Simplifying The Hybrid Work Experience with Cisco Secure Access

Joe Abraham
Solutions Engineer – Security

CCIE | GCIA | CISSP
SLED West

December 3, 2024

cisco

What are you in for?

- Changing access requirements
- Where we are at
- Introducing Cisco Secure Access
- Secure Internet Access
- Private Application Access
- If you’re not ready for ZTNA
- Client-based access
- QUIC and MASQUE
- Clientless access
- Streamlining operations
- Putting it all together

About Me

Las Vegas, NV

Originally from Buffalo, NY, prior US Army Satcom Operator.

15 years in IT

Military, DoD contracting, Advanced Services

8 years with Cisco Security

Advanced Services/Customer Experience, XDR Incubation Team, SLED West Solutions Engineer

CCIE #62417 (R&S), GCIA, GCED

To name a few. Working on CCIE Security currently.

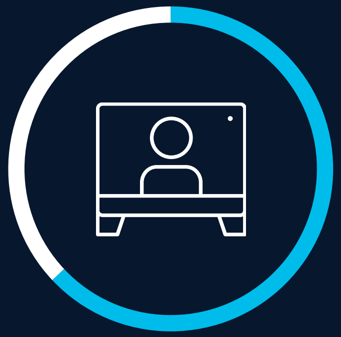
Movies, Tinkering

Family time, Marvel, home-renovation projects, other IT projects, educating and mentoring

Changing access requirements

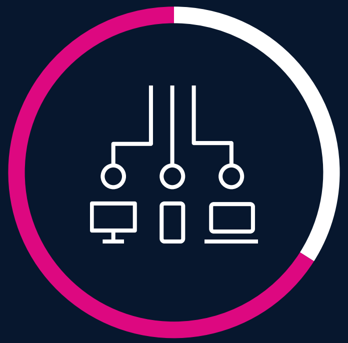
Hybrid work. Cloud/SaaS explosion. Unabated threats.

Need to reduce the attack surface and enforce least privilege access



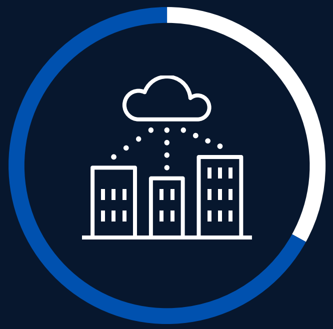
49%

Employees are remote/hybrid users



53%

Remote/hybrid workers using DIA



55%

Traffic to/from off-premises, cloud-based facilities

Capacity constraints. User frustration (opting out). Security gaps.

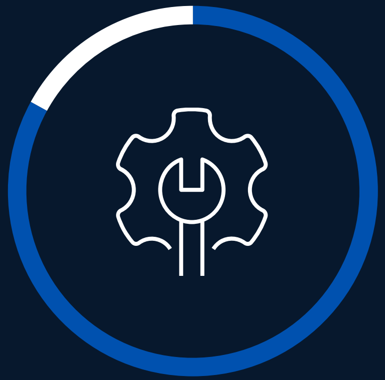
Reference: ESG SSE Survey, June 2023

What Organizations Have Done to Adapt

New high-volume remote/hybrid work environment

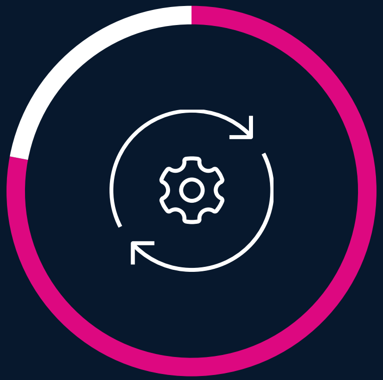
- Majority have ramped up their current on-premise VPN solution
- Some have adopted ZTNA (but still have on-premise VPN)

Why are users so frustrated?



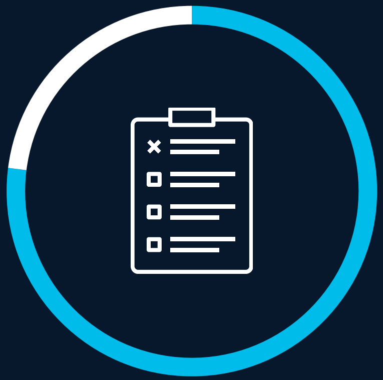
52%

Repeated authentication /verification



45%

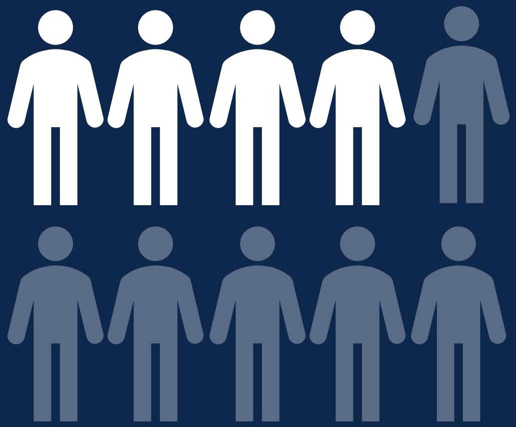
Having to choose method to connect based
on the app



50%

Number of steps to get to the app they need

User fatigue opens the door for successful attacks



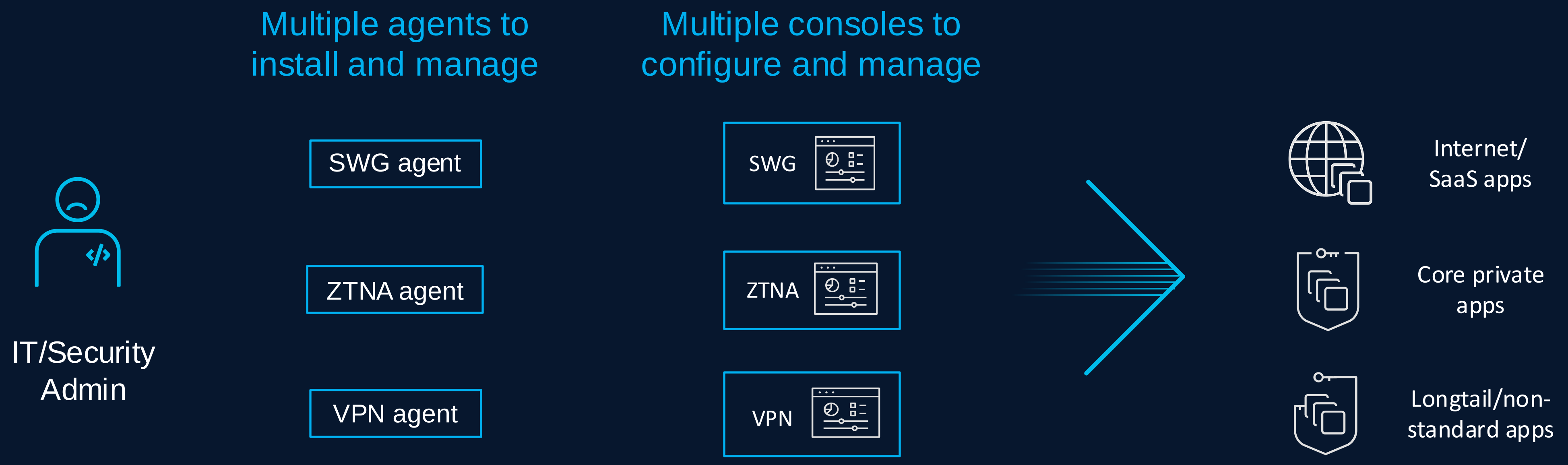
40%

Of remote/hybrid users have bypassed recommended VPN use in the past

Reference: ESG SSE Survey, June 2023

Operational and Security Challenges Remain for IT

Multi-vendor/tool approach increases complexity and overhead


Multiple agents to install and manage
Multiple consoles to configure and manage
IT/Security Admin
SWG agent
ZTNA agent
VPN agent
SWG
ZTNA
VPN
Internet/ SaaS apps
Core private apps
Longtail/non-standard apps

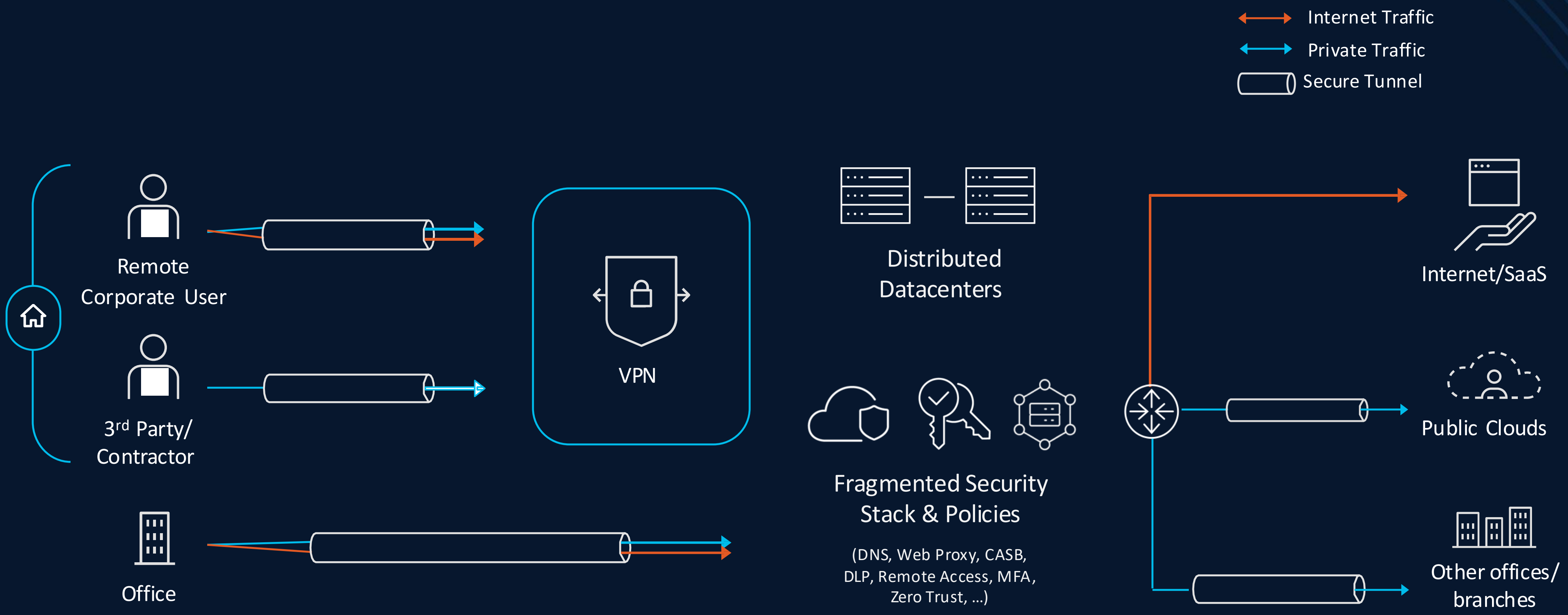
- Licenses/hardware
- Cumbersome deployments
- Increased attack surface

- App support limitations
- Suboptimal performance
- Additional user training and support

65% of enterprises plan on consolidating vendors for better risk posture

Where we are at

An architecture never designed for hybrid work



Poor user experience
Lower productivity

Large sets of individual solutions and vendors
Complexity of operations and costs

Gaps in security posture born out of complexity and fragmentation

What customers want in a remote access solution

Addresses IT/security challenges

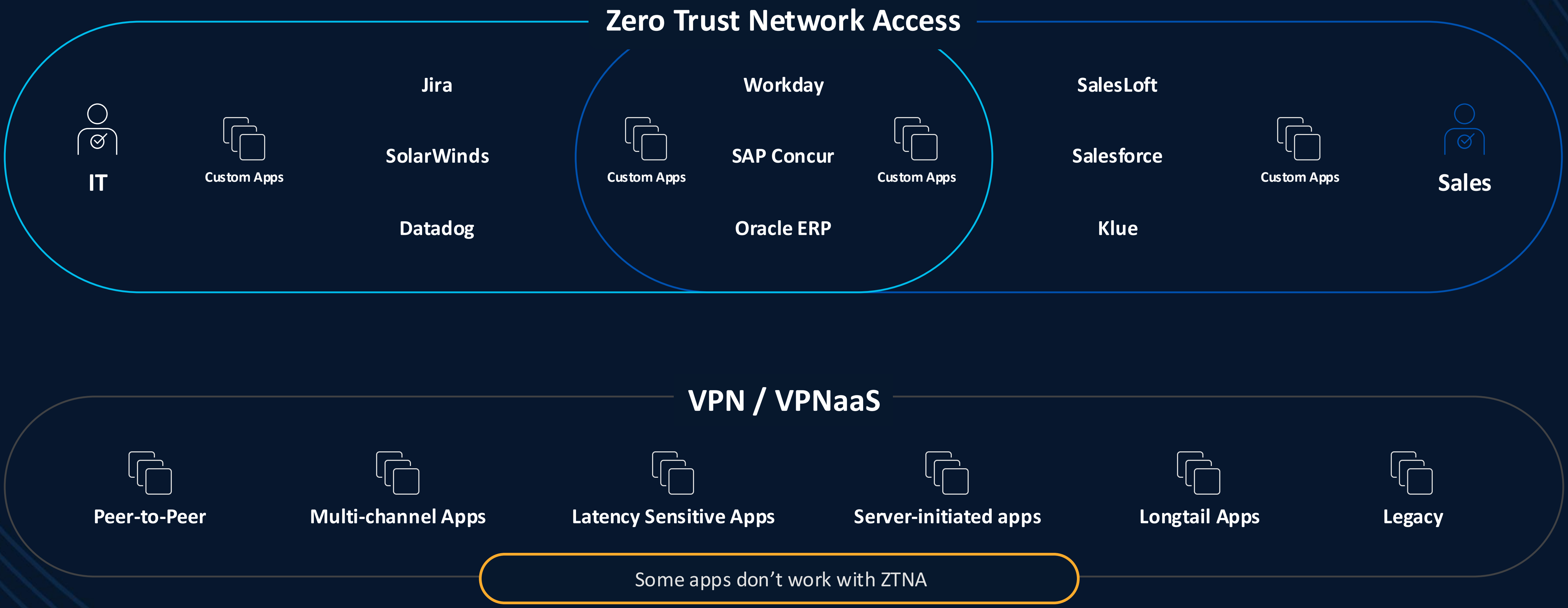
- Security for all apps (not some)
- Simplified deployment and configuration
- Unified security platform with one console
- Obfuscate resources

Addresses user challenges

- Simple user experience with seamless access to private/SaaS apps, internet
- No need to know if/when to use VPN
- Faster performance
- Intelligent, not highly-repetitive authentication tasks

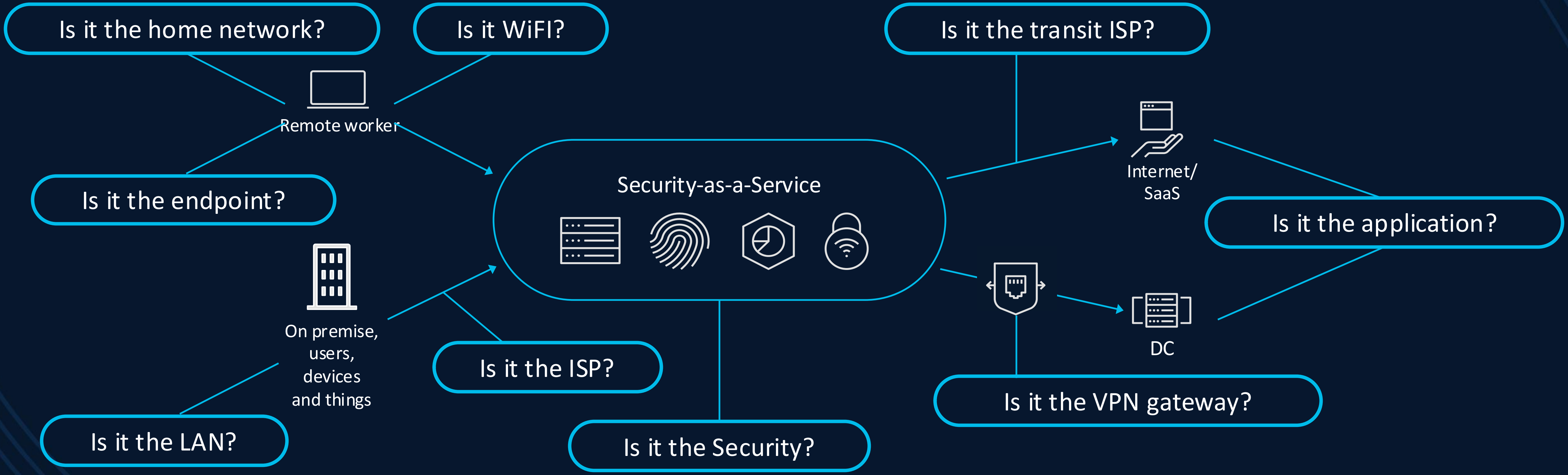
Cover all private apps over any port or protocol

ZTNA Delivers, But Can’t Cover All Scenarios

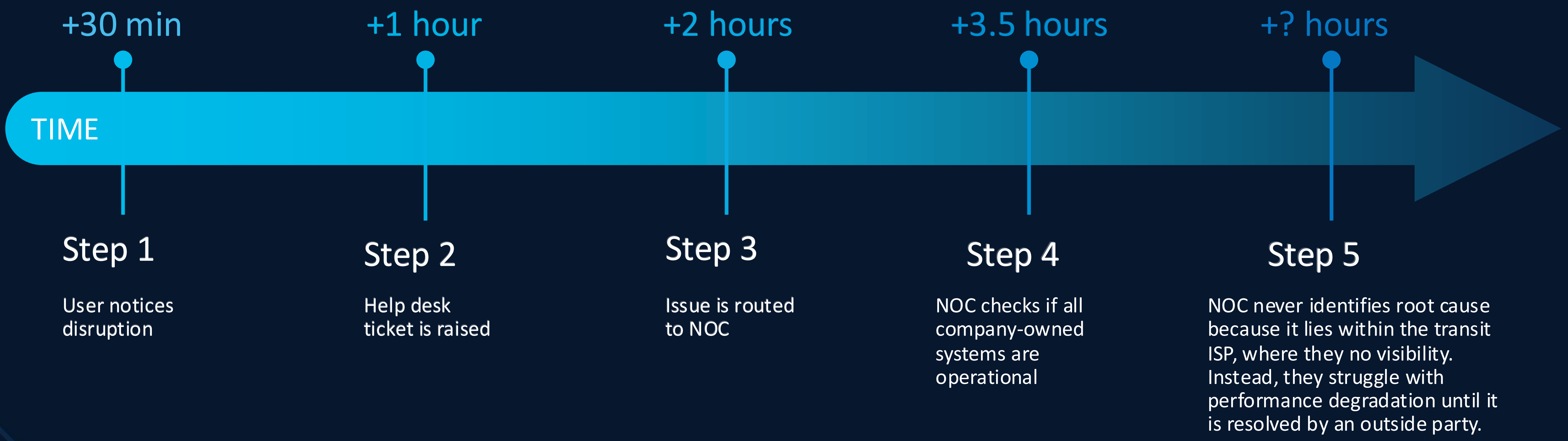


Some apps don’t work with ZTNA

Troubleshooting the hybrid work experience



Lack of end-to-end visibility increases mean time to resolution



+30 min

Step 1

User notices disruption

+1 hour

Step 2

Help desk ticket is raised

+2 hours

Step 3

Issue is routed to NOC

+3.5 hours

Step 4

NOC checks if all company-owned systems are operational

+? hours

Step 5

NOC never identifies root cause because it lies within the transit ISP, where they no visibility. Instead, they struggle with performance degradation until it is resolved by an outside party.

