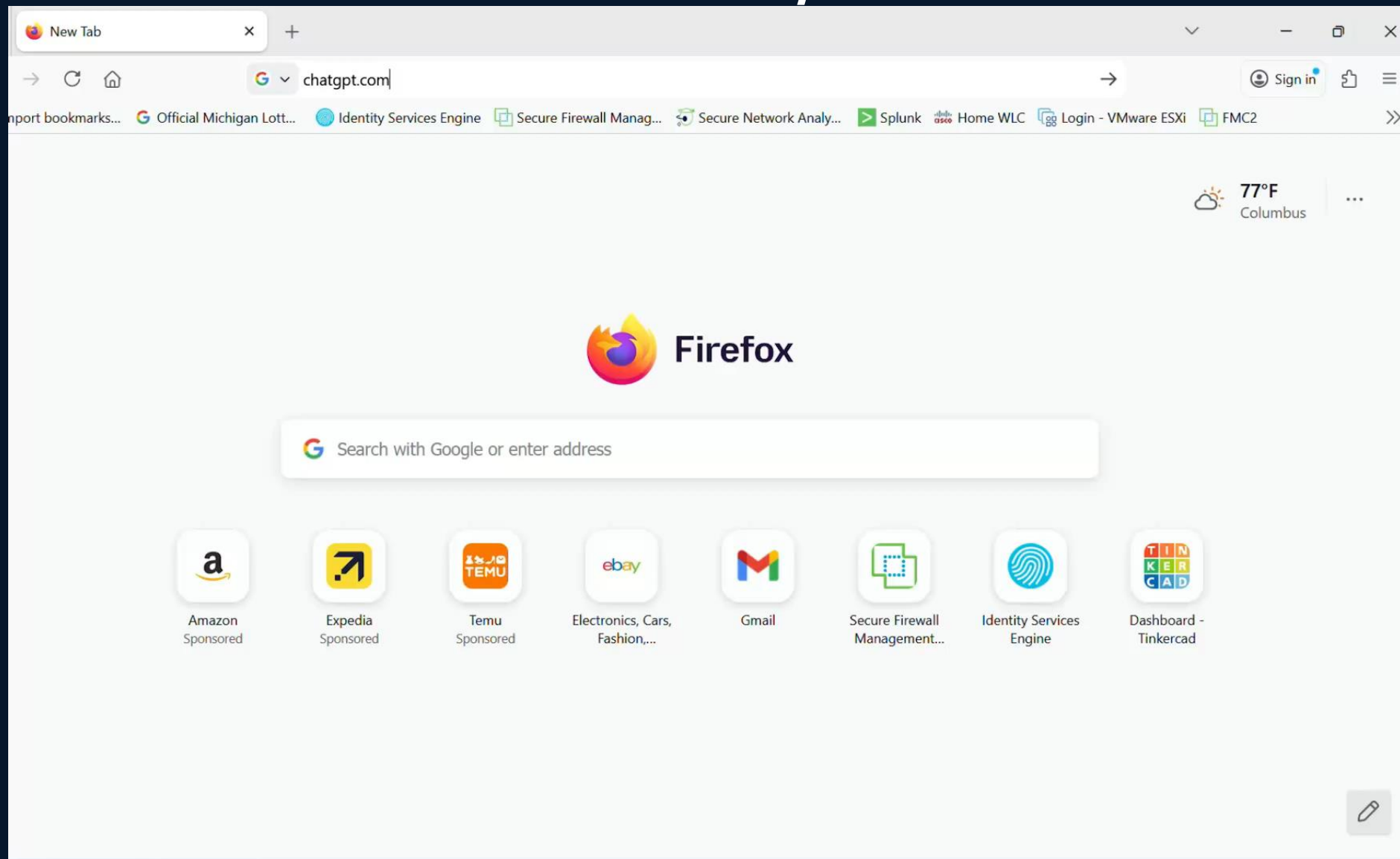
Safety

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

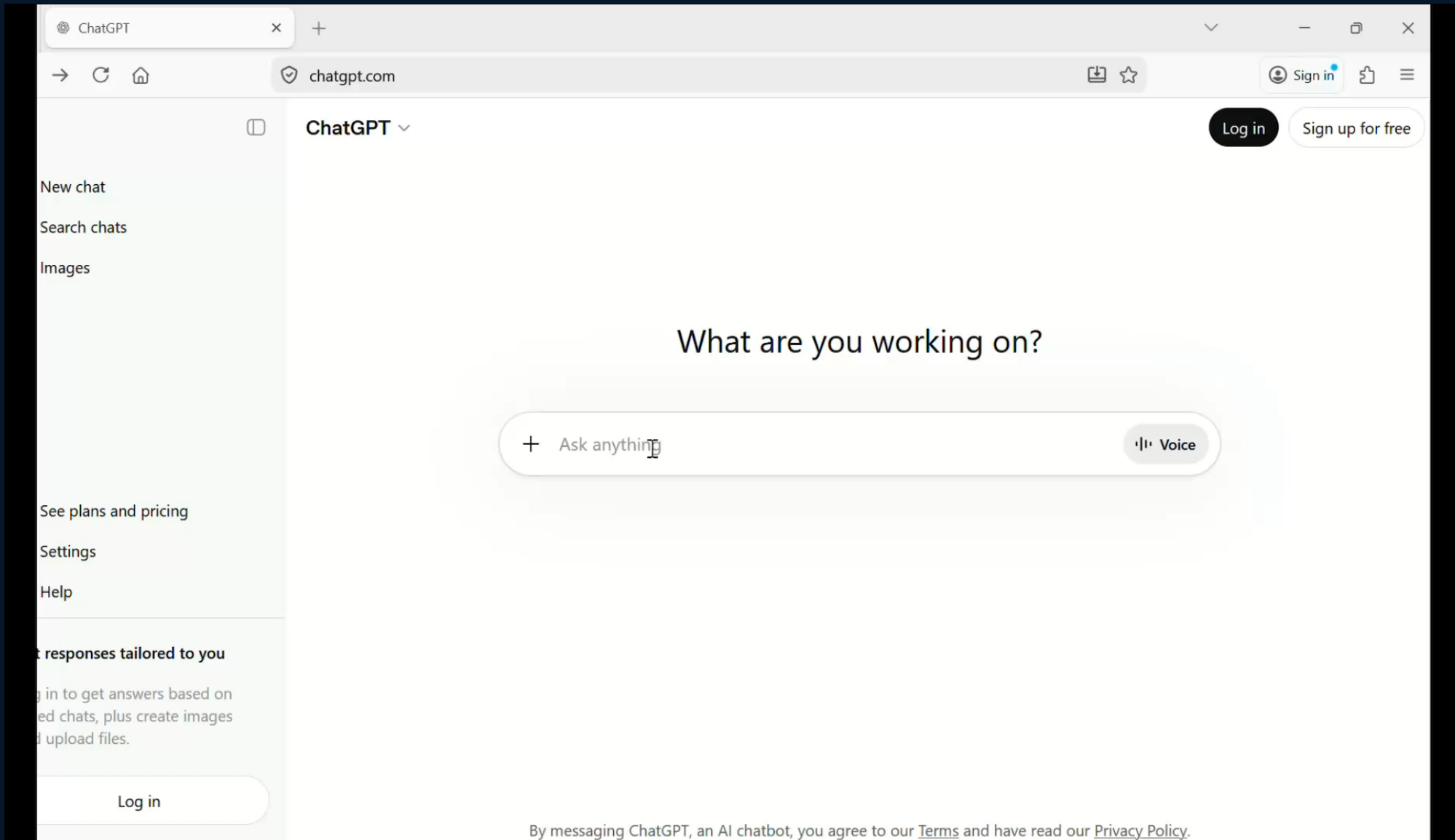
Map guardrails to standards and frameworks like:



Demo - SIA AI Access/DLP CC



Demo AI Access Guardrails



Demo AI Access Reporting

Security Cloud Control | Type 'Ctrl' + '/' to search | Mathew Hendrickson

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	Resource connector groups	FTDs
2 Disconnected (Warning)	1 Connected (Success)	1 Synced (Success)
3 Connected (Success)		