Introducing Cisco Secure Access

ZTNA for the ultimate in secure private access

Least privileged access

Efficient and secure access to all private apps

- ✓ Groundbreaking security
- ✓ Incredibly easy to use
- ✓ Synergistic with VPNaaS

- Per user/app access control protects resources
- Frictionless user experience boosts productivity
- Continuous posture checks for user compliance
- Obfuscate resources to prevent discovery
- Unified dashboard enables operational simplicity
- Optimized throughput for superior performance

Cisco Secure Access ZTNA plus VPNaaS in one common experience

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 (ZTNA)**
- Firewall as a Service (FWaaS) and IPS

+

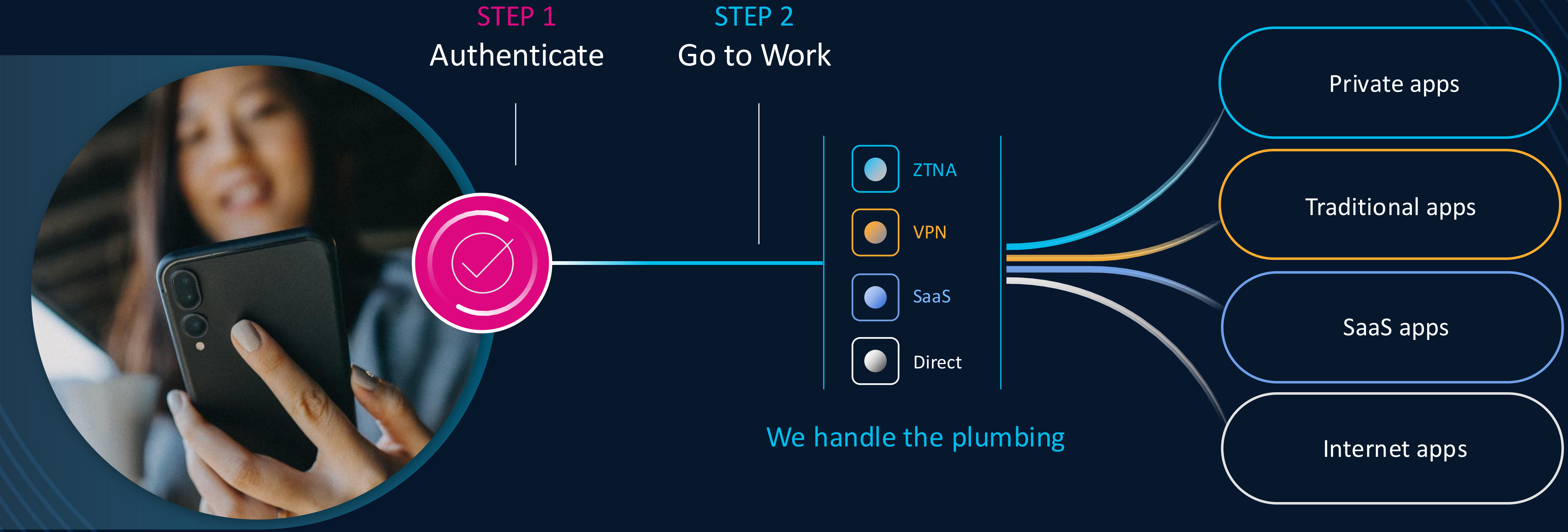
Cisco delivers the core and more in a single subscription…

- 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

Seamless user to app Zero Trust

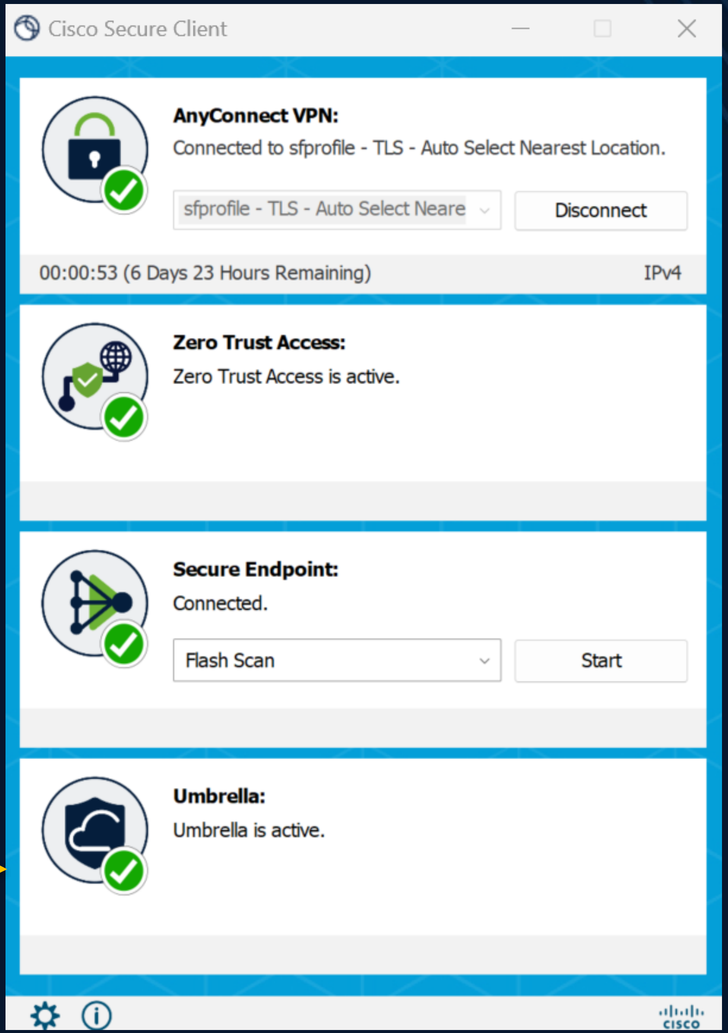


We handle the plumbing

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)



Cisco Secure Client

AnyConnect VPN:
Connected to sfprofile - TLS - Auto Select Nearest Location.

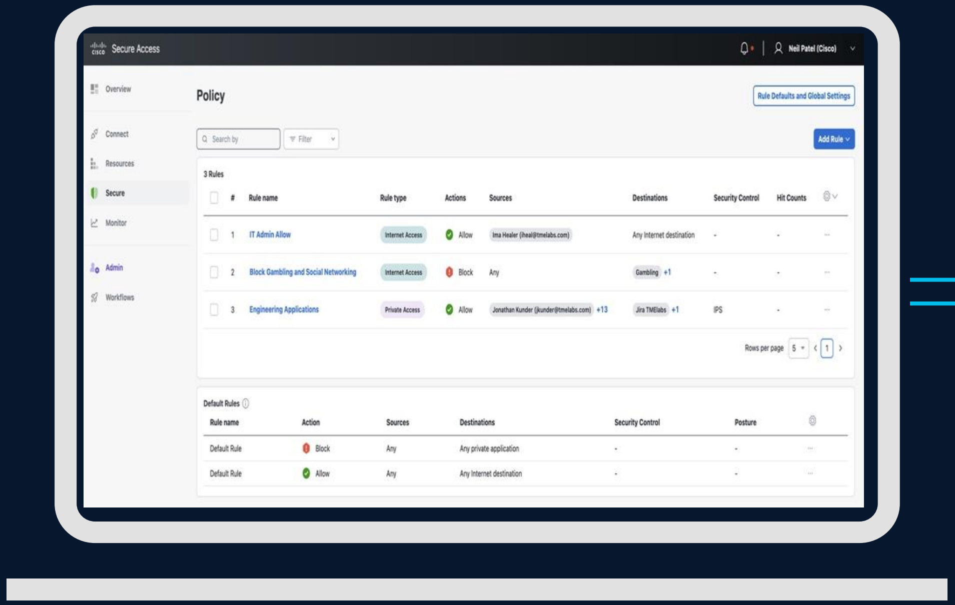
00:00:53 (6 Days 23 Hours Remaining) IPv4

Zero Trust Access:
Zero Trust Access is active.

Secure Endpoint:
Connected.

Umbrella:
Umbrella is active.

Cisco Secure Access: Easier for IT



3 Rules

	#	Rule name	Rule type	Actions	Sources	Destinations	Security Control	Hit Counts
□	1	IT Admin Allow	Internet Access	✓ Allow	Ima Healer (iheal@tmelabs.com)	Any Internet destination	-	-
□	2	Block Gambling and Social Networking	Internet Access	! Block	Any	Gambling +1	-	-
□	3	Engineering Applications	Private Access	✓ Allow	Jonathan Kunder (jkunder@tmelabs.com) +13	Jira TMElabs +1	IPS	-

Default Rules

Rule name	Action	Sources	Destinations	Security Control	Posture
Default Rule	! Block	Any	Any private application	-	-
Default Rule	✓ Allow	Any	Any Internet destination	-	-

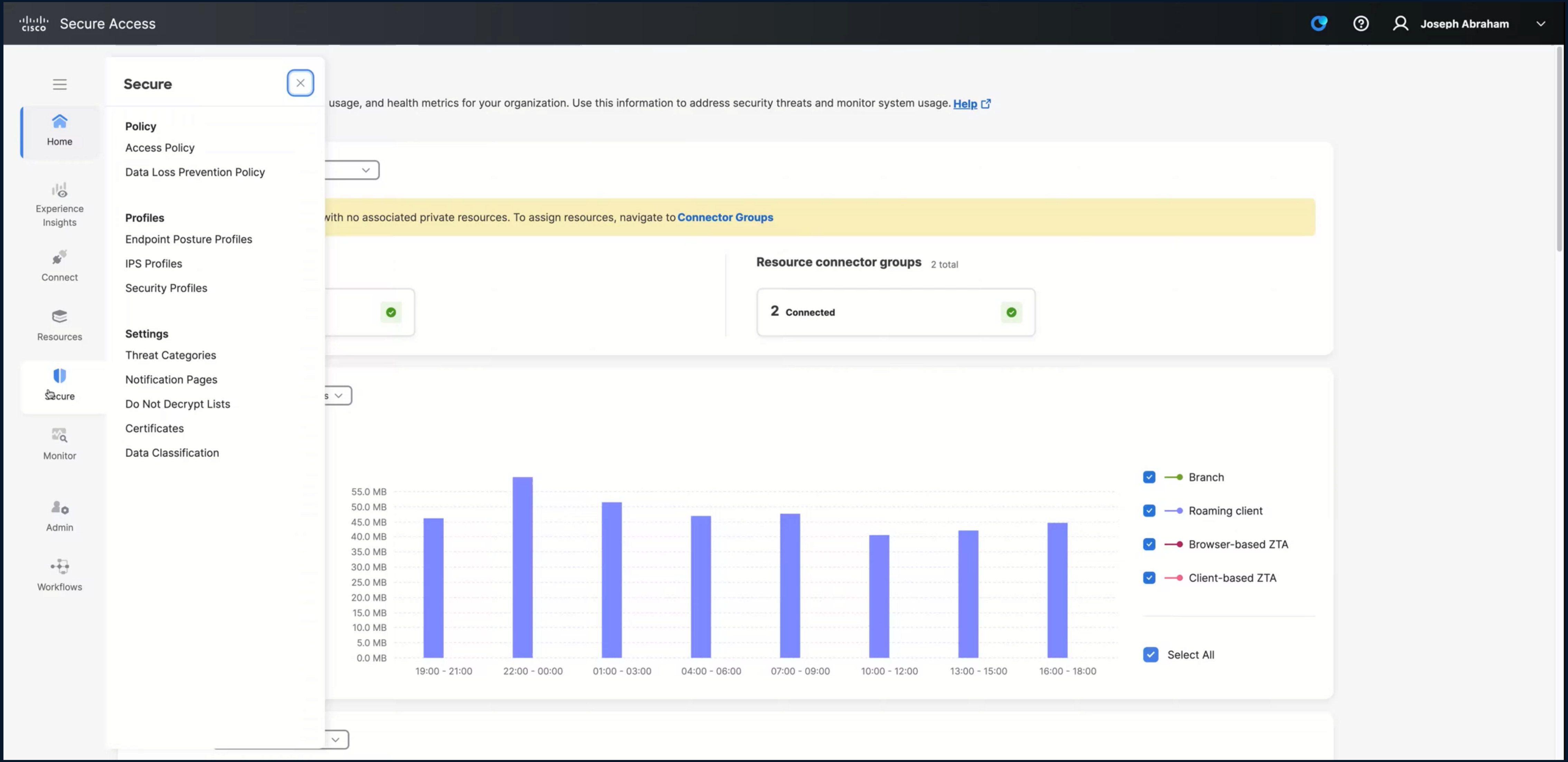
Higher efficiency

- *Single* agent, console and policy engine, identity and posture
- Digital Experience Monitoring (DEM)
- Single SLA

Lower costs

- Consolidated licensing
- Less hardware
- Ecosystem

One place to see traffic, set policies, and analyze risk.



usage, and health metrics for your organization. Use this information to address security threats and monitor system usage. Help

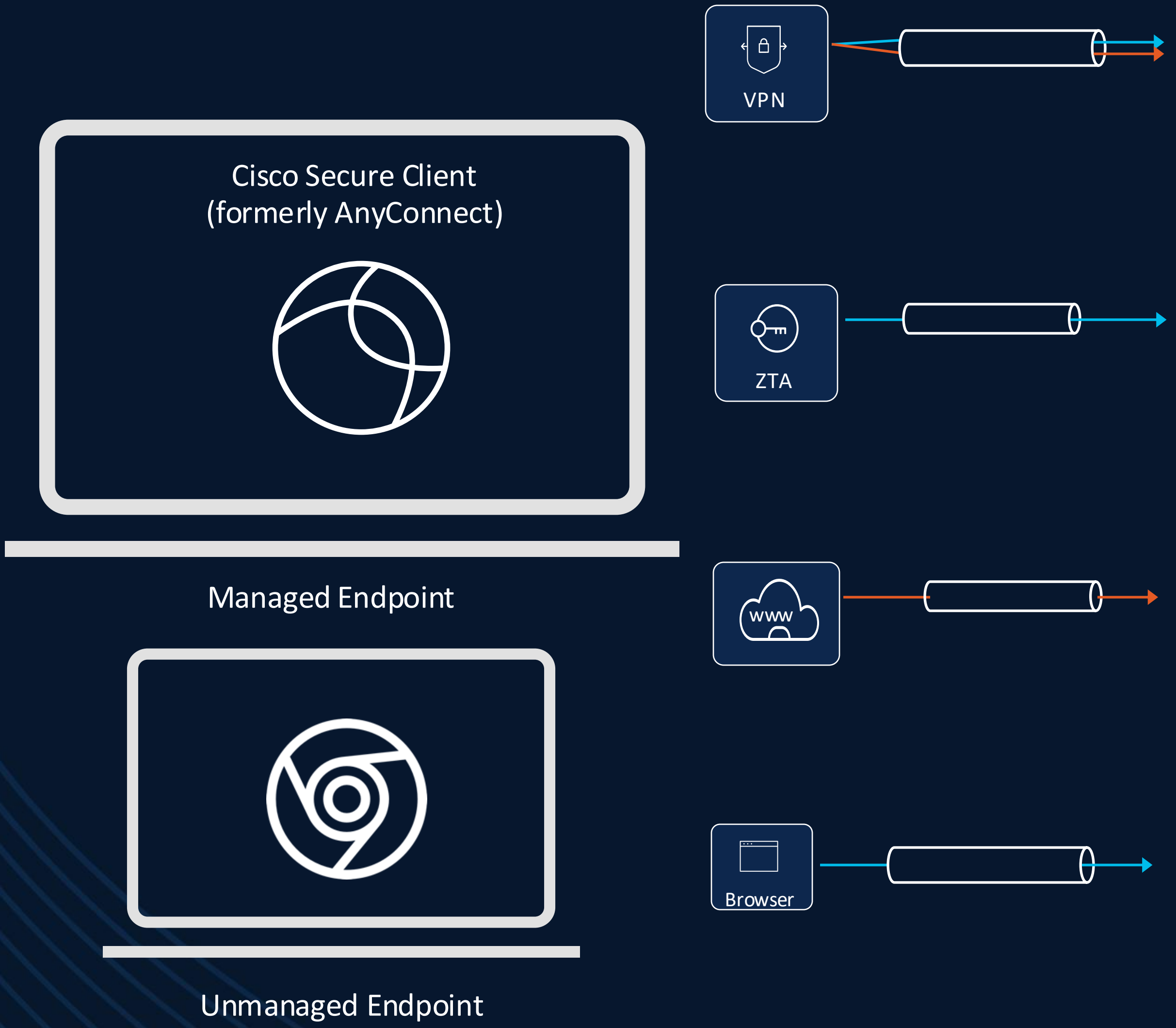
with no associated private resources. To assign resources, navigate to Connector Groups

Resource connector groups 2 total

2 Connected ✓

User based Traffic Acquisition Methods

⟷ Internet Traffic
⟷ Private Traffic
▭ Secure Tunnel



VPNaaS

- Authentication & Posture @ Connect time
- DTLS Tunnel
- Carry Internet & Private Traffic (All ports & protocols)
- SAML, (+) Cert, & (+) Multi-Cert Authentication

ZTA Module

- Authentication & Posture per session
- QUIC tunnel (MASQUE proxy)
- Carry **Private Traffic** (All ports & protocols)
- SAML Auth + Auto re-new

Web Roaming Module

- Device Enrollment (profile)
- Carry Internet Web Traffic (80/443)

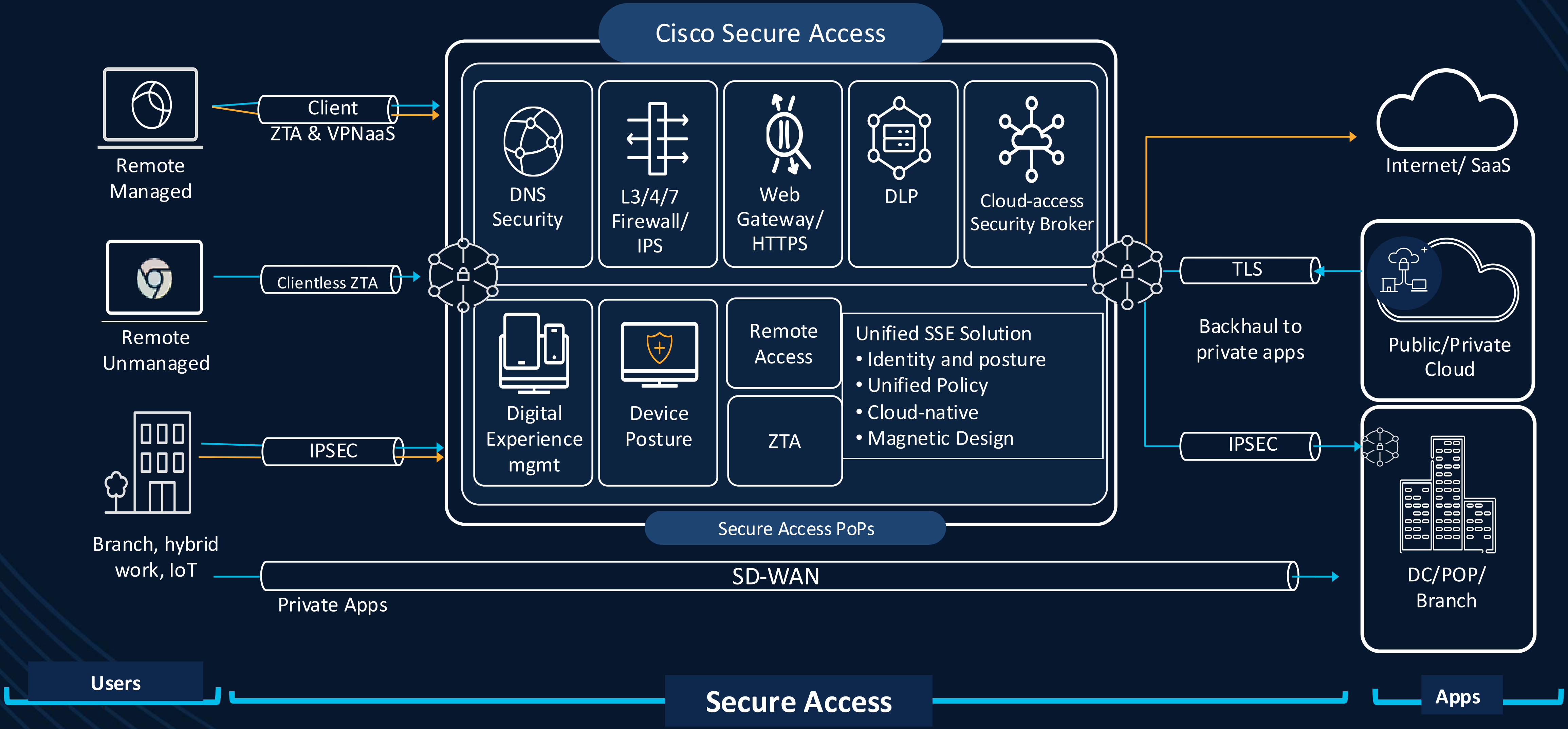
Clientless ZTA

- Accessible from any browser that supports SAML/Cookies
- Request based posture (browser version, OS)
- Web Apps Only