Data Transfer

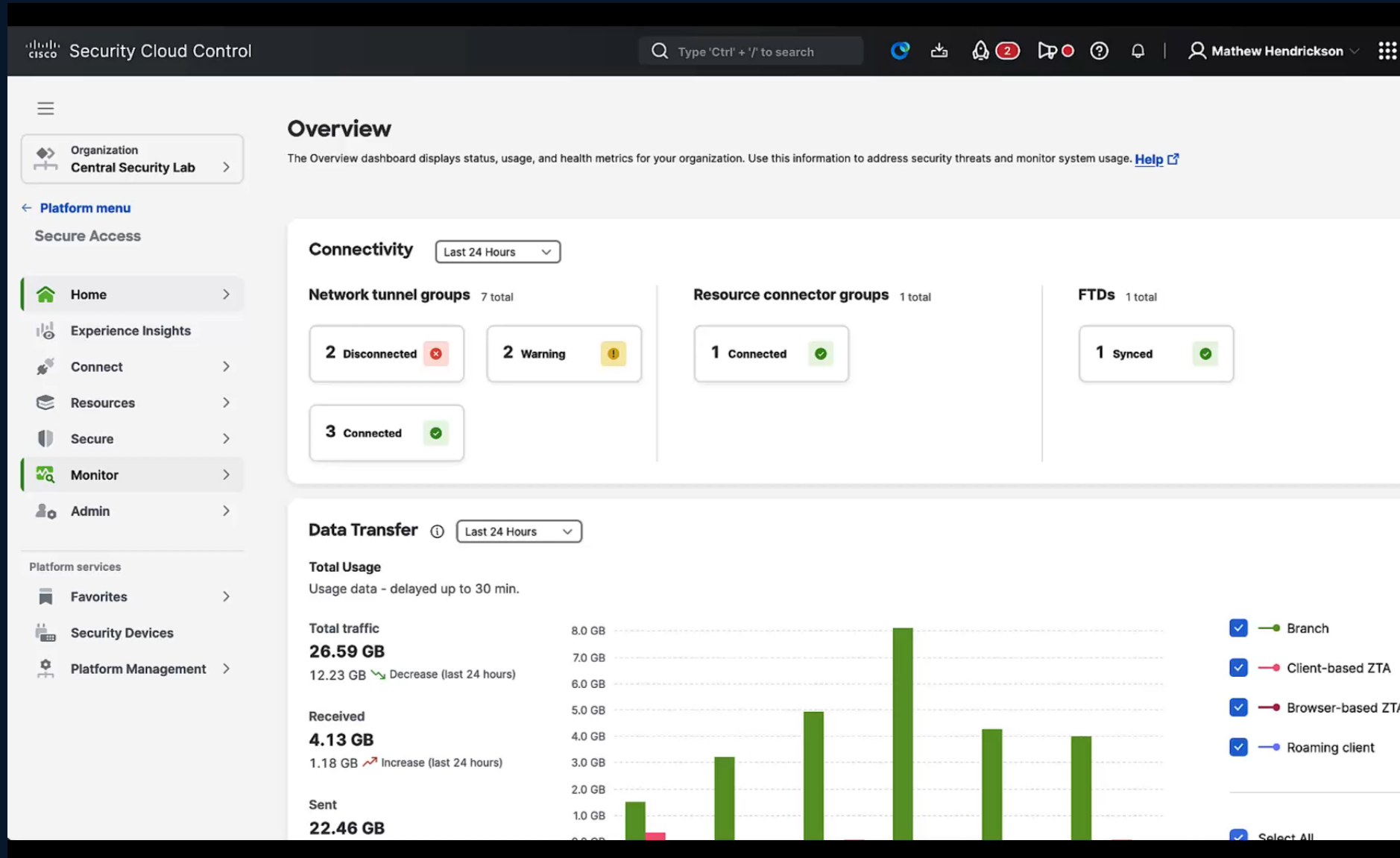
Last 24 Hours

Total Usage
Usage data - delayed up to 30 min.

Metric	Value	Trend
Total traffic	38.41 GB	13.77 GB Decrease (last 24 hours)
Received	2.99 GB	1.91 GB Decrease (last 24 hours)
Sent	35.41 GB	

Legend: Branch, Roaming client, Client-based ZTA, Browser-based ZTA, Select All

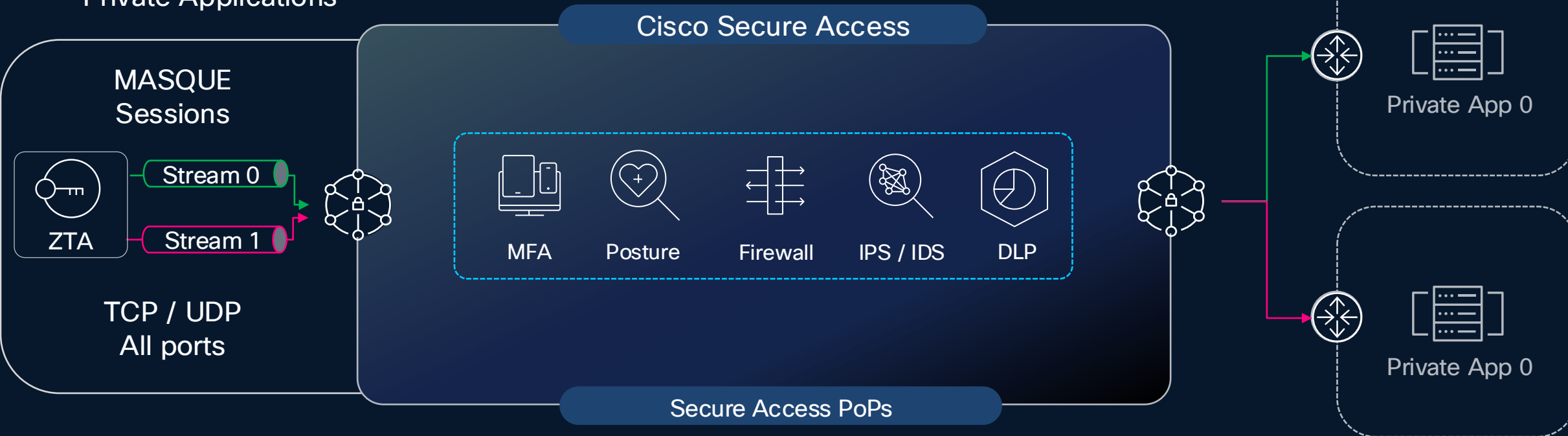
Demo SGTs in Secure Access



Zero Trust Access (SPA)