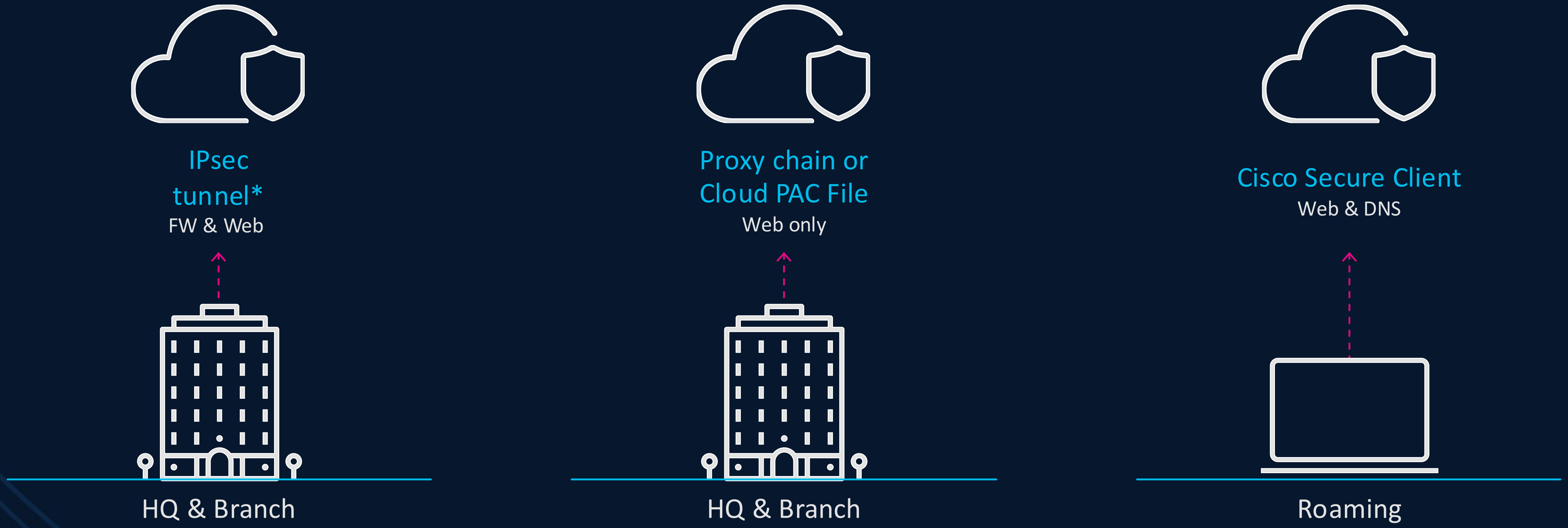
Secure Internet Access

Cisco Secure Access

Capabilities view



Flexible SIG connection methods



IPsec tunnel*
FW & Web

HQ & Branch

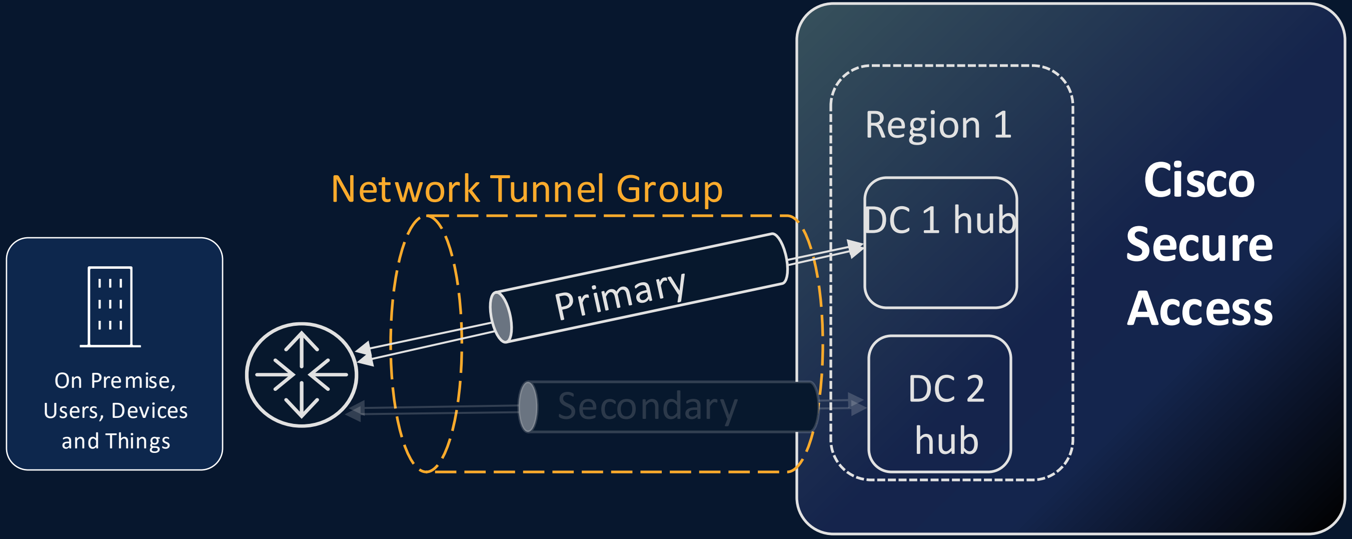
Proxy chain or Cloud PAC File
Web only

HQ & Branch

Cisco Secure Client
Web & DNS

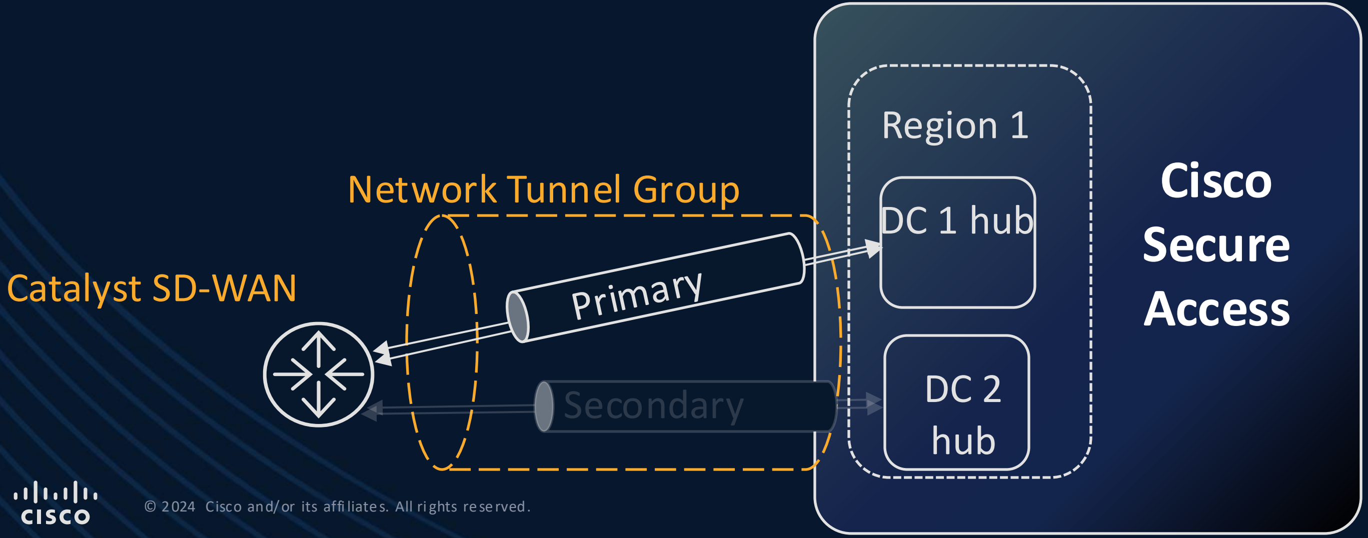
Roaming

Branch



Site-to-site Tunnels with IPsec

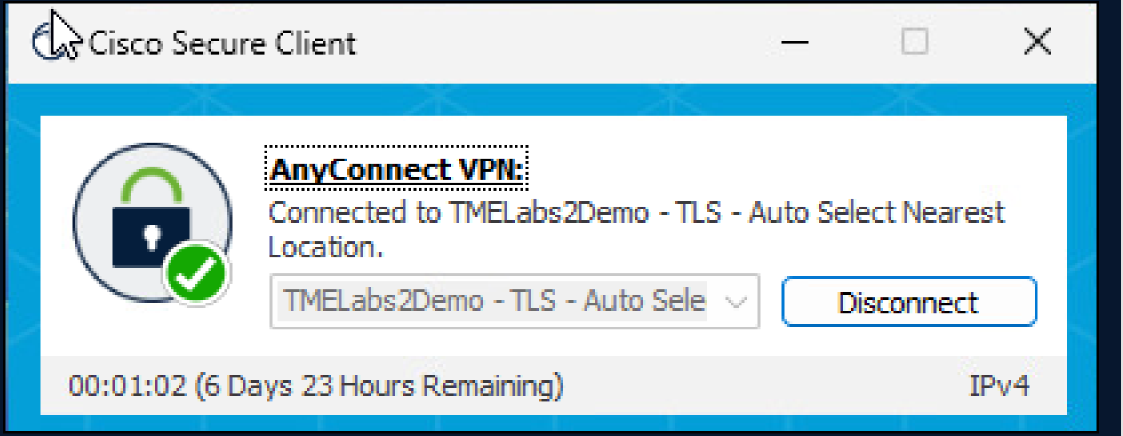
- Standards-based IPsec connection
- Single tunnel for Internet and private application access
- Static or BGP routing support
- Auto failover for redundancy + ECMP for scale
- Regional redundancy
- Outbound NAT support for internet only tunnels



Catalyst SD-WAN

- Auto tunnel creation from Catalyst SD-WAN manager (version 20.13/17.13)
- 1GB per tunnel
- Up to 8 active, 8 backup per tunnel group
- Tunnels for Internet access only
- Outbound NAT
- SD-WAN tracker support for regional redundancy

Remote Access VPN



AnyConnect VPN:

Connected to TMELabs2Demo - TLS - Auto Select Nearest Location.

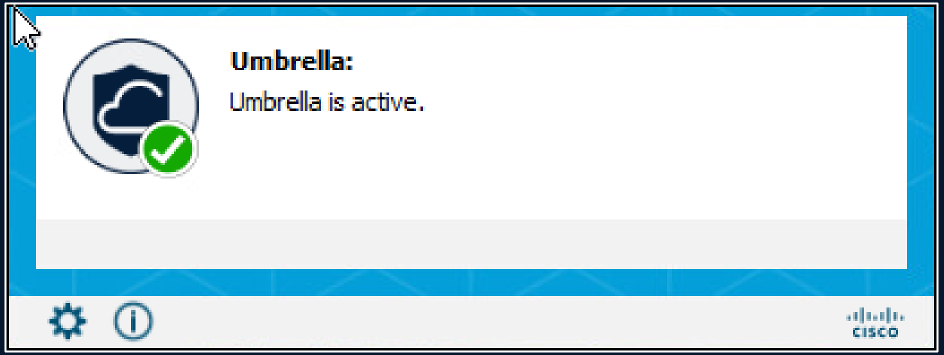
TMELabs2Demo - TLS - Auto Sele

00:01:02 (6 Days 23 Hours Remaining) IPv4

Cisco Secure Client 5.1 (formerly AnyConnect)

- Full or split-tunnel options are available
- Same deployment as the private access use-case
- Web traffic is evaluated by Cloud Firewall and Secure Web Gateway
  - Snort IDP/IPS
  - Layer 3-7 firewall rules
  - Data Loss Prevention
  - Anti-malware
  - Tenant controls
  - CASB
- Non-web traffic is evaluated by Cloud Firewall
  - Snort IDP/IPS
  - Layer 3-7 firewall rules

Roaming Security Module



Umbrella:

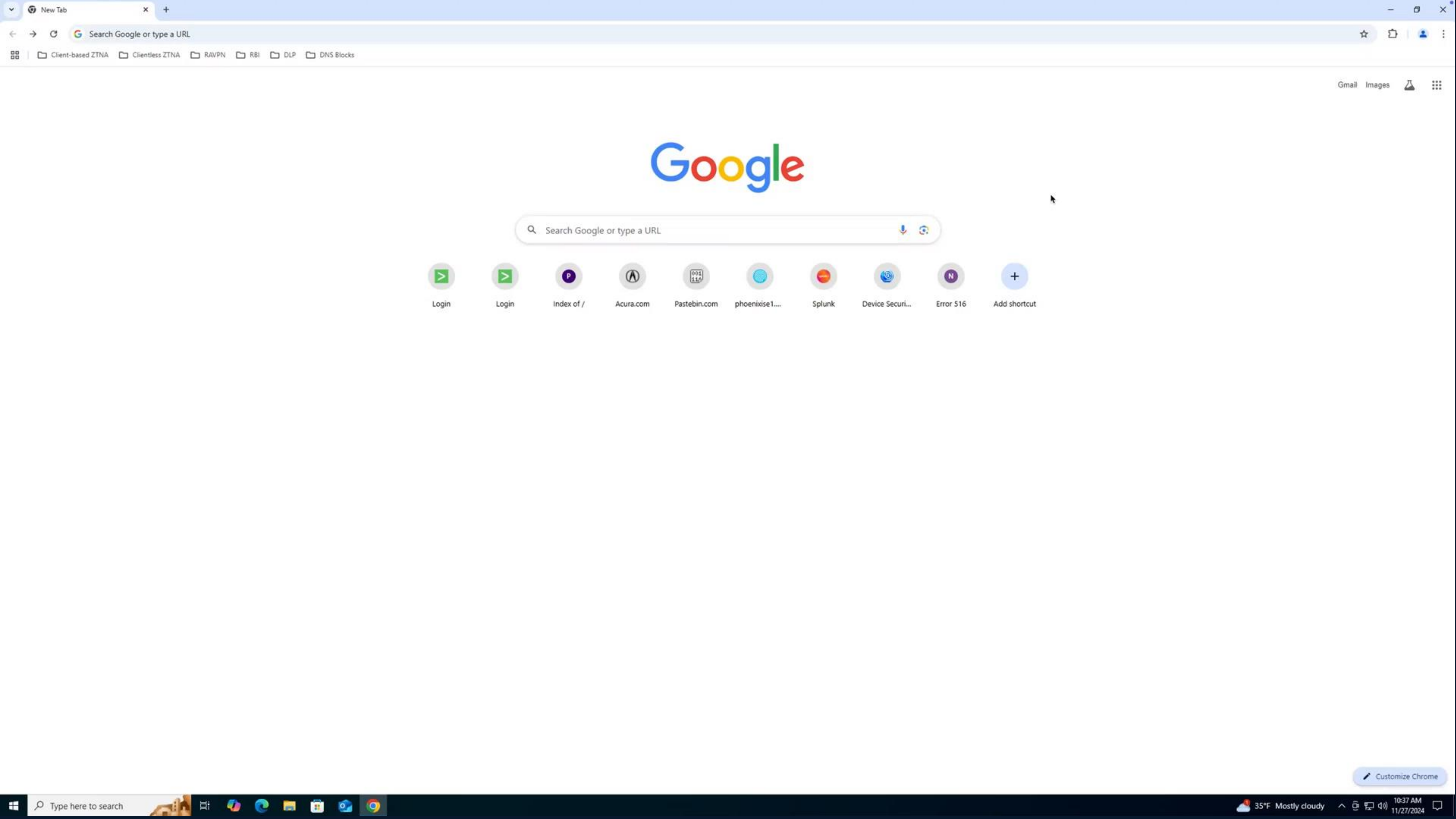
Umbrella is active.

Cisco Secure Client 5.1 (formerly AnyConnect)

- Redirects DNS and HTTP(s)
  - DNS is sent over DNSCrypt
  - HTTP/s is converted to explicit proxy requests
  - HTTP only redirected on TCP 80/443
- Exceptions for destinations added in dashboard
  - Local domain suffix is excluded
  - Same exemptions apply to PAC file deployment
  - Download and deploy OrgInfo file from dashboard
- Dual stack is supported but not native IPv6
- Authentication occurs using UPN of the logged-in user

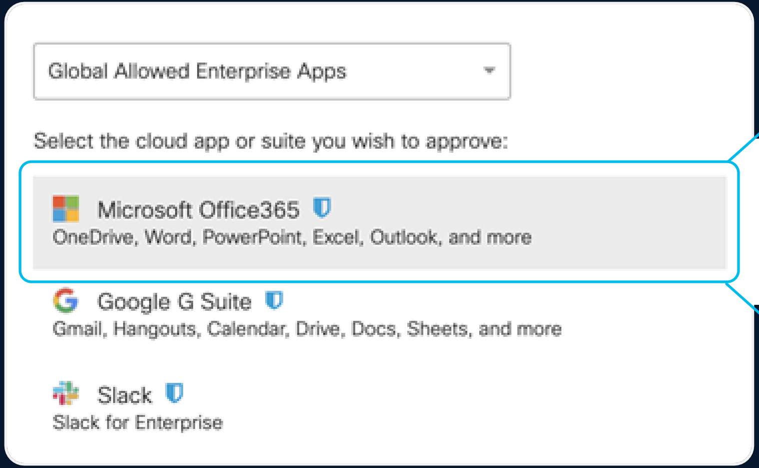
https://docs.sse.cisco.com/sse-user-guide/docs/roaming-security-module-requirements

https://docs.sse.cisco.com/sse-user-guide/docs/download-the-orginfo-json


New Tab
Search Google or type a URL
Client-based ZTNA
Clientless ZTNA
RAVPN
RBI
DLP
DNS Blocks
Gmail
Images
Google
Search Google or type a URL
Login
Login
Index of /
Acura.com
Pastebin.com
phoenixise1....
Splunk
Device Securi...
Error 516
Add shortcut
Customize Chrome
Type here to search
35°F Mostly cloudy
10:37 AM
11/27/2024

Tenant Controls

Select the instance(s) of core SaaS applications that can be accessed by all users or by specific groups/individuals



Global Allowed Enterprise Apps

Select the cloud app or suite you wish to approve:

- Microsoft Office365
  OneDrive, Word, PowerPoint, Excel, Outlook, and more
- Google G Suite
  Gmail, Hangouts, Calendar, Drive, Docs, Sheets, and more
- Slack
  Slack for Enterprise

✓ Cisco.com
Corporate instance

✗ Deb Smith
Personal instance

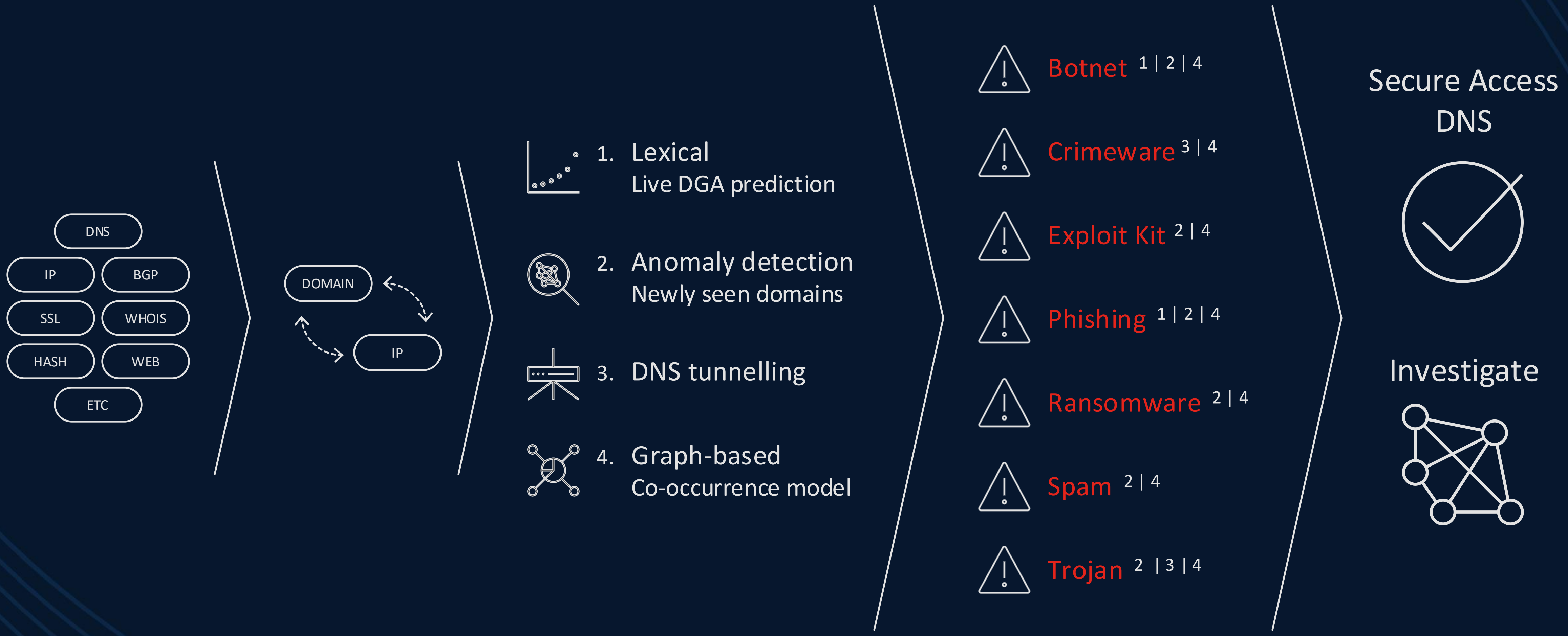
✗ Bob Jones
Personal instance

Key use cases

Security
Ensure, sensitive data is created and stored in approved instances of cloud apps

Productivity
Only provide access to corporate instances of core SaaS apps

Multi-faceted threat intel



DNS

IP

BGP

SSL

WHOIS

HASH

WEB

ETC

DOMAIN

IP

1. Lexical
   Live DGA prediction
2. Anomaly detection
   Newly seen domains
3. DNS tunnelling
4. Graph-based
   Co-occurrence model

Botnet 1 | 2 | 4

Crimeware 3 | 4

Exploit Kit 2 | 4

Phishing 1 | 2 | 4

Ransomware 2 | 4

Spam 2 | 4

Trojan 2 | 3 | 4

Secure Access DNS

Investigate

Secure Access: protecting the usage of AI

Protect intellectual property as it flows in and out of AI systems

Threat Visibility

Discover and Assess Activities

Leakage Prevention

DLP Inspection of Prompts/Uploads

Threat Prevention

Block Apps and Control Downloads

Discovers and controls over **70** Gen AI apps (including APIs)

Cisco Talos Threat Intelligence

Unmatched visibility across the threat landscape powered by experts, data, and Gen AI

715B security events/**day**

~9M emails blocked/**hour**

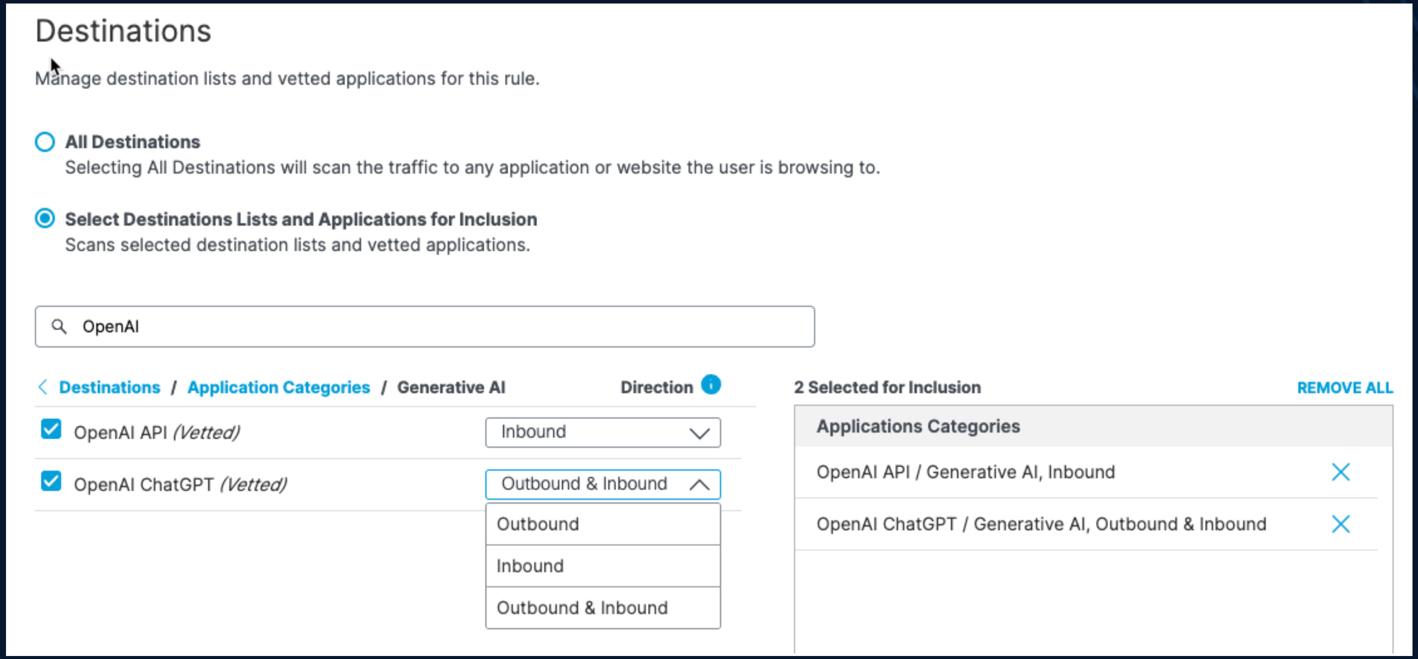
~2,000 new samples/**minute**

~2,000 domains blocked/**second**

Multimode DLP: Inbound and Outbound for ChatGPT

Empowers our customers to monitor and, if necessary, block content generated by ChatGPT

- Scan ChatGPT responses (i.e., inbound traffic) for any type of generated content.
- Stop users from using AI-generated source code to prevent the usage of copyrighted or unsafe code



Destinations

Manage destination lists and vetted applications for this rule.