Client-based Zero Trust Access

Private Applications

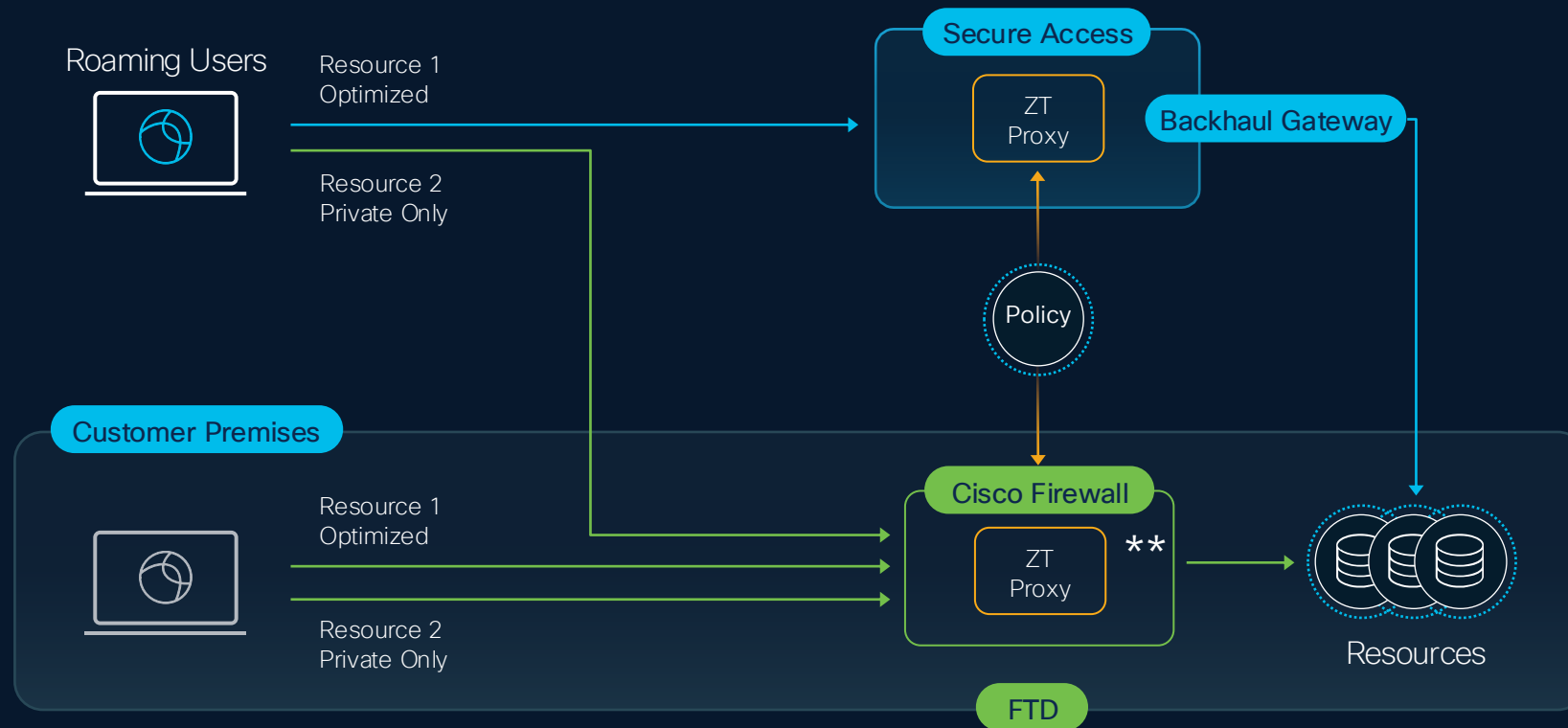


- Transparent user experience
- Forward proxied resource access with coarse or fine-grained access control
- Service managed client certificates with TPM-protected key storage

- 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

The screenshot shows a web browser window with a Google search page in the background. Overlaid on the browser is the Cisco Secure Client application window. The client interface is divided into four main sections:

- AnyConnect VPN:** Shows a status of "Ready to connect." with a dropdown menu set to "matthen_VPNaaS_SAML - TLS - Ai" and a "Connect" button.
- Zero Trust Access:** Shows a status of "Zero Trust Access is active." with a green checkmark icon.
- ISE Posture:** Shows a status of "System scan not required on current Wi-Fi." with a green checkmark icon.
- Umbrella:** Shows a status of "Umbrella is active." with a green checkmark icon.

At the bottom of the client window, there are settings and information icons on the left and the Cisco logo on the right. The background browser page shows the Google search interface with a "Sign in" button and various navigation links like "Gmail" and "Images".

Demo SPA Admin

Security Cloud Control

Type 'Ctrl' + '/' to search

Mathew Hendrickson

Set default homepage

Home

Top Insights & Alerts 2 Active Insights [All Insights](#)

Best practices and recommendations

Data source: Matthen_FTDv

AI Ops has detected 1 needs review check.

5d ago [Details](#)

Software Upgrade Recommendation

Data source: Matthen_FTDv

Device Matthen_FTDv (version 7.7.11) has 1 product defects and is in need of a software upgrade.

40d ago [Details](#)

Overall Inventory

3 Total Devices

Issues	1
Pending Action	0
Other	0
Online	2
Device End-of-Life	0

[View All Devices](#)