○ **All Destinations**
Selecting All Destinations will scan the traffic to any application or website the user is browsing to.

● **Select Destinations Lists and Applications for Inclusion**
Scans selected destination lists and vetted applications.

OpenAI

Destinations / **Application Categories** / **Generative AI** — **Direction**

		Direction
☑	OpenAI API *(Vetted)*	Inbound
☑	OpenAI ChatGPT *(Vetted)*	Outbound & Inbound

2 Selected for Inclusion — REMOVE ALL

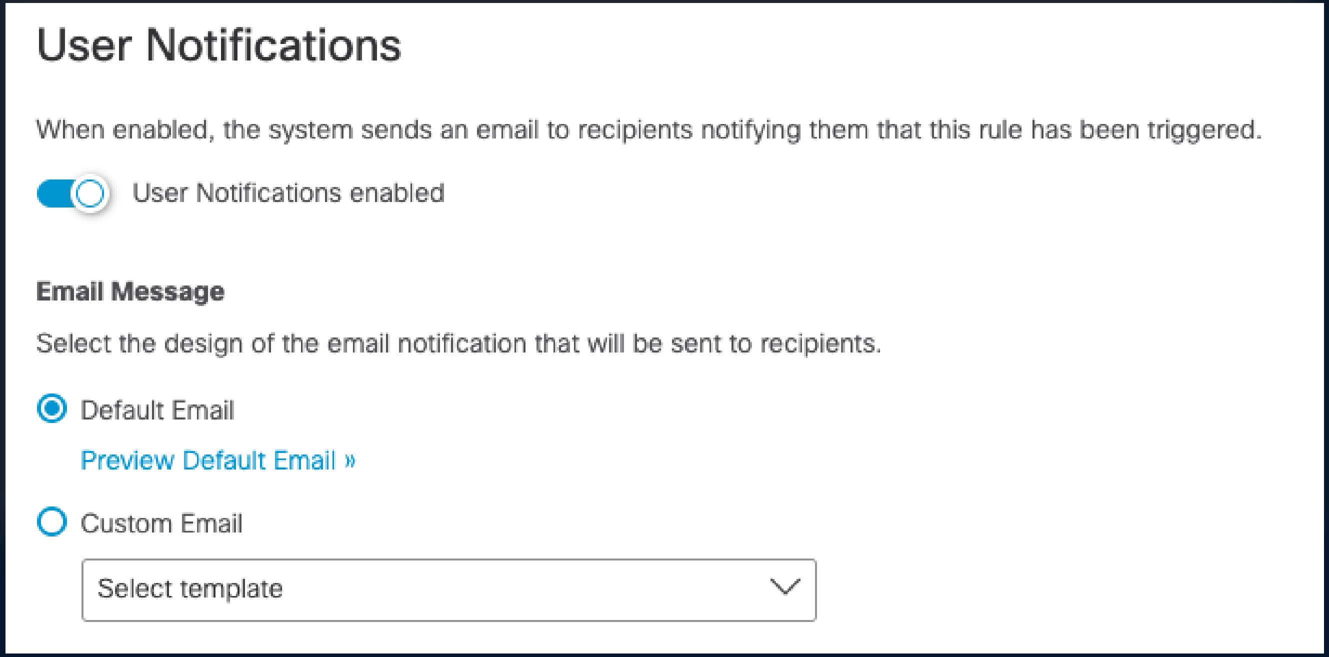
Applications Categories

- OpenAI API / Generative AI, Inbound ✕
- OpenAI ChatGPT / Generative AI, Outbound & Inbound ✕

Multimode DLP: Email End User Notification

End-users are promptly notified when they send out sensitive data or when their cloud-hosted files violate the organization's data security policy

- Available for both Real Time and SaaS API rules
- Default and custom email template, including 'variables' templates
- Aggregated email every 5 minutes



User Notifications

When enabled, the system sends an email to recipients notifying them that this rule has been triggered.

User Notifications enabled

Email Message

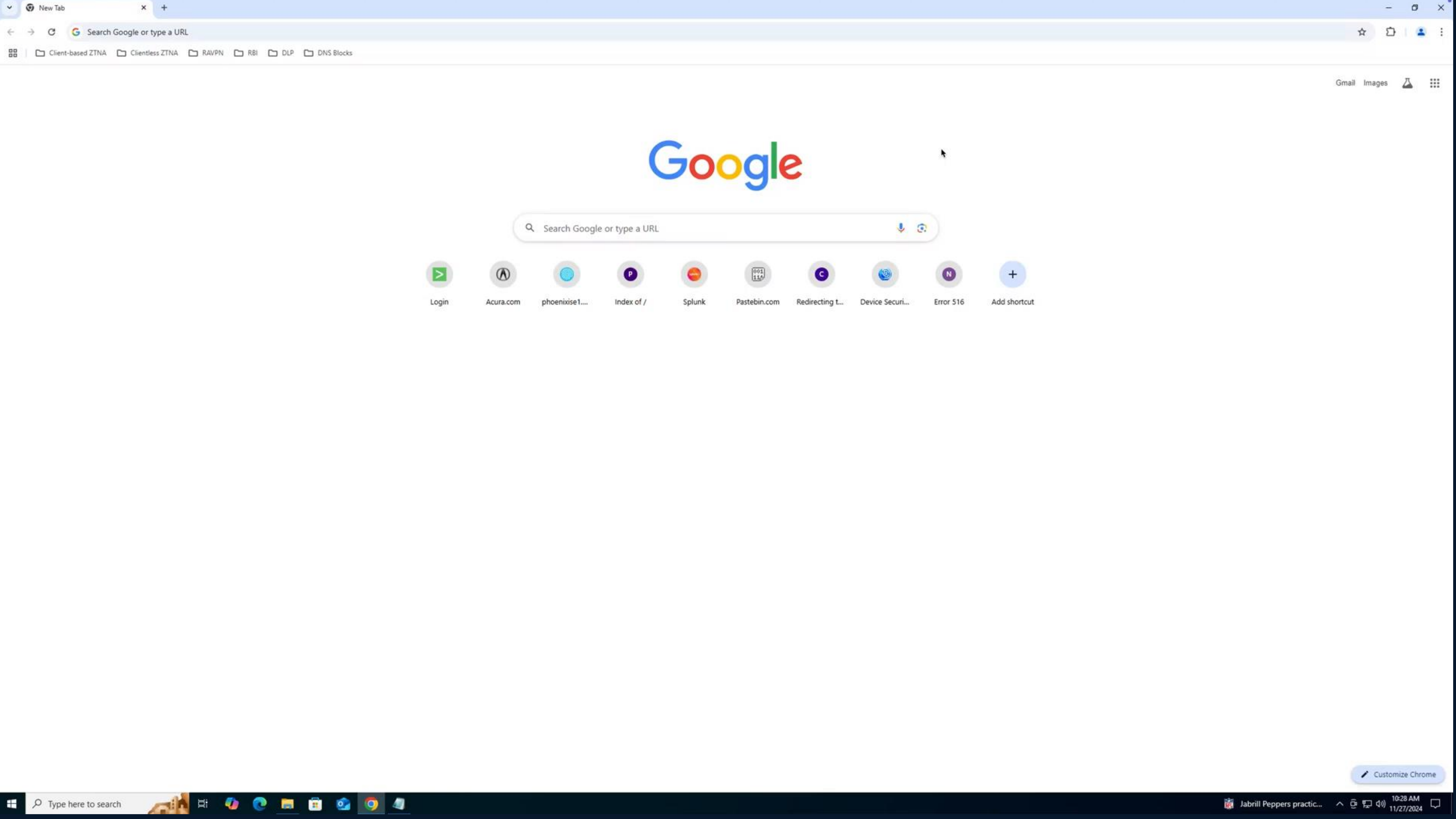
Select the design of the email notification that will be sent to recipients.

● Default Email

Preview Default Email »

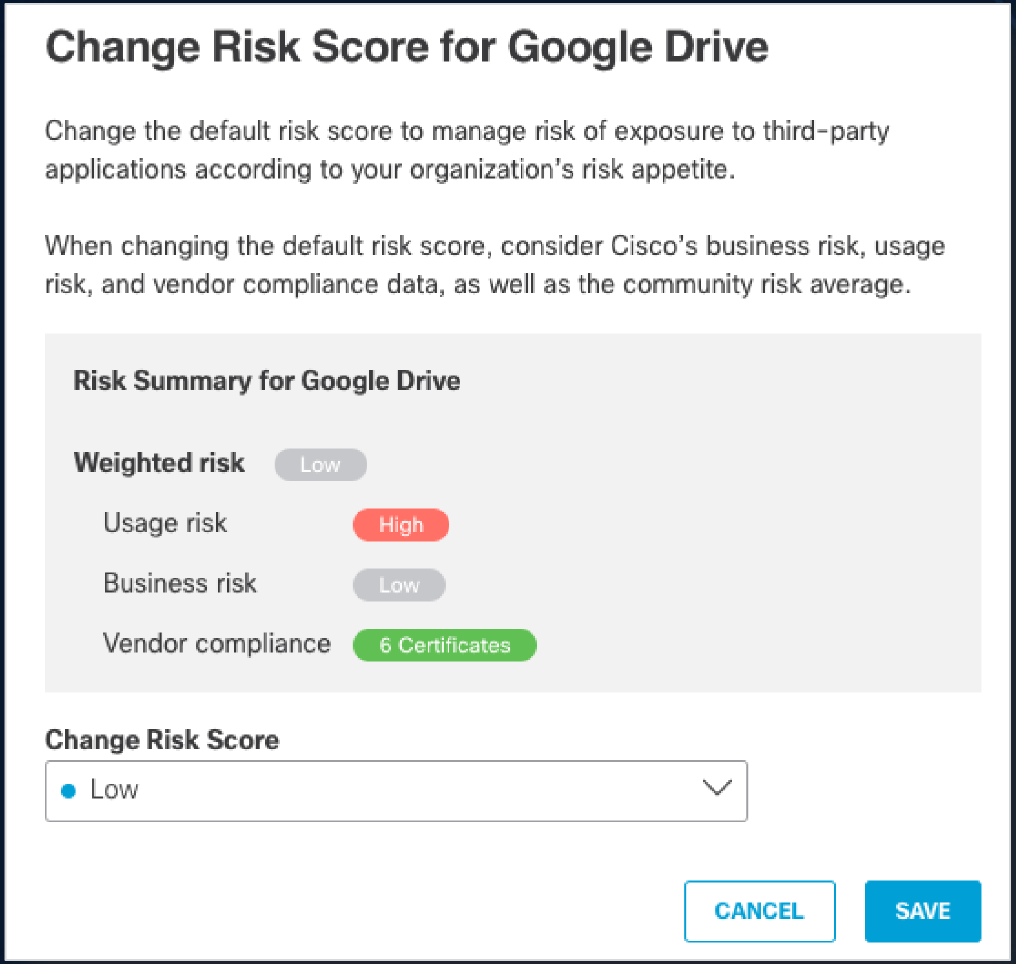
○ Custom Email

Select template


New Tab
Search Google or type a URL
Client-based ZTNA
Clientless ZTNA
RAVPN
RBI
DLP
DNS Blocks
Gmail
Images
Google
Search Google or type a URL
Login
Acura.com
phoenixise1....
Index of /
Splunk
Pastebin.com
Redirecting t...
Device Securi...
Error 516
Add shortcut
Customize Chrome
Type here to search
Jabrill Peppers practic...
10:28 AM
11/27/2024

CASB: Application Risk Override

- Enabling customers to modify an application's risk score seamlessly and instantly for their organization
- Reverting to Weighted Risk is always available
- Community Risk Score:
  This score is calculated as the median of all customized risk scores for each application among our customers



Change Risk Score for Google Drive

Change the default risk score to manage risk of exposure to third-party applications according to your organization's risk appetite.

When changing the default risk score, consider Cisco's business risk, usage risk, and vendor compliance data, as well as the community risk average.

Risk Summary for Google Drive

Weighted risk Low

Usage risk High

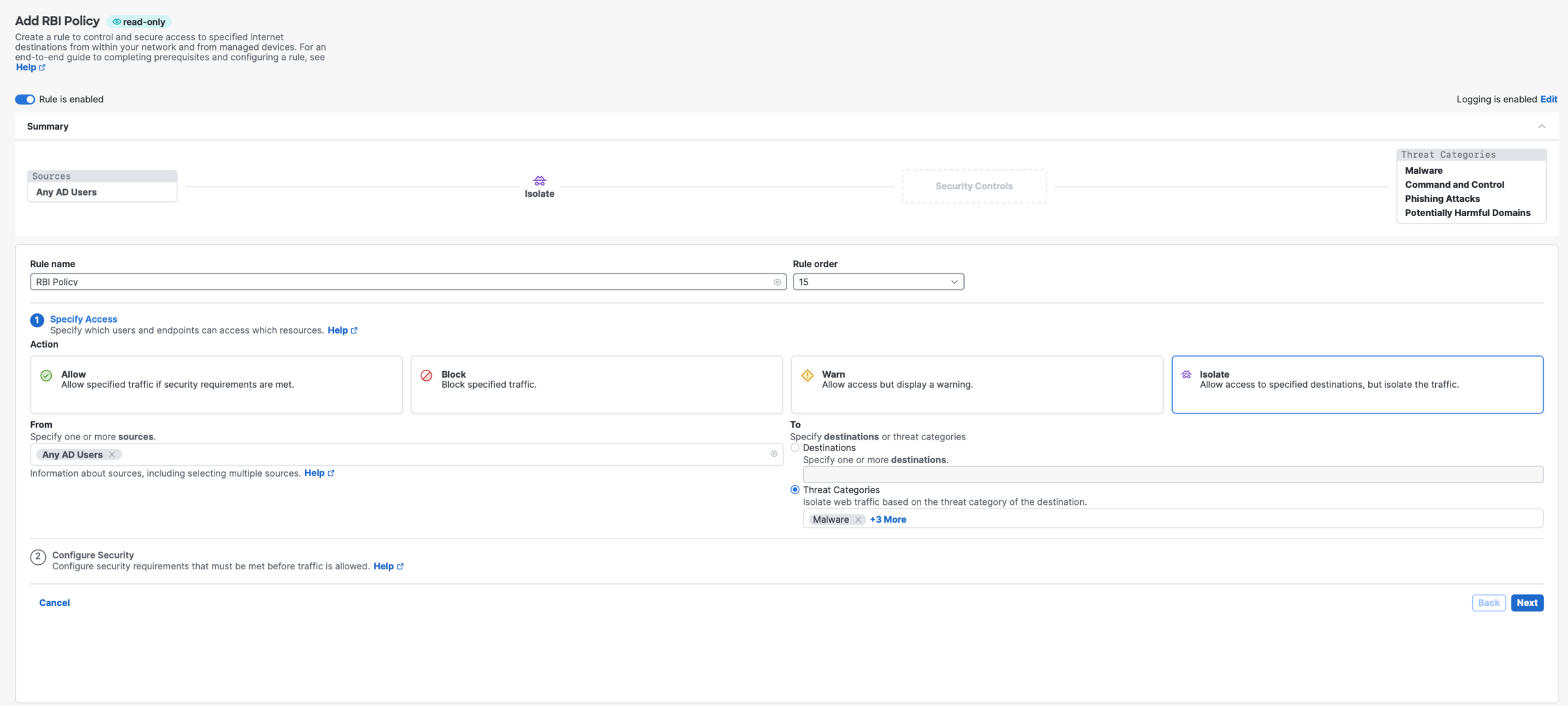
Business risk Low

Vendor compliance 6 Certificates

Change Risk Score

● Low

Our integrated RBI capability illustrates the single dashboard experience



Add RBI Policy read-only

Create a rule to control and secure access to specified internet destinations from within your network and from managed devices. For an end-to-end guide to completing prerequisites and configuring a rule, see **Help**

Rule is enabled

Logging is enabled **Edit**

Summary

Sources: Any AD Users → Isolate → Security Controls → Threat Categories: Malware, Command and Control, Phishing Attacks, Potentially Harmful Domains

Rule name: RBI Policy

Rule order: 15

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.
- **Warn** Allow access but display a warning.
- **Isolate** Allow access to specified destinations, but isolate the traffic.

From

Specify one or more **sources**.

Any AD Users

Information about sources, including selecting multiple sources. **Help**

To

Specify **destinations** or threat categories

○ Destinations

Specify one or more **destinations**.

● Threat Categories

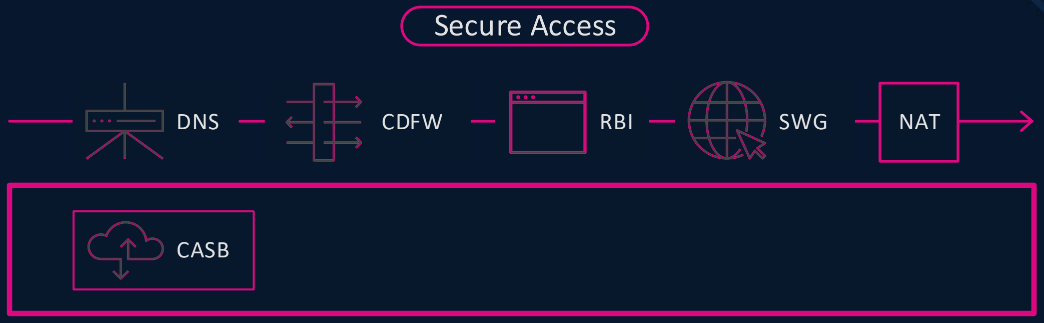
Isolate web traffic based on the threat category of the destination.

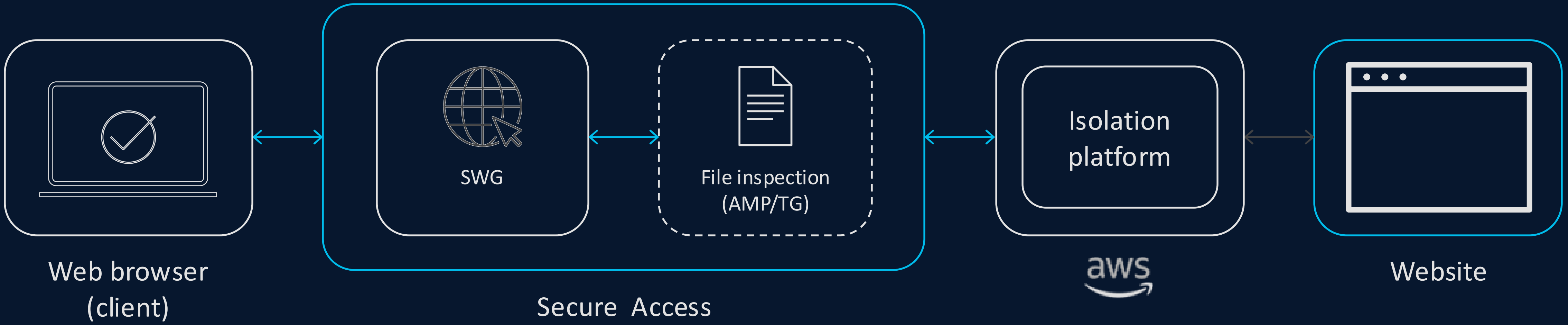
Malware +3 More

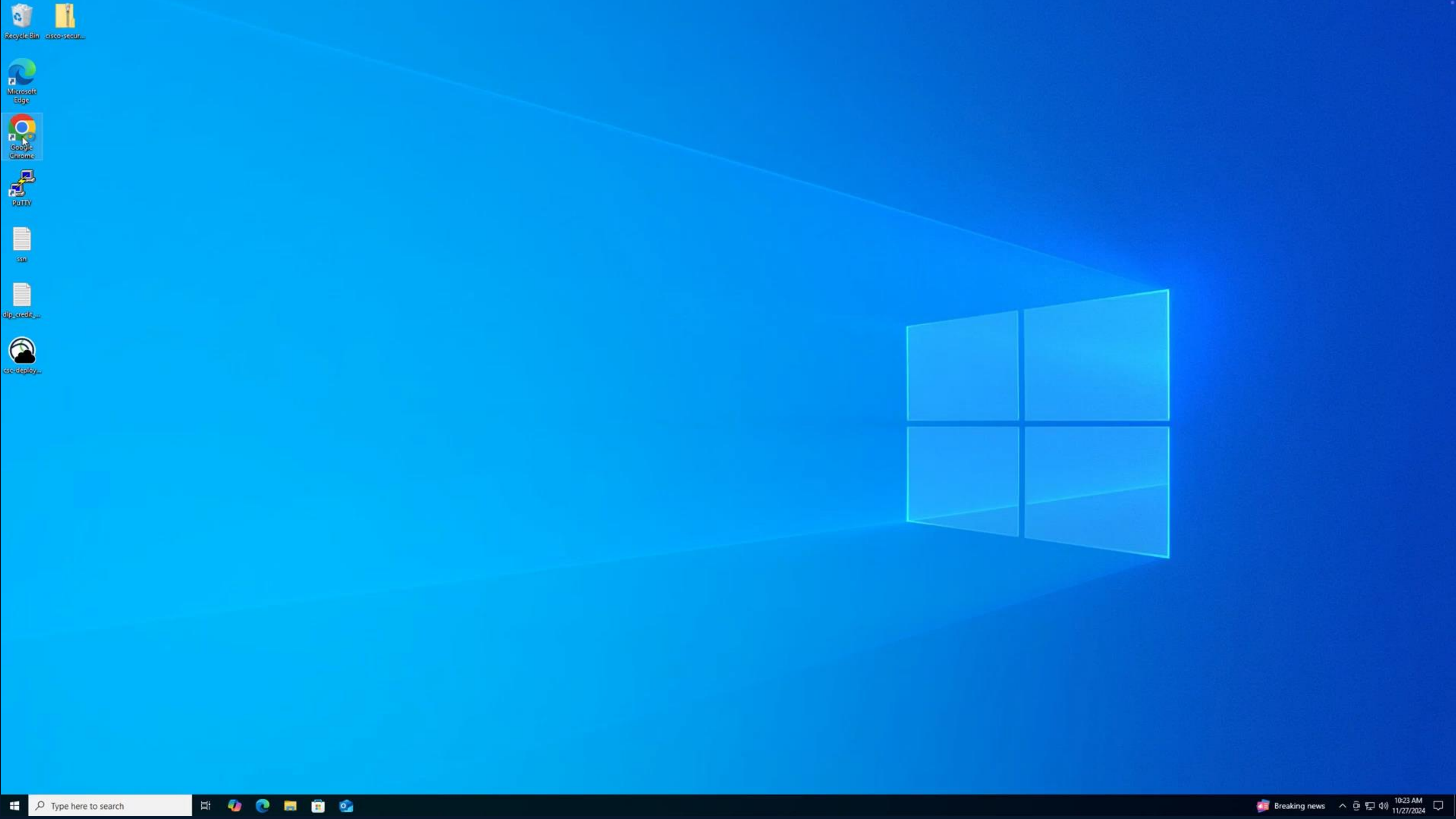
2 **Configure Security**

Configure security requirements that must be met before traffic is allowed. **Help**

RBI traffic flow overview

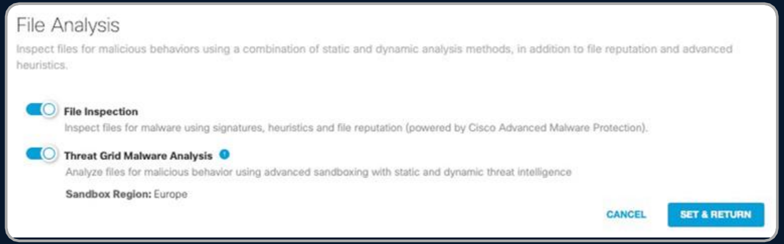





Recycle Bin
cisco-secur...
Microsoft Edge
Google Chrome
PuTTY
ssn
dlp_credit_...
csc-deploy...
Type here to search
Breaking news
10:23 AM
11/27/2024

Cisco Secure Malware Analytics (Threat Grid) sandboxing

- Ability to detect hidden threats in files that are being downloaded
- A set of new or higher risk files are placed in a sandbox environment and checked for malicious activity/content
  - Alerts posted on files that show bad activity
  - Secure Access threat intelligence is updated for that file



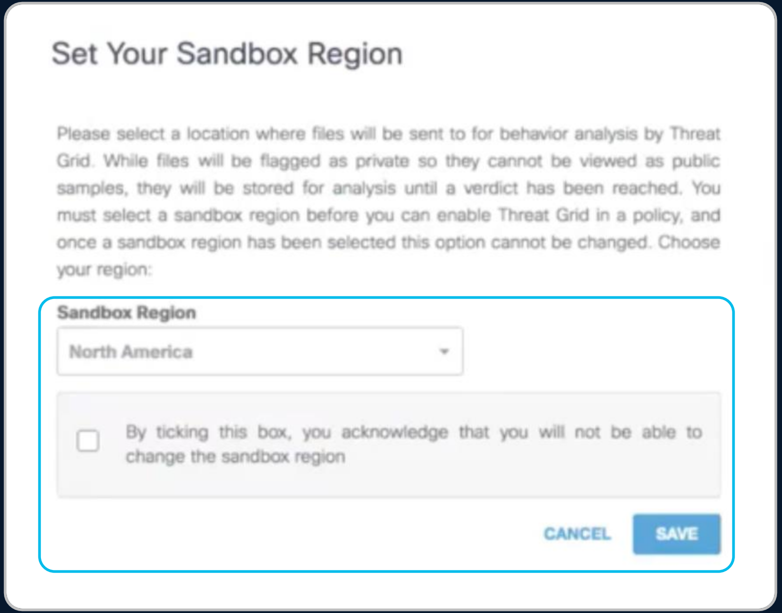
File Analysis

Inspect files for malicious behaviors using a combination of static and dynamic analysis methods, in addition to file reputation and advanced heuristics.

File Inspection
Inspect files for malware using signatures, heuristics and file reputation (powered by Cisco Advanced Malware Protection).

Threat Grid Malware Analysis
Analyze files for malicious behavior using advanced sandboxing with static and dynamic threat intelligence

Sandbox Region: Europe



Set Your Sandbox Region

Please select a location where files will be sent to for behavior analysis by Threat Grid. While files will be flagged as private so they cannot be viewed as public samples, they will be stored for analysis until a verdict has been reached. You must select a sandbox region before you can enable Threat Grid in a policy, and once a sandbox region has been selected this option cannot be changed. Choose your region:

Sandbox Region: North America

□ By ticking this box, you acknowledge that you will not be able to change the sandbox region

Regions:
Europe or North America

Private Application Access

Zero trust is required in today’s workplace

Addressing all kinds of:

Users

(and devices)

Places

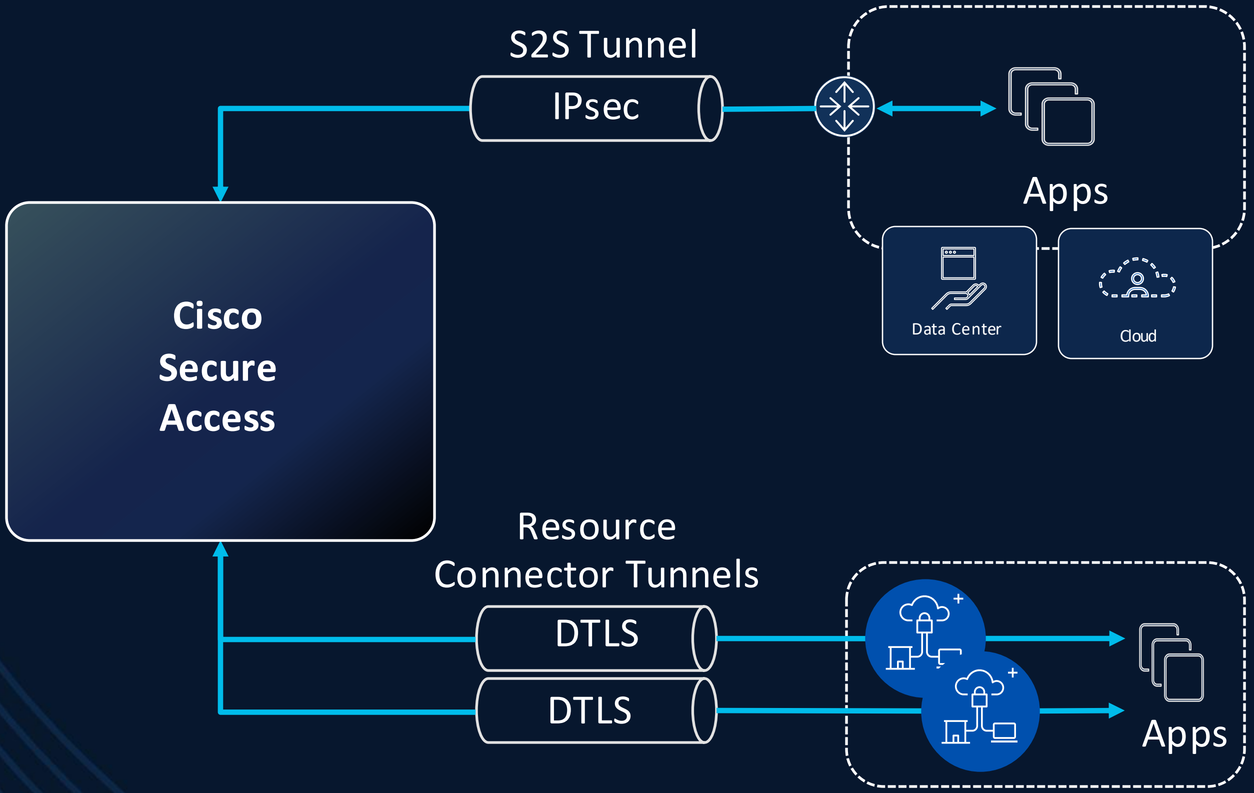
(and networks)

Apps

(and data)

… yet most zero trust projects are failing to deliver.

Apps: Private Applications



Site-to-site Tunnels with IPsec

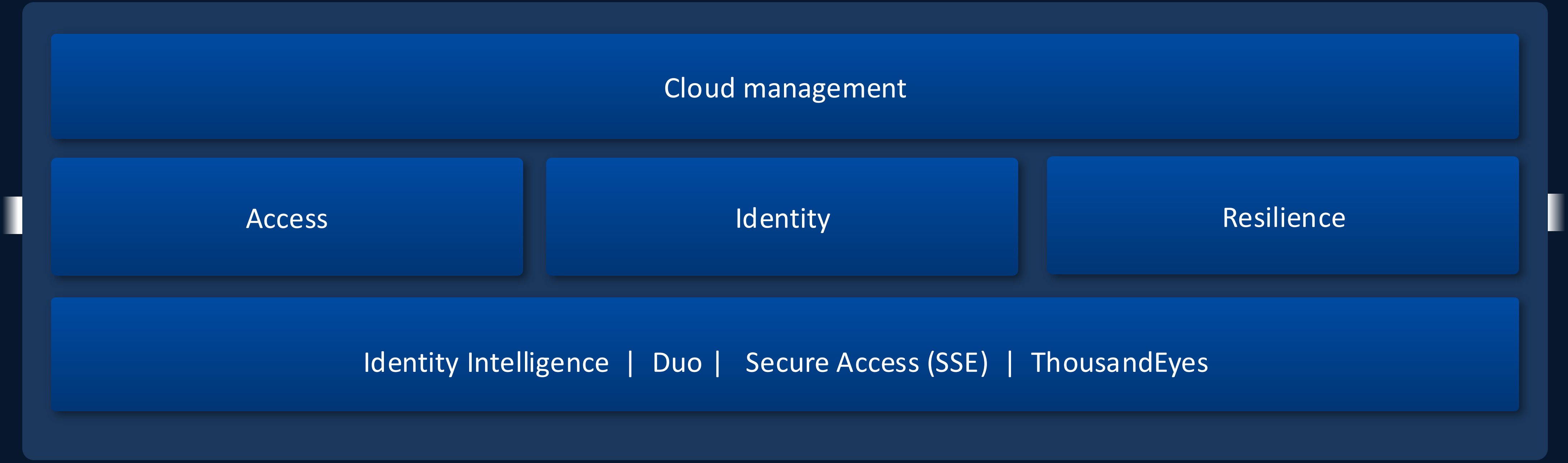
- Standards-based IPsec connection
- Single tunnel for Internet and private application access
- Static or BGP routing support
- Auto failover for redundancy + ECMP for scale
- Fallback for resource connectors

Resource Connectors

- Lightweight VM for AWS and ESXi
- All traffic egresses from Resource Connector IP
- Access applications with overlapping IPs
- Outbound connection / no firewall holes required
- No routing configuration required
- Auto failover / load balancing

Cisco Zero Trust Access

The first SSE with Identity Intelligence



Cloud management

Access

Identity

Resilience

Identity Intelligence | Duo | Secure Access (SSE) | ThousandEyes

Identity is foundation of zero trust, and is under attack

ATTACK TECHNIQUES

MFA Interception

Device Registration

MFA Flood

Web Session Hijacking

Identity is foundation of zero trust, and is under attack

ATTACK TECHNIQUES

MFA Interception

Device Registration

MFA Flood

Web Session Hijacking

STOPPED BY MODERN AUTHENTICATION

Passwordless

Biometric Login

Non-domain Employee

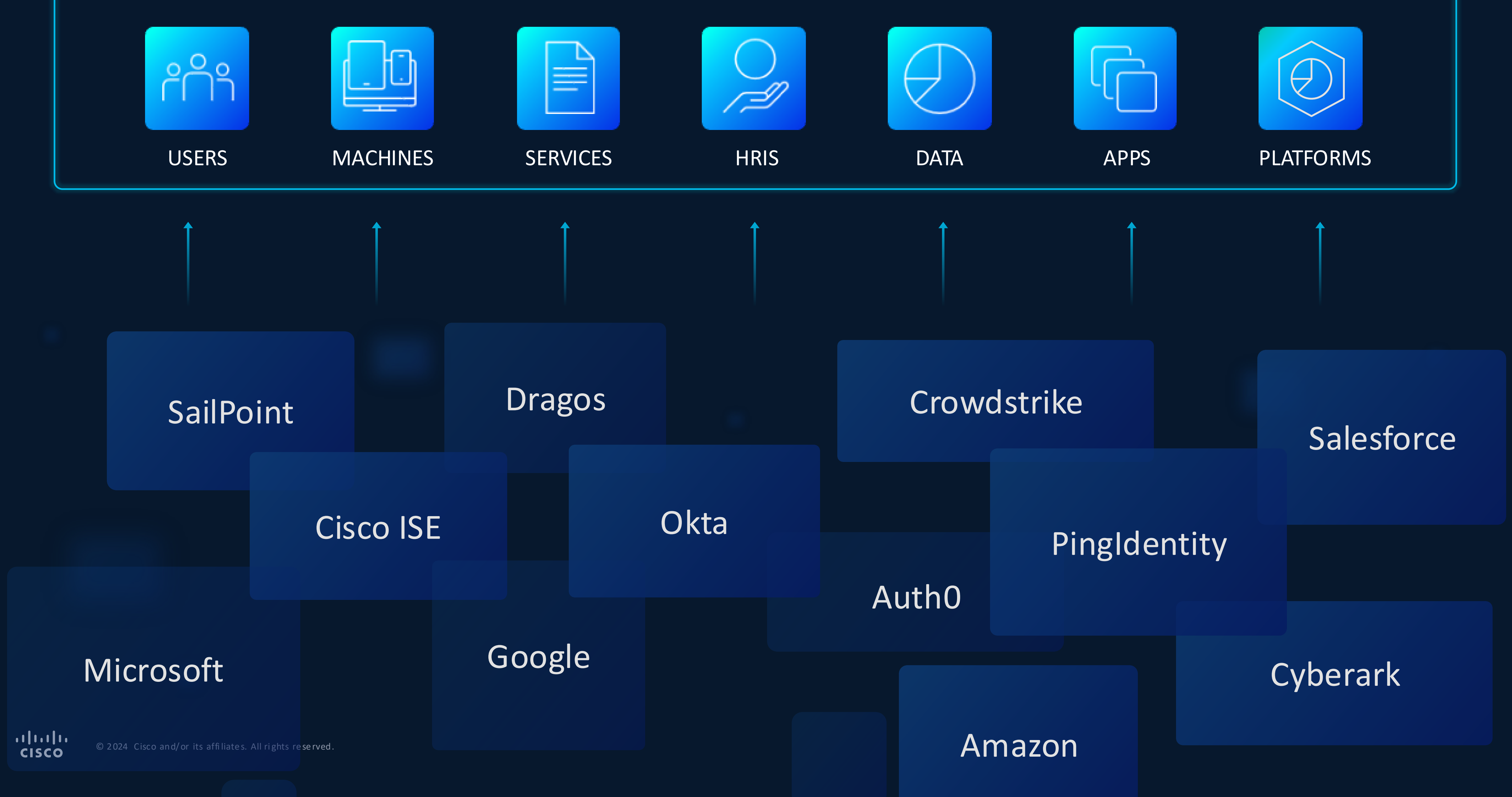
Legacy Apps

Crypto Secure

Extended Workforce

Device-based Trust

Cisco Identity Intelligence



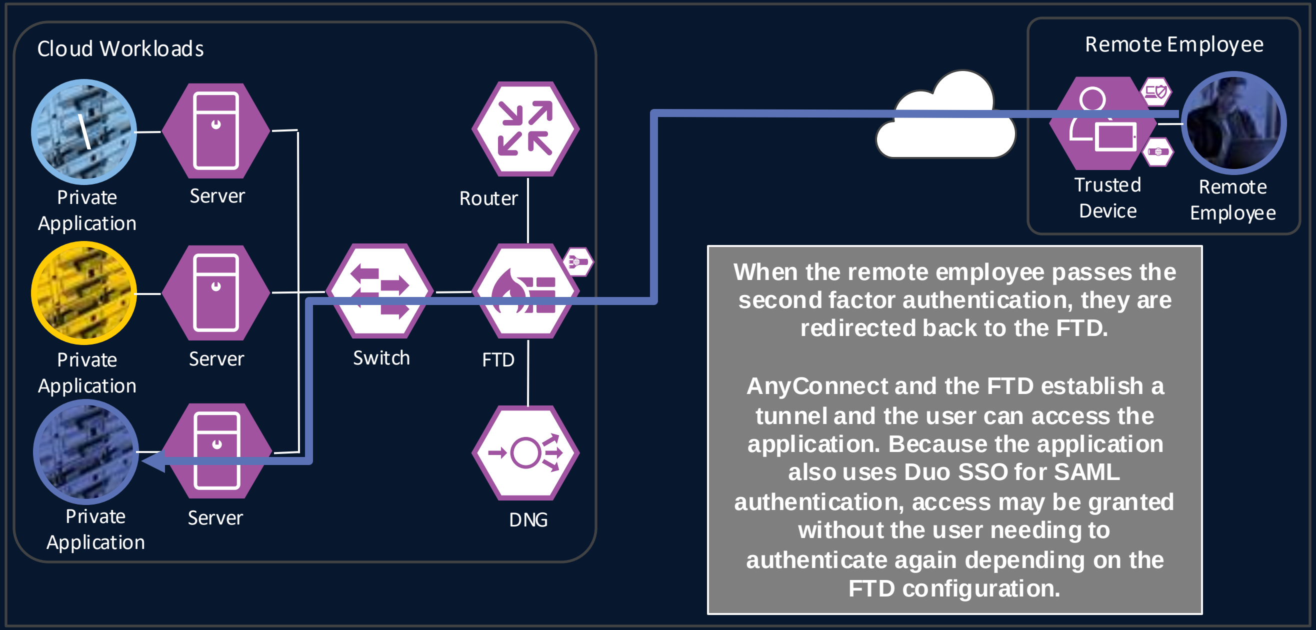
Cisco Identity Intelligence
USERS
MACHINES
SERVICES
HRIS
DATA
APPS
PLATFORMS
RELATIONSHIPS
LOCATION
EMAILS
UID
ROLE
FACTORS
LOGS
SESSIONS
SESSIONS
SESSIONS
CONNECTED
UNMANAGED
USER DEVICES
INFRASTRUCTURE
MDM
IDENTITIES
IOT
PASSKEYS
BROWSERS
PERMISSIONS
LOCATION
GROUPS
SUBSET
ACCESSED THROUGH
workday
okta
LOCATION
SESSIONS
PERMISSIONS
SaaS
SaaS
ON PREM
ON PREM
aws
SUBSET
WORKLOADS

Smart authentication for users

Smart authentication for things

Remote Employee with Trusted Device:

Remote Access - Accessing Private App (any tcp/udp) (Private IaaS)

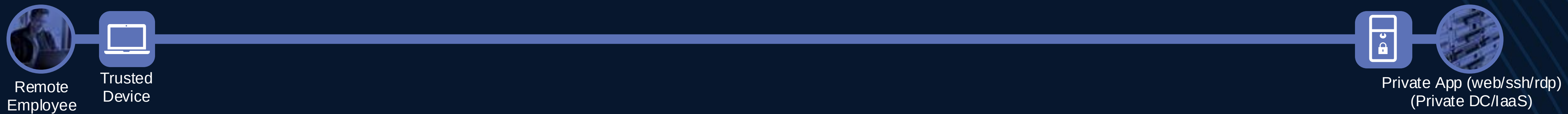


When the remote employee passes the second factor authentication, they are redirected back to the FTD.

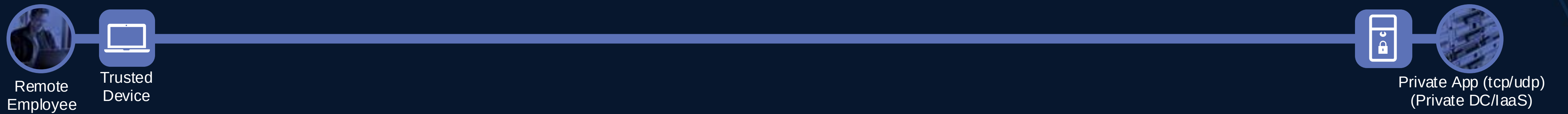
AnyConnect and the FTD establish a tunnel and the user can access the application. Because the application also uses Duo SSO for SAML authentication, access may be granted without the user needing to authenticate again depending on the FTD configuration.