RA VPN Sessions

No results found

Threat Intelligence

Latest Bulletins

Customer-exclusive

Intelligence Bulletin: [Tip Amber] Inc Ransomware

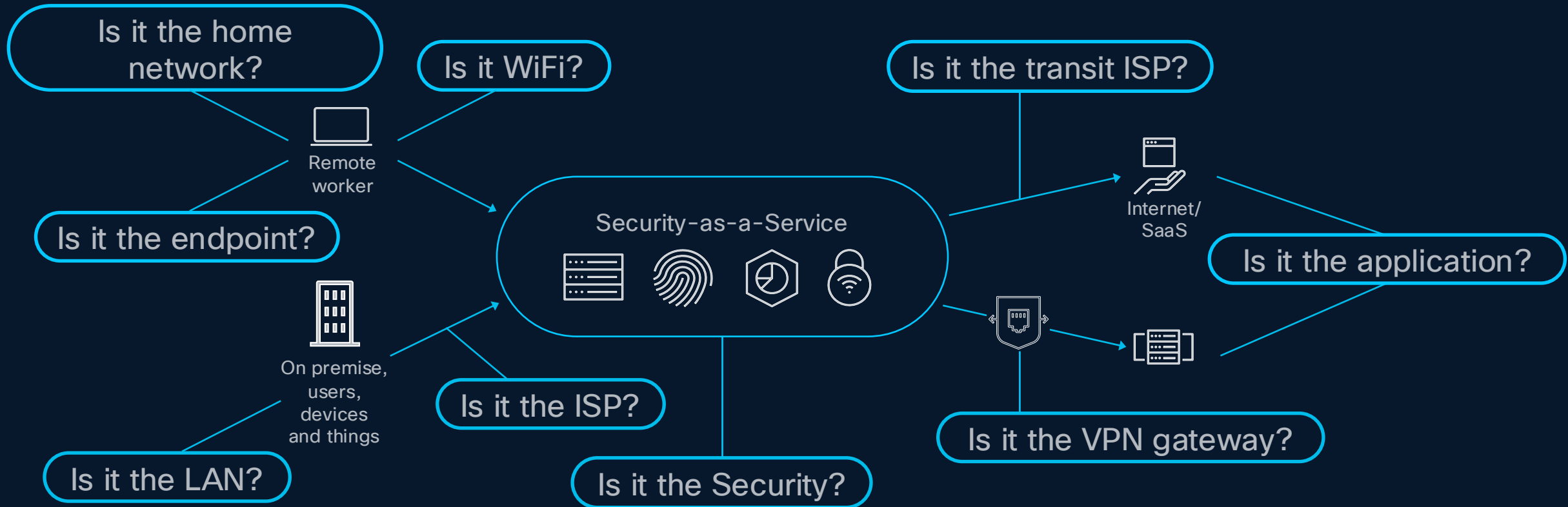
New

4/14/2026

Cisco Talos observed INC ransomware affiliates using new tools like Bitvise SSH Client and a vulnerable Windows kernel driver, STProcessMonitor, for persistent access and defense evasion, marking a notable expansion in their attack techniques. The attackers employed these tools to gain and maintain access, conduct reconnaissance, and exfiltrate data before deploying the ransomware.

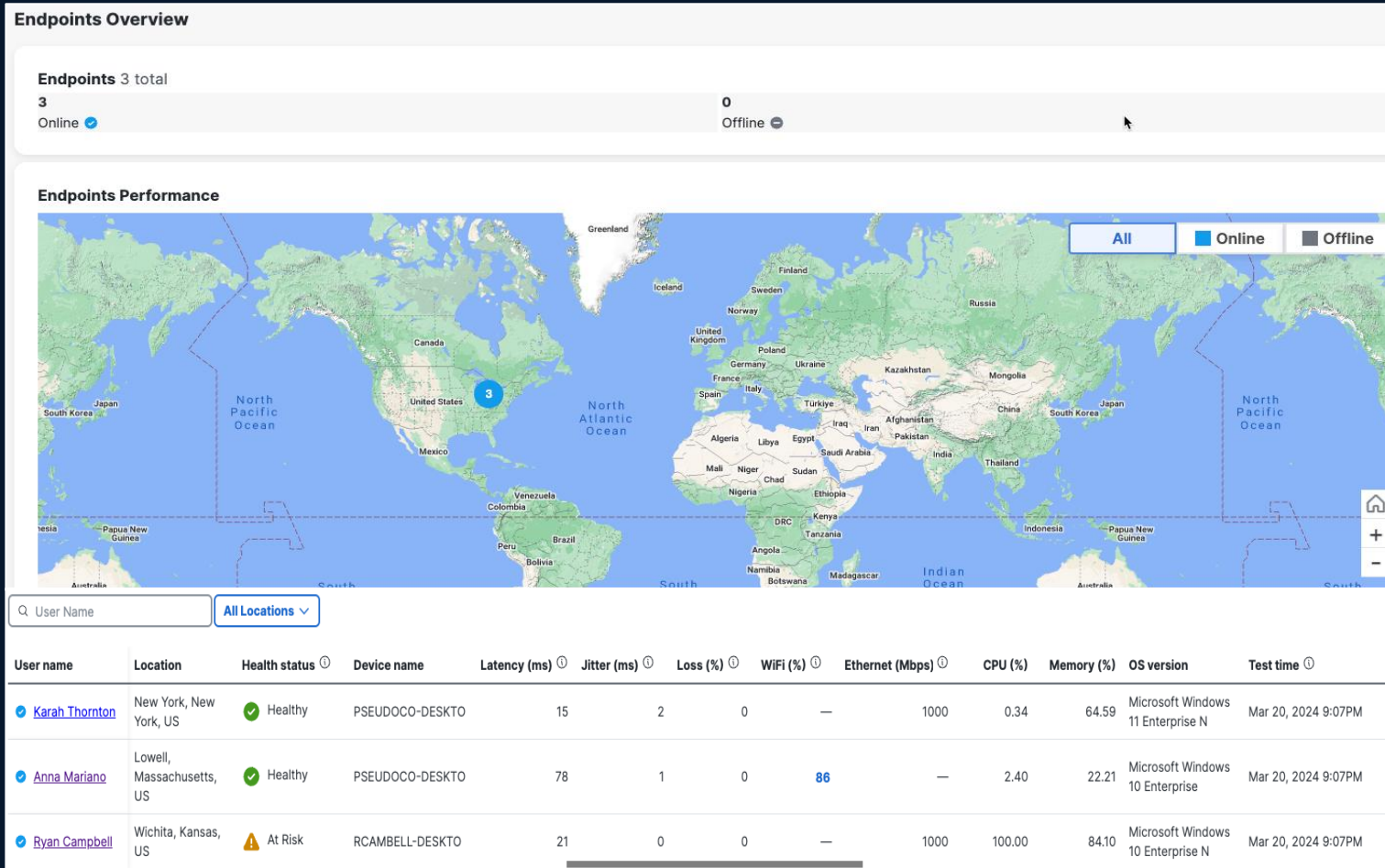
[Download PDF](#)

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


WiFi Signal Quality
91 % ↘ 0.0 % mean

Memory Usage
92.95 % ↘ 1.6 % mean

CPU Usage
2.36 % ↘ 0.1 % mean


Device path to Secure Access ⓘ

Device




ELLIEPC

Local Network



wireless: Orion

Destination



Secure Access Cloud

Avg. Latency (ms) ⓘ	Max. Latency (ms) ⓘ	Min. Latency (ms) ⓘ	Jitter (ms) ⓘ	Loss (%) ⓘ	Destination IP Address ⓘ
35	38	35	1	0	54.80.225.126

Collaboration Application Summary ⓘ

Webex Application Score
Visited Pages - Application Score

68.1%

↘ 31.9% mean

Latency
High latency - more than 150 ms

82.0 ms

↗ 42.0 ms

Jitter
jitterCollabAppCardSubtext

38.0 ms

↗ 35.0 ms

Loss
High loss - more than 10%

0.0%

No change

Endpoint posture ⓘ


Client-based Zero Trust Access

[Endpoint posture profiles](#)

[Unenroll device](#)

Certificate status	✔ Enrolled (Expires in 33 days)	Last resource accessed	Sep 05, 2024 12:50:00
Last certificate issue	Sep 03, 2024 14:12:47	Device firewall	✔ Running system firewall
ZTA module version	5.1.2.5191	Disk encryption	✔ Running system disk encryption
Last configuration sync	Sep 05, 2024 13:34:19	System password	✔ Set
		Endpoint security agent	✔ Running windows-defender

© 2025 Cisco and/or its affiliates. All rights reserved.



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

User Trust Score

The screenshot shows the Cisco Identity Intelligence interface for user Brian Hayes (brian.hayes@simubiz.com). The user is active and located in the US. A notification at the top indicates that other users with similar usernames or employee IDs were identified, with options to 'Dismiss' or 'Review'. The 'Summary' section lists attributes: Inconsistent, Non Employee; N/A; N/A; Oort; US; MFA Configured; Last login on Sep 18, 2024 at 03:59:00 UTC (20 hours ago); and N/A. The 'Trust Score' section, last updated on Sep 18, 2024 at 04:50:14 UTC, is marked as 'Untrusted'. It lists several security events: 'Special account engaged in MFA flood attack', 'New country for tenant and special account', and 'New country for tenant, special account, resurrected account, and unmanaged device'. Under 'Additional details', it lists 'Special Account', 'Resurrected Account', 'MFA Flood', 'New Country for Tenant', and 'Unmanaged Device', each with associated failing checks and links for more information. At the bottom, it shows '5 events matching score' with buttons to 'View in Activity Tab' and 'View all activities with a 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

The screenshot shows the Cisco Security Cloud Control interface. A modal window titled "User trust Profiles" is open, displaying a table of trust levels and their corresponding authentication requirements. The background shows the "Rule Definition" page for "Secure Access".

Trust Level	Authentication
Trusted	Allowed
Favourable	Reauthenticated Every 7 days
Neutral	Reauthenticated Every 3 days
Questionable	Reauthenticated Every 24 hrs
Untrusted	Blocked
Unknown	Reauthenticated Every 24 hrs

The modal also includes a "Profile Name" input field and a "Done" button at the bottom right.

Thank you