Zero Trust Business Flows

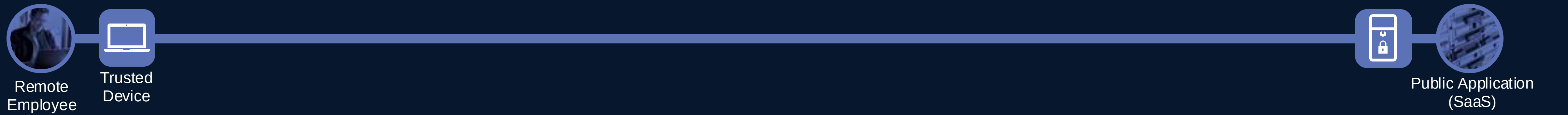
Remote Employee with Trusted Device: Clientless Remote Access to Private Application (web/ssh/rdp) (DC/IaaS)



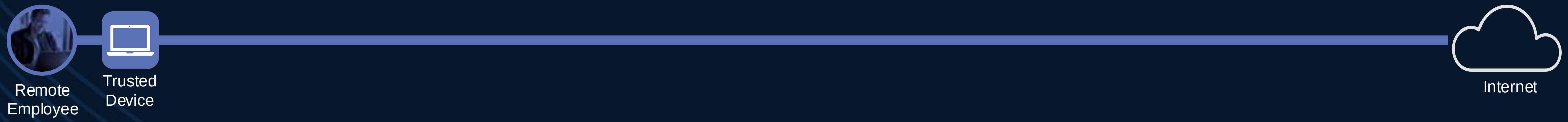
Remote Employee with Trusted Device: Remote Access to Private Application (tcp/udp) (DC/IaaS)



Remote Employee with Trusted Device: Accessing Public Application (SaaS)

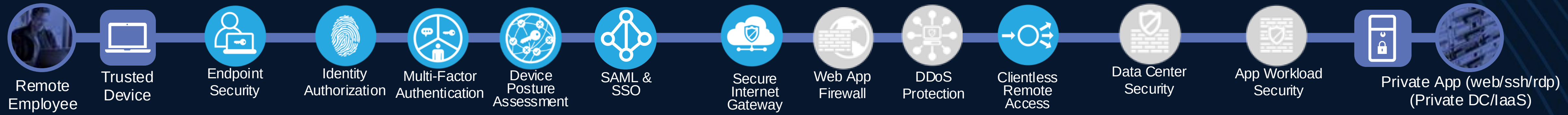


Remote Employee with Trusted Device: Accessing public Internet website



Zero Trust Business Flows

Remote Employee with Trusted Device: Clientless Remote Access to Private Application (web/ssh/rdp) (DC/IaaS)



Remote Employee

Trusted Device

Endpoint Security

Identity Authorization

Multi-Factor Authentication

Device Posture Assessment

SAML & SSO

Secure Internet Gateway

Web App Firewall

DDoS Protection

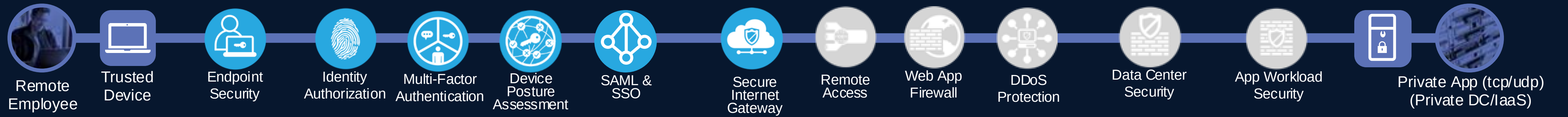
Clientless Remote Access

Data Center Security

App Workload Security

Private App (web/ssh/rdp) (Private DC/IaaS)

Remote Employee with Trusted Device: Remote Access to Private Application (tcp/udp) (DC/IaaS)



Remote Employee

Trusted Device

Endpoint Security

Identity Authorization

Multi-Factor Authentication

Device Posture Assessment

SAML & SSO

Secure Internet Gateway

Remote Access

Web App Firewall

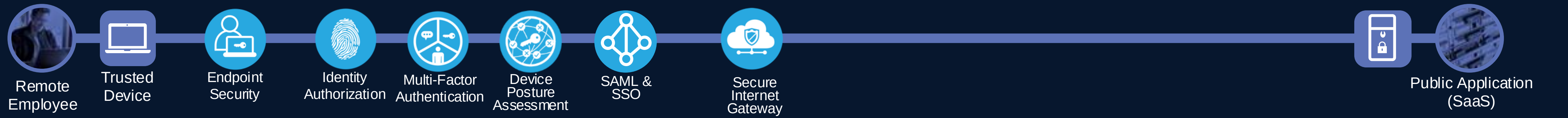
DDoS Protection

Data Center Security

App Workload Security

Private App (tcp/udp) (Private DC/IaaS)

Remote Employee with Trusted Device: Accessing Public Application (SaaS)



Remote Employee

Trusted Device

Endpoint Security

Identity Authorization

Multi-Factor Authentication

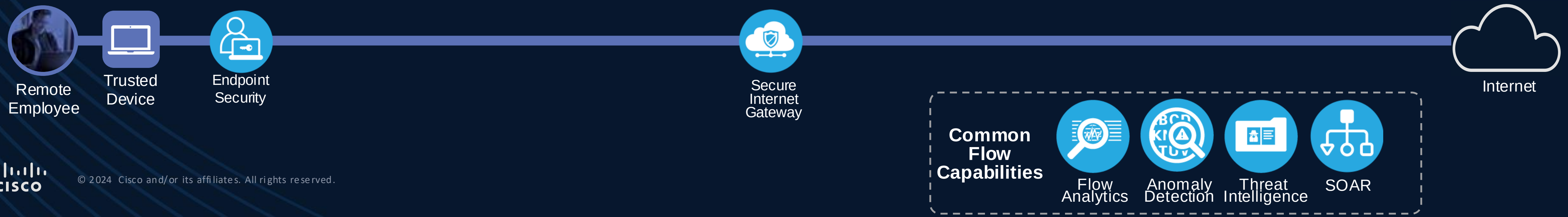
Device Posture Assessment

SAML & SSO

Secure Internet Gateway

Public Application (SaaS)

Remote Employee with Trusted Device: Accessing public Internet website



Remote Employee

Trusted Device

Endpoint Security

Secure Internet Gateway

Internet

Common Flow Capabilities

Flow Analytics

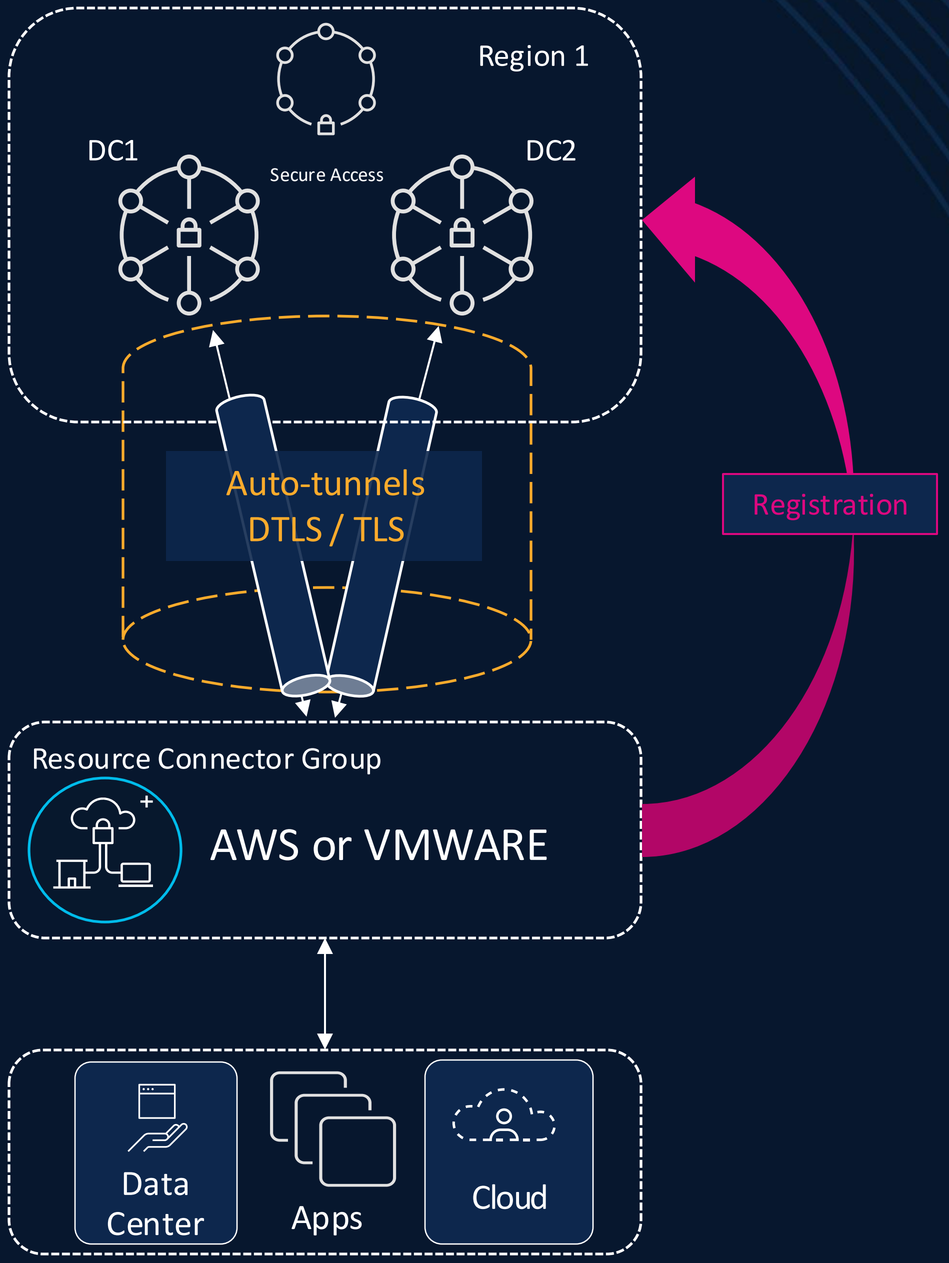
Anomaly Detection

Threat Intelligence

SOAR

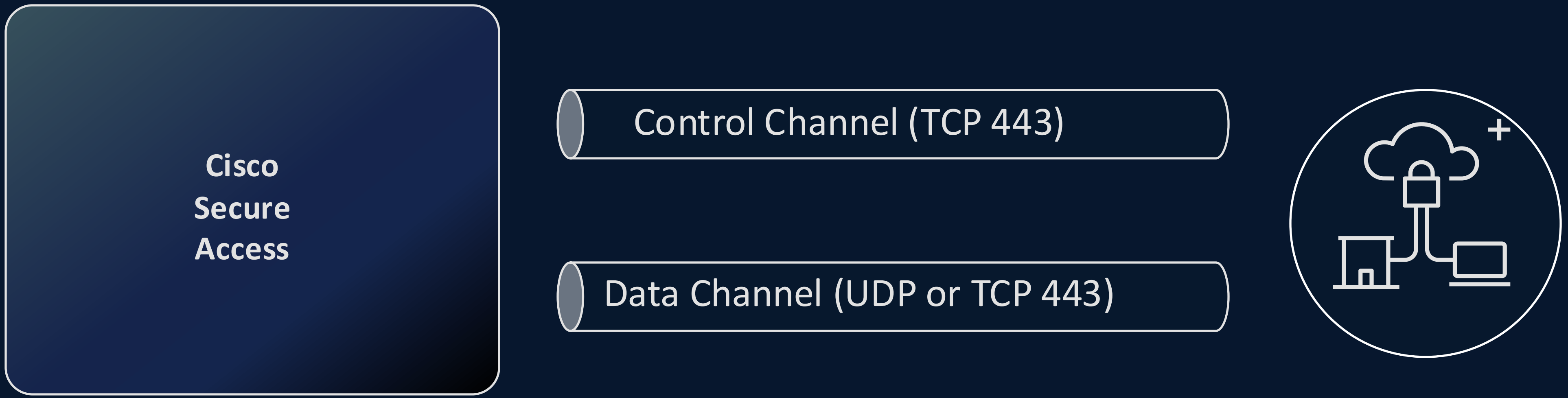
Resource Connector

- Deployed in a group
  - Can be deployed with one member
- Virtual machines
  - AWS Marketplace (c5.xlarge only)
  - VMWare image (OVA)
  - Intel x86_64/AMD64 only
  - IPv4 only
- Registers with dashboard
  - Provisioning key
  - Manual confirmation
- Load balancing
  - Automatic across all in a group
  - Must be same instance type
  - Must be in same region



https://docs.sse.cisco.com/sse-user-guide/docs/allow-resource-connector-traffic-to-secure-access

Resource Connector Communication Channels



Inside-out, Always On

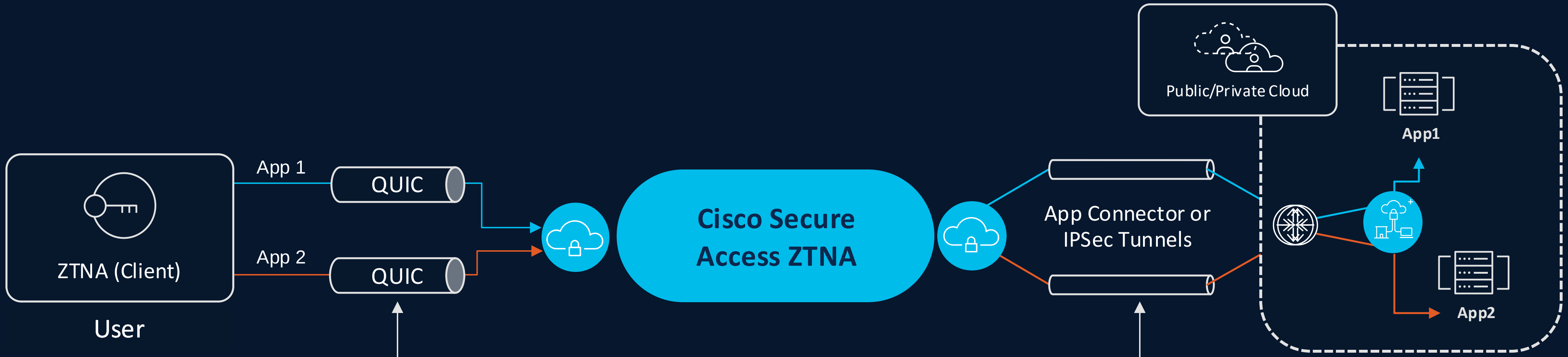
- Data: D(TLS) tunnels for application traffic
- Control: MQTT over TLS
  - on-demand messages from controller to agent: upgrade, revoke, troubleshooting
  - Metrics: basic system and networks statistics, monitor status

Resource Connector Benefits

- Resource connectors can be quickly deployed in AWS and VMWare without any additional infrastructure.
- Resource connectors typically do not require any additional route configuration on the network, nor do they require any changes to firewall rules in most environments.
- Resource connectors can provide connectivity to applications on overlapping IP space. This is very beneficial for mergers and acquisitions where applications in the acquired DC may be on overlapping IP space.
- They are deployed in groups for load balancing and redundancy purposes. Providing the necessary bandwidth and high availability for mission critical applications.

Secure Private Access with Cisco

Industry-first HTTP3-based proxy for secure, segmented zero trust access control



- Dedicated user to app micro-tunnels
- ‘One click’ seamless access
- Advanced protocols speed content delivery

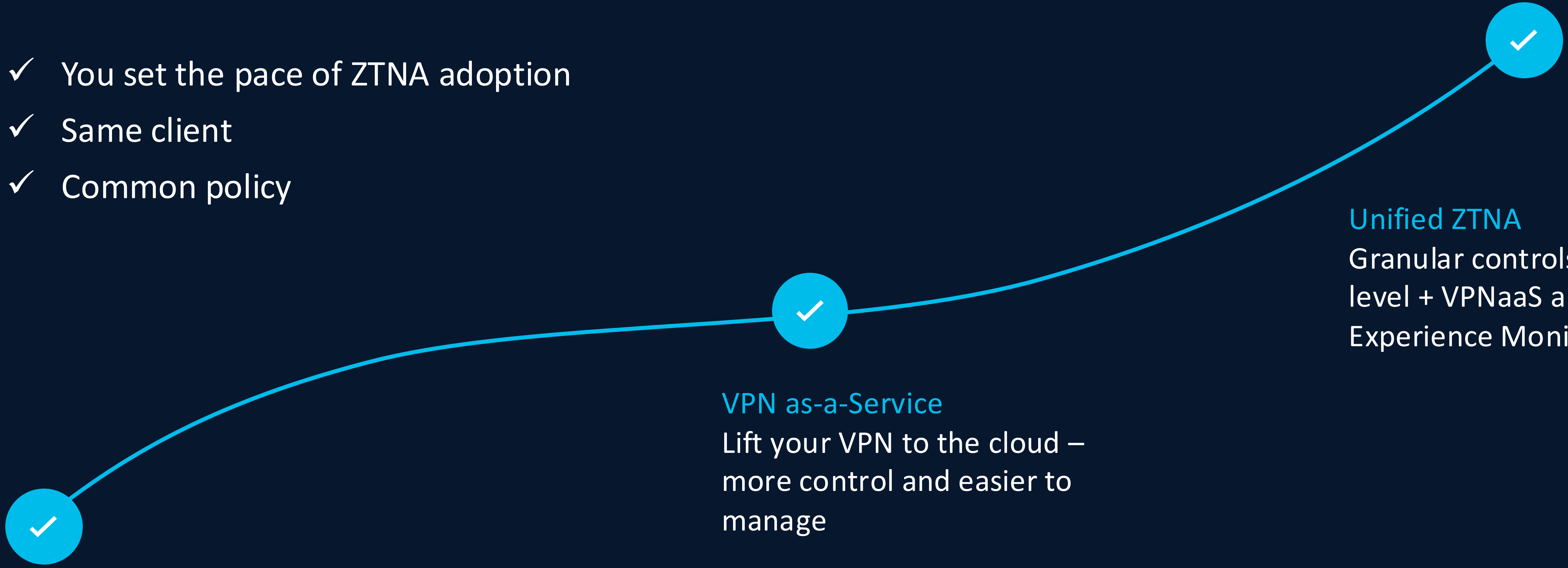
- Optimized L4-7 user to app connectivity
- Fully isolated network-resources are hidden
- Fast deployment with no firewall setting changes

If you’re not ready for ZTNA

Cisco’s flexible approach simplifies migration

Accelerate your SSE and SASE journey with zero trust

- ✓ You set the pace of ZTNA adoption
- ✓ Same client
- ✓ Common policy

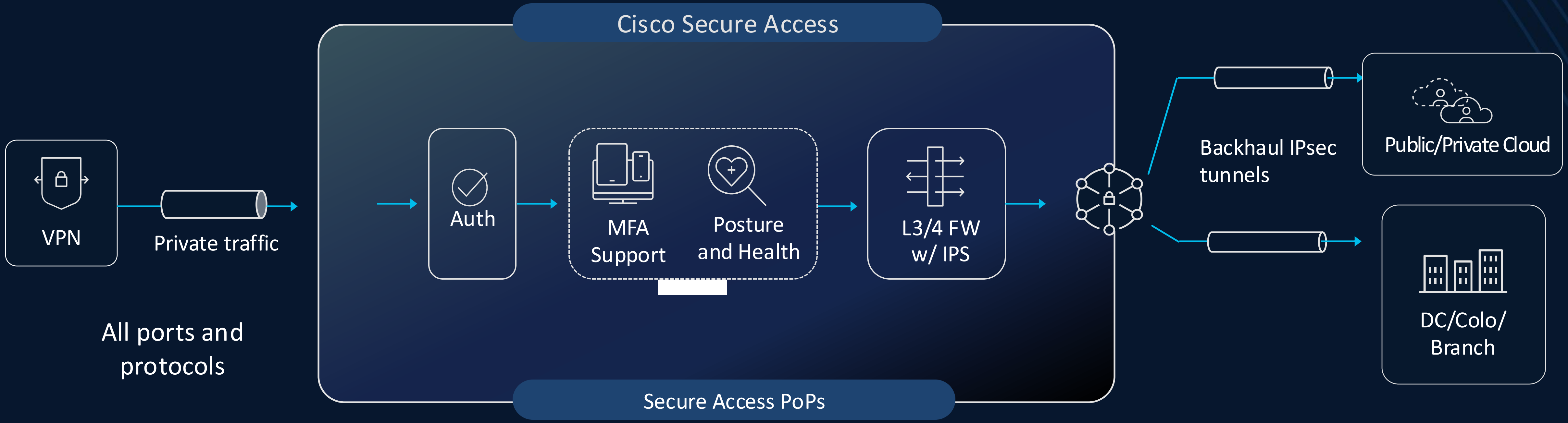


Unified ZTNA
Granular controls at the application level + VPNaaS and Digital Experience Monitoring

VPN as-a-Service
Lift your VPN to the cloud – more control and easier to manage

Traditional VPN
Network level access – cannot control at app level

VPN-as-a-Service



- Authentication Methods:
  SAML 2.0, SAML+ certificate, Certificate, RADIUS
- Identity based access
- Region specific IP pool for client addressing

- Posture Verification: (optional)
  Secure Firewall (formerly hostscan) or ISE with RADIUS
- IPS (optional)
- Connection profiles

Posture

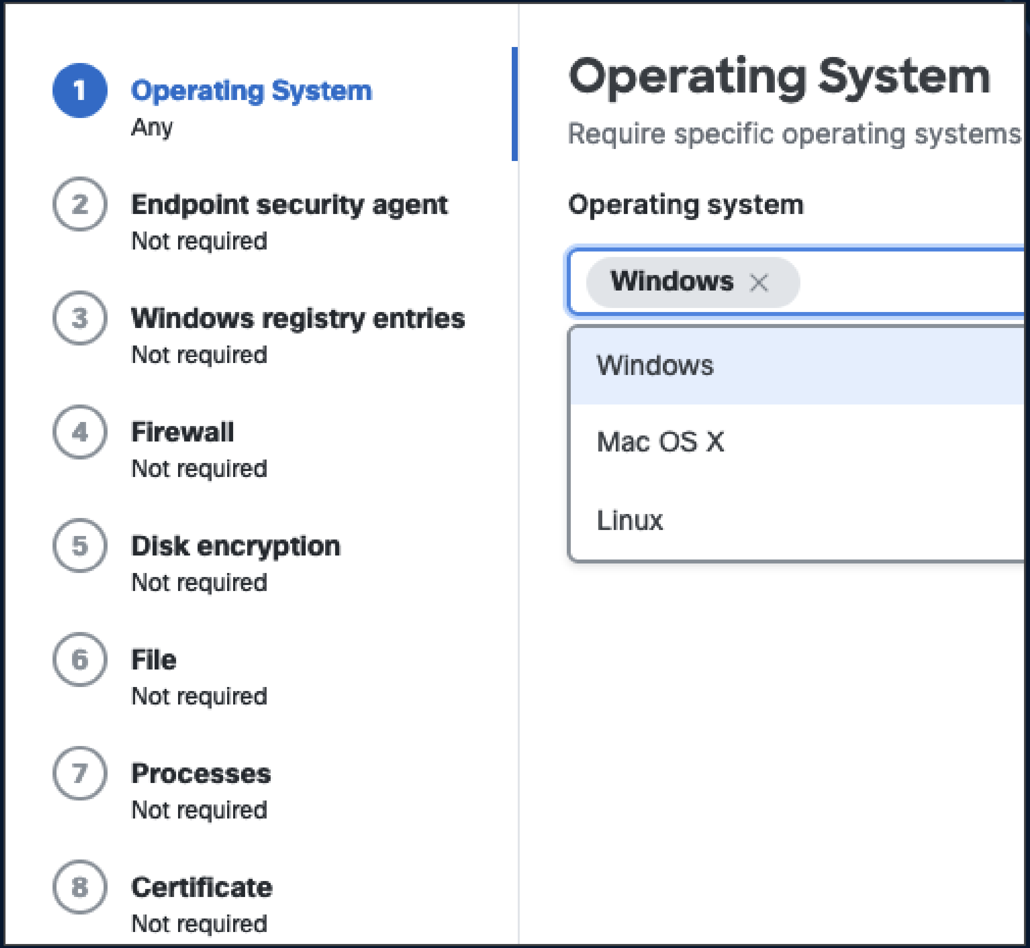
Hostscan

- Packaged with the client installer
- Supports the following attributes:

  Operating system
  Firewall
  Endpoint security agent
  System password
  Disk encryption
  Browser
  Files
  Processes
  Certificates

ISE

- Packaged with the client installer
- [ISE Posture Prescriptive Deployment Guide]



1 Operating System
Any

2 Endpoint security agent
Not required

3 Windows registry entries
Not required

4 Firewall
Not required

5 Disk encryption
Not required

6 File
Not required

7 Processes
Not required

8 Certificate
Not required

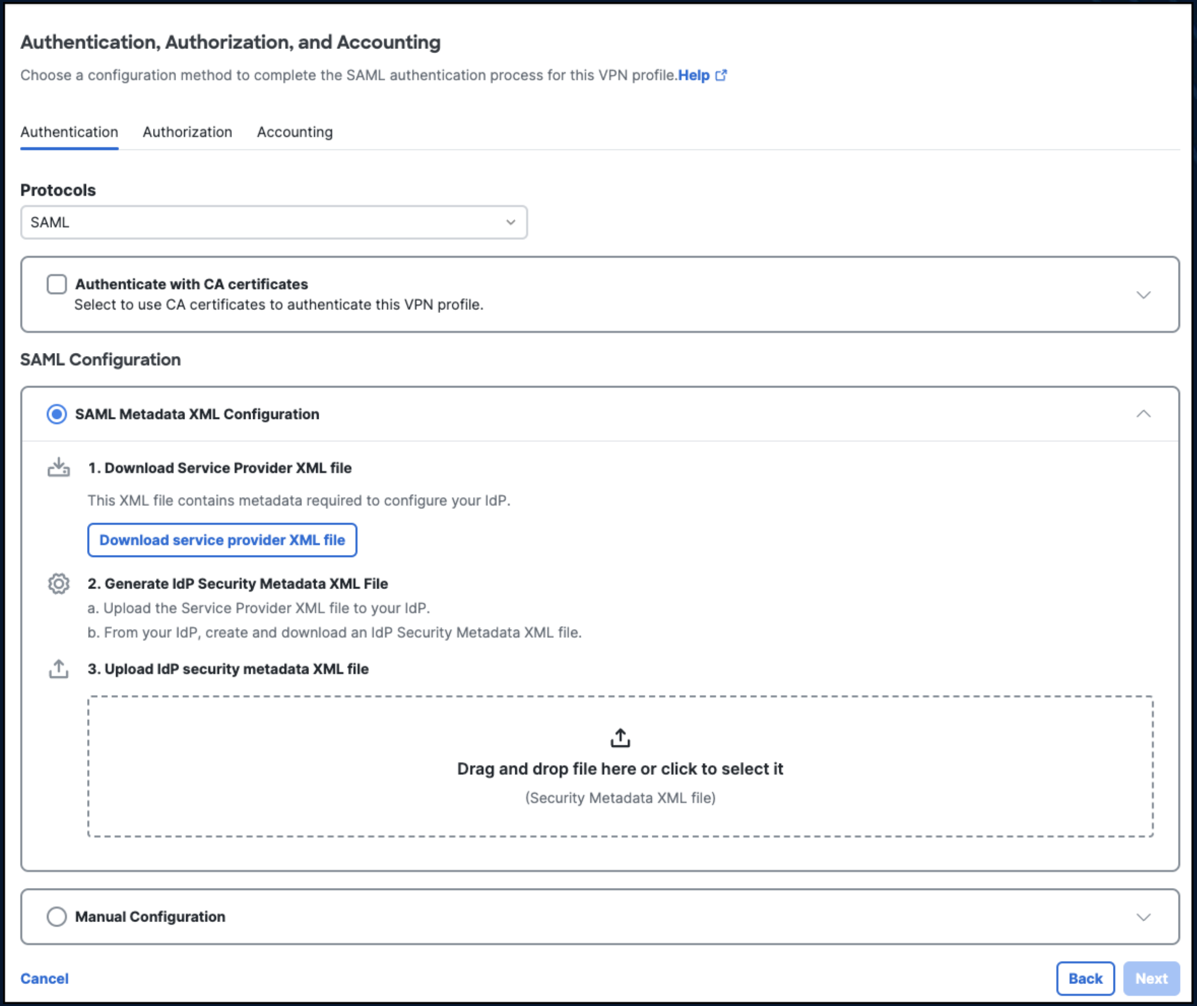
Operating System

Require specific operating systems

Operating system: Windows ×

Authentication Methods: SAML & Certificates

- SAML
  - Any SAML 2.0 Identity provider (IdP)
  - Users must be imported into Secure Access
- Certificate
  - Can be used alone or with SAML
  - PKI is client-managed and must be pre-deployed



Authentication, Authorization, and Accounting

Choose a configuration method to complete the SAML authentication process for this VPN profile.**Help**

Protocols

SAML

□ **Authenticate with CA certificates**
Select to use CA certificates to authenticate this VPN profile.

SAML Configuration

● **SAML Metadata XML Configuration**

1. Download Service Provider XML file

This XML file contains metadata required to configure your IdP.

2. Generate IdP Security Metadata XML File

a. Upload the Service Provider XML file to your IdP.

b. From your IdP, create and download an IdP Security Metadata XML file.

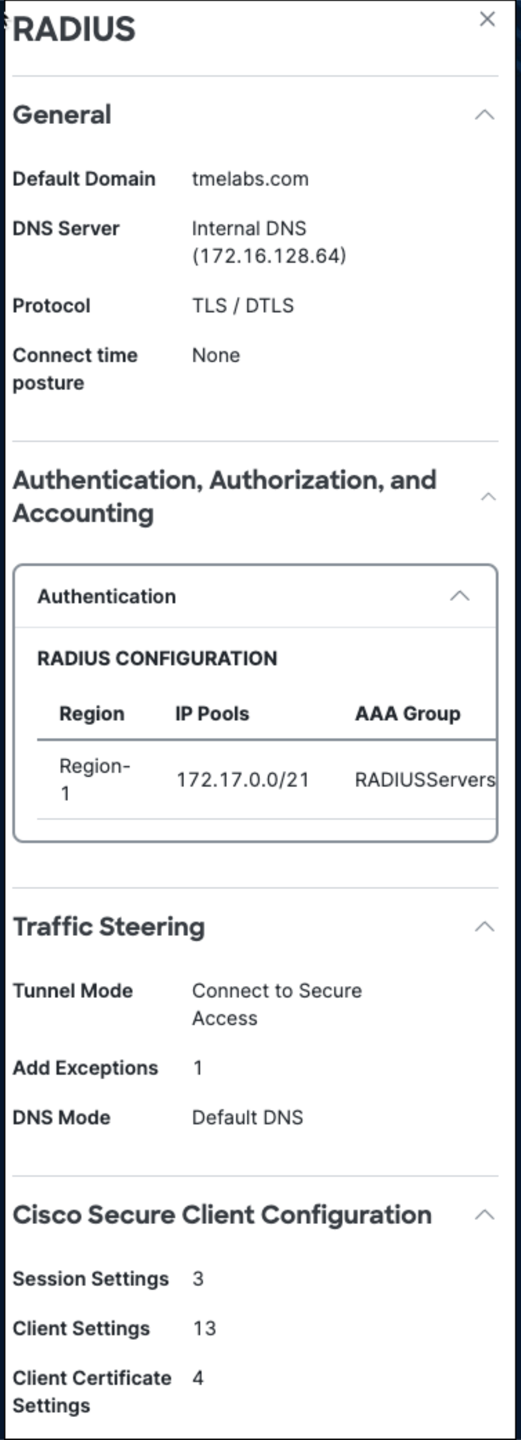
3. Upload IdP security metadata XML file

Drag and drop file here or click to select it
(Security Metadata XML file)

○ **Manual Configuration**

Authentication Methods: RADIUS

- Cisco Identity Services Engine (ISE) or 3rd Party RADIUS supported
- AAA or authorize only
- Up to 8 servers within a single server group
- Dynamic ACLs supported
- CoA support with Cisco ISE
- ISE posture supported (optional)



RADIUS

General

Default Domain	tmelabs.com
DNS Server	Internal DNS (172.16.128.64)
Protocol	TLS / DTLS
Connect time posture	None

Authentication, Authorization, and Accounting

Authentication

RADIUS CONFIGURATION

Region	IP Pools	AAA Group
Region-1	172.17.0.0/21	RADIUSServers

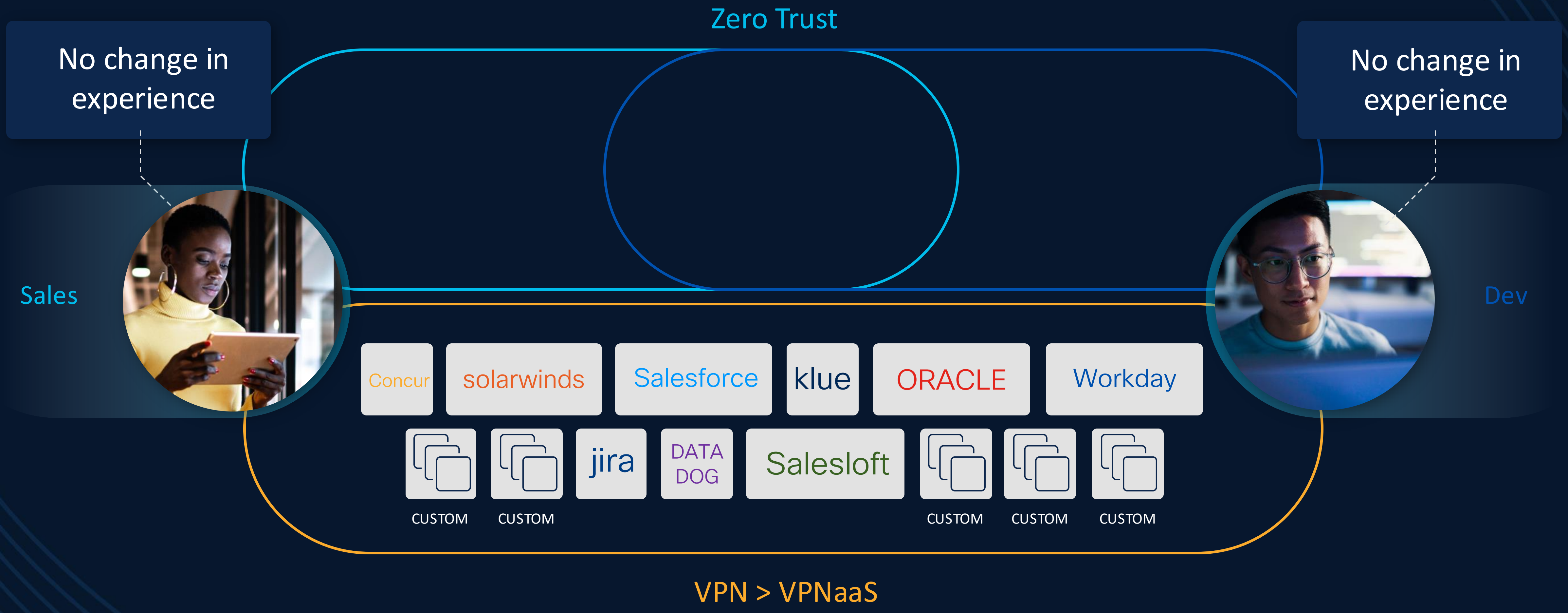
Traffic Steering

Tunnel Mode	Connect to Secure Access
Add Exceptions	1
DNS Mode	Default DNS

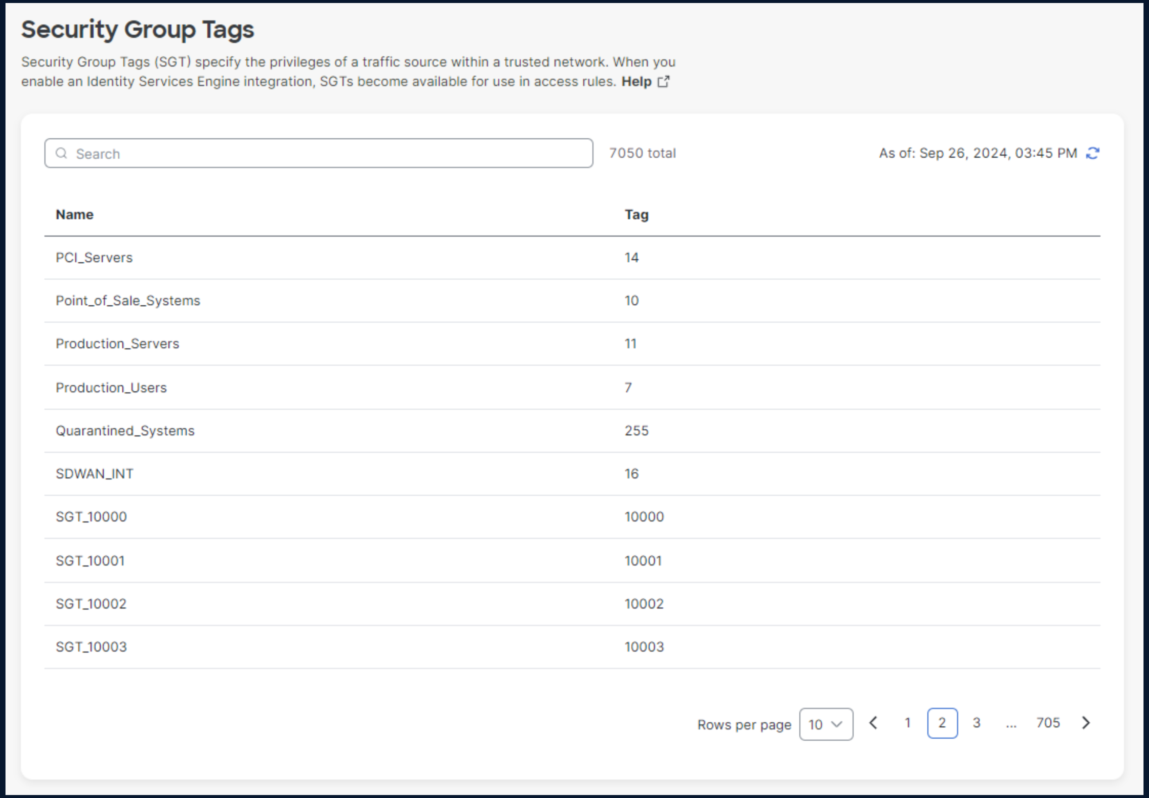
Cisco Secure Client Configuration

Session Settings	3
Client Settings	13
Client Certificate Settings	4

Simplifying the journey to zero trust



Segmentation with ISE and Trustsec



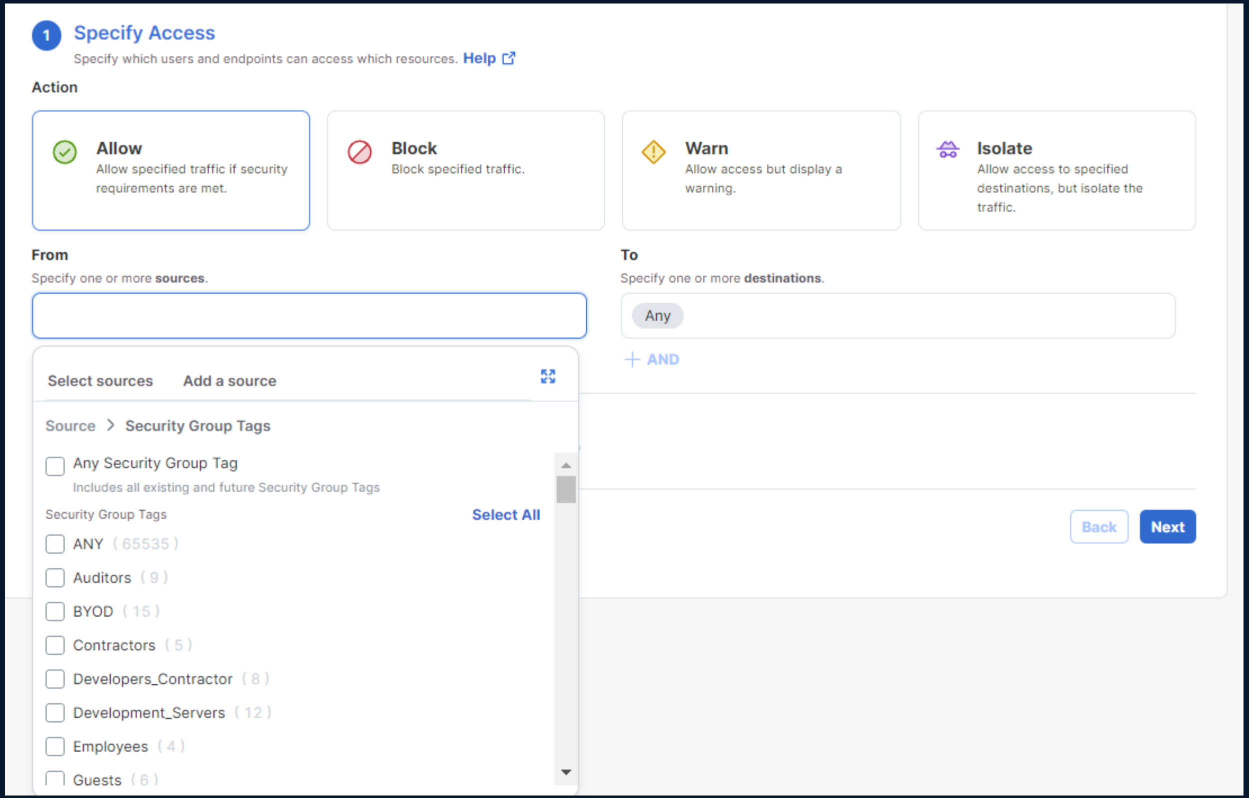
Security Group Tags

Security Group Tags (SGT) specify the privileges of a traffic source within a trusted network. When you enable an Identity Services Engine integration, SGTs become available for use in access rules. **Help**

Search | 7050 total | As of: Sep 26, 2024, 03:45 PM

Name	Tag
PCI_Servers	14
Point_of_Sale_Systems	10
Production_Servers	11
Production_Users	7
Quarantined_Systems	255
SDWAN_INT	16
SGT_10000	10000
SGT_10001	10001
SGT_10002	10002
SGT_10003	10003

Rows per page 10 ‹ 1 2 3 ... 705 ›



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.
- **Warn** – Allow access but display a warning.
- **Isolate** – Allow access to specified destinations, but isolate the traffic.

From

Specify one or more **sources**.

To

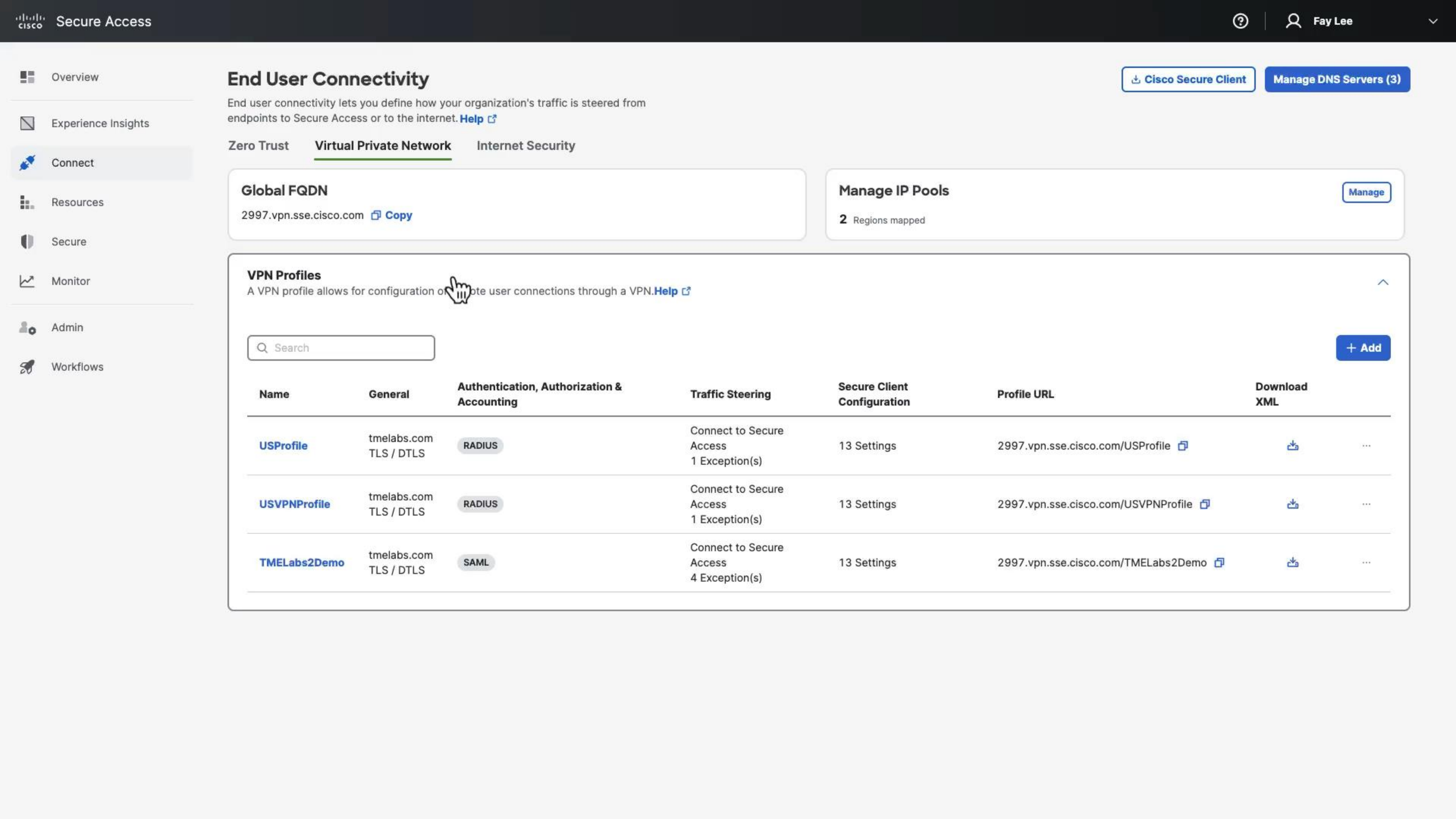
Specify one or more **destinations**.

Any

□ Any Security Group Tag
Includes all existing and future Security Group Tags

Security Group Tags **Select All**

□ ANY (65535)
□ Auditors (9)
□ BYOD (15)
□ Contractors (5)
□ Developers_Contractor (8)
□ Development_Servers (12)
□ Employees (4)
□ Guests (6)



End User Connectivity

End user connectivity lets you define how your organization's traffic is steered from endpoints to Secure Access or to the internet. Help

Global FQDN

2997.vpn.sse.cisco.com Copy

Manage IP Pools

2 Regions mapped

VPN Profiles

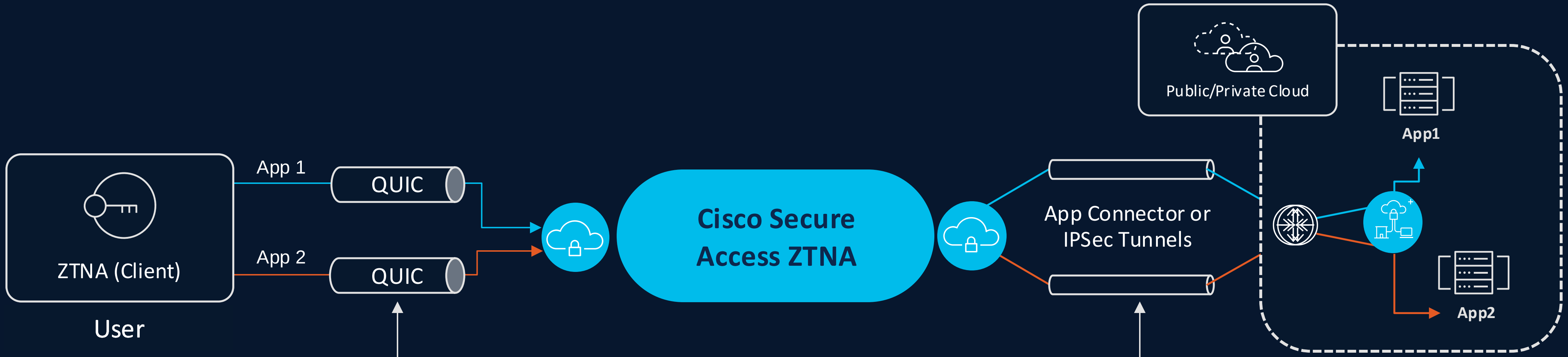
A VPN profile allows for configuration of remote user connections through a VPN. Help

Name	General	Authentication, Authorization & Accounting	Traffic Steering	Secure Client Configuration	Profile URL	Download XML
USProfile	tmelabs.com TLS / DTLS	RADIUS	Connect to Secure Access 1 Exception(s)	13 Settings	2997.vpn.sse.cisco.com/USProfile	
USVPNProfile	tmelabs.com TLS / DTLS	RADIUS	Connect to Secure Access 1 Exception(s)	13 Settings	2997.vpn.sse.cisco.com/USVPNProfile	
TMELabs2Demo	tmelabs.com TLS / DTLS	SAML	Connect to Secure Access 4 Exception(s)	13 Settings	2997.vpn.sse.cisco.com/TMELabs2Demo	

Client-based access

Client-based Zero Trust Access

Industry-first HTTP3-based proxy for secure, segmented zero trust access control

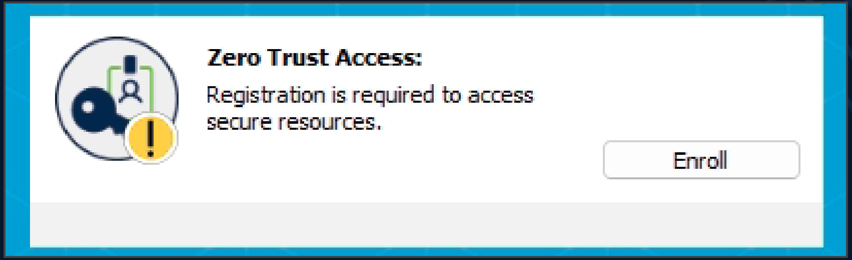


- Dedicated user to app micro-tunnels
- ‘One click’ seamless access
- Advanced protocols speed content delivery

- Optimized L4-7 user to app connectivity
- Fully isolated network-resources are hidden
- Fast deployment with no firewall setting changes

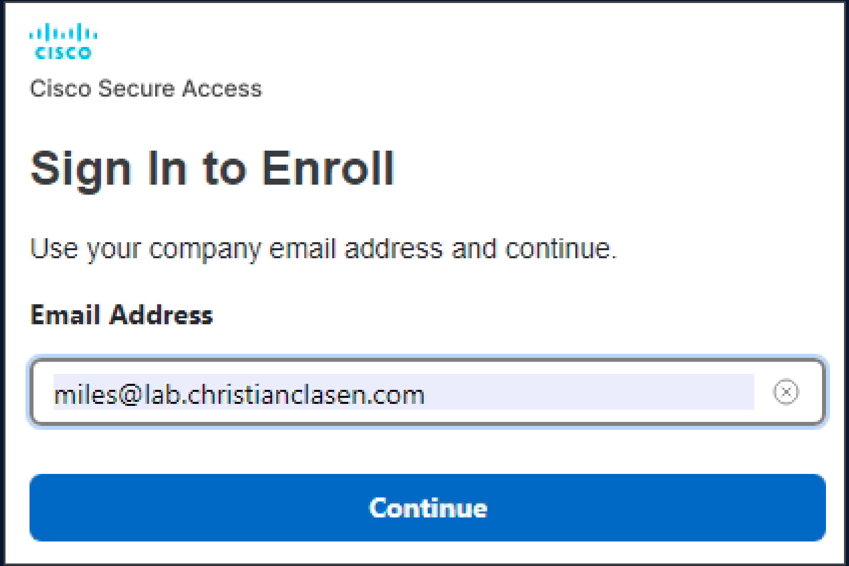
Client-based ZTA: Enrollment

- New users are prompted to enroll by the Secure Client
  - User input email address as username
  - IdP must be pre-configured in Secure Access
  - User must be in the list of imported users
- User is presented with a list of their tenants
  - One IdP per tenant is supported
  - One enrollment per local user is supported
  - SAML redirection to configured IdP
- Once enrolled, a certificate is pushed to the client
  - Saved in the TPM (required)
  - Auto-renewal occurs within two weeks of expiration
  - Re-enrollment is required if the device is offline during renewal period



Zero Trust Access:

Registration is required to access secure resources.



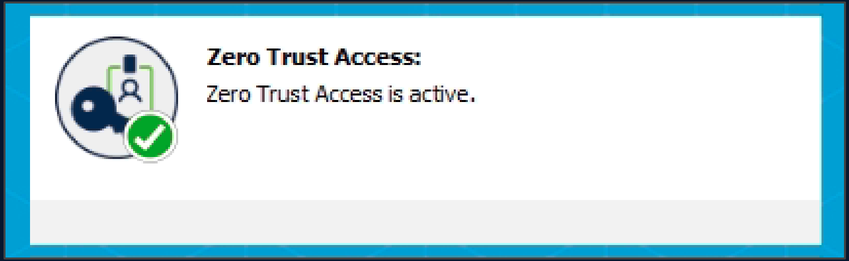
Cisco Secure Access

Sign In to Enroll

Use your company email address and continue.

Email Address

miles@lab.christianclasen.com

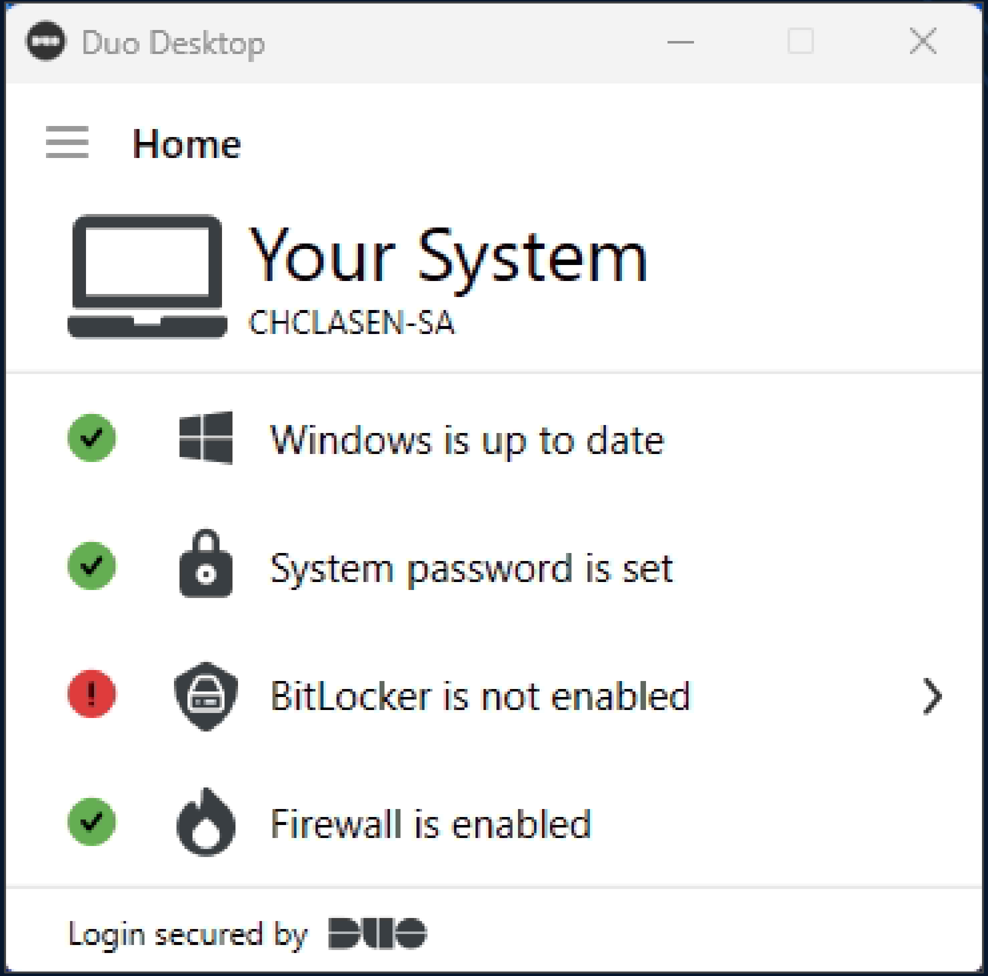


Zero Trust Access:

Zero Trust Access is active.

Client-based ZTA: Posture

- Posture checks provided by Duo Health Agent
  - Packaged with the client installer
  - Updated every 30 minutes
- Supports the following attributes:
  - Operating system
  - Firewall
  - Endpoint security agent
  - System password
  - Disk encryption
  - Browser



Your System
CHCLASEN-SA

✓ Windows is up to date

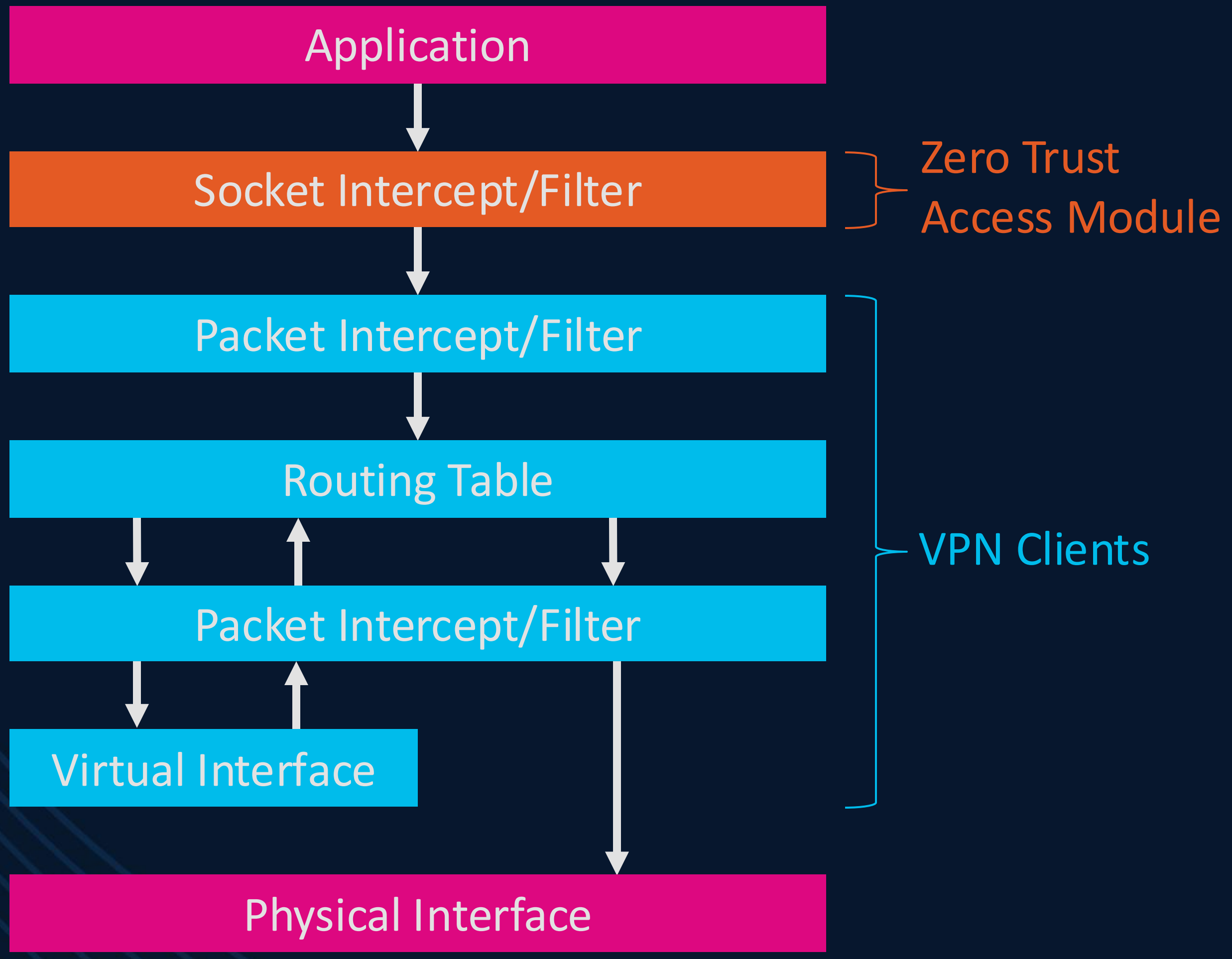
✓ System password is set

! BitLocker is not enabled

✓ Firewall is enabled

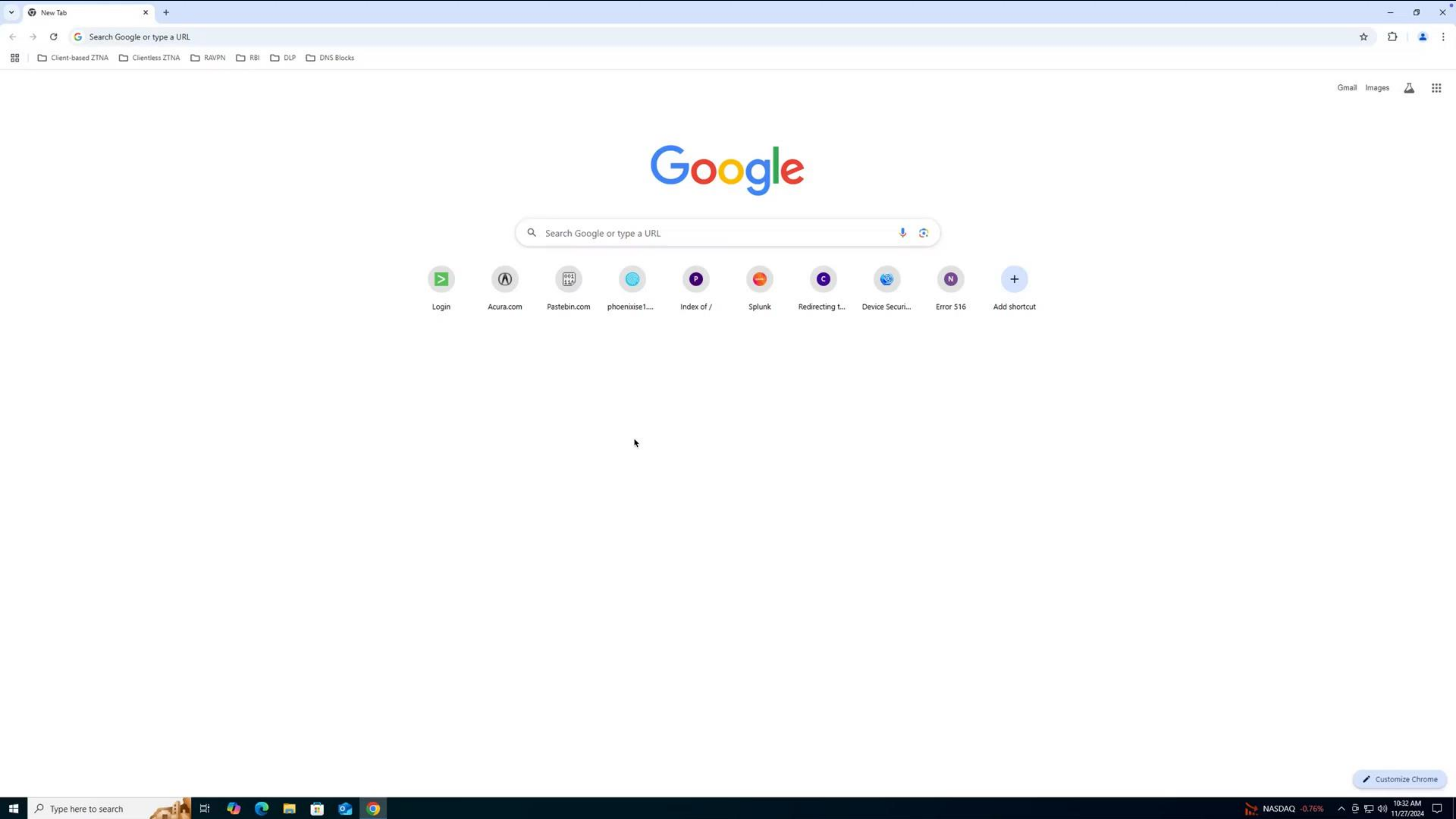
Login secured by DUO

Secure Client ZTA Module: Socket Intercept



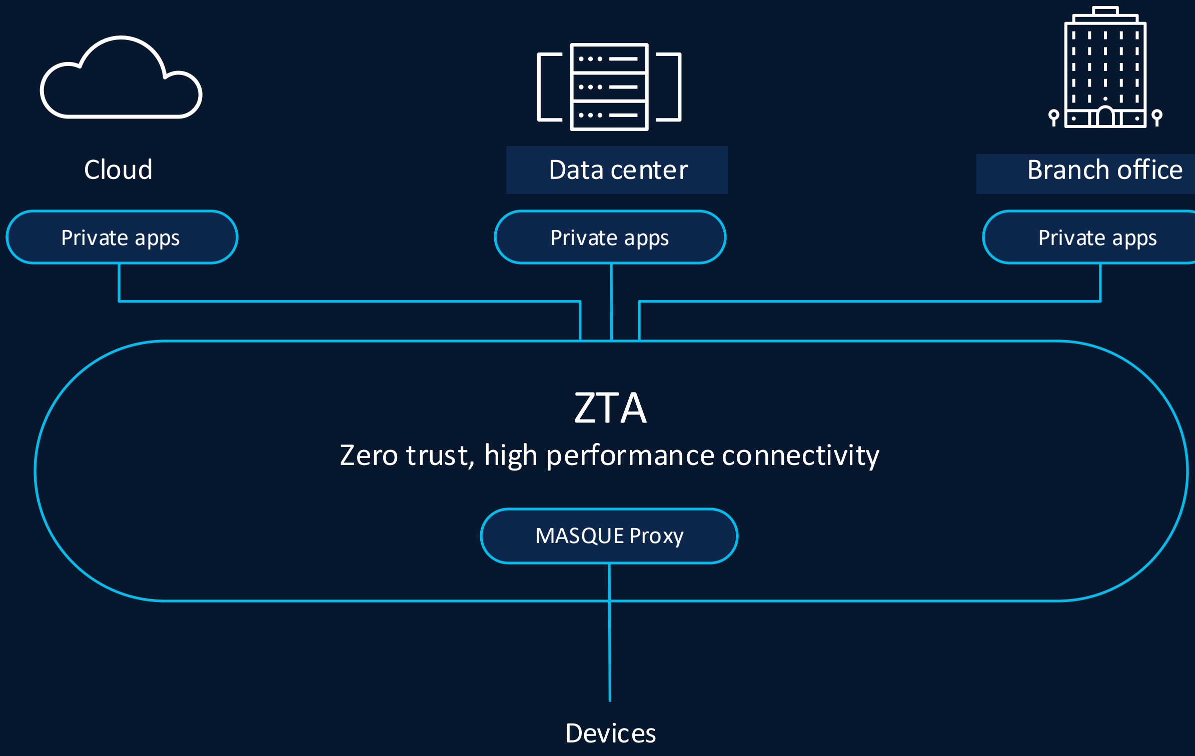
Why Socket Intercept?

- Control of DNS and application traffic *before* VPN clients
- No route table manipulation
- Ability to capture traffic by IP, IP subnet, FQDN and FQDN wildcard
- Interoperability with Cisco and non-Cisco VPNs


New Tab
Search Google or type a URL
Client-based ZTNA
Clientless ZTNA
RAVPN
RBI
DLP
DNS Blocks
Gmail
Images
Google
Search Google or type a URL
Login
Acura.com
Pastebin.com
phoenixise1....
Index of /
Splunk
Redirecting t...
Device Securi...
Error 516
Add shortcut
Customize Chrome
Type here to search
NASDAQ -0.76%
10:32 AM
11/27/2024

Mobile

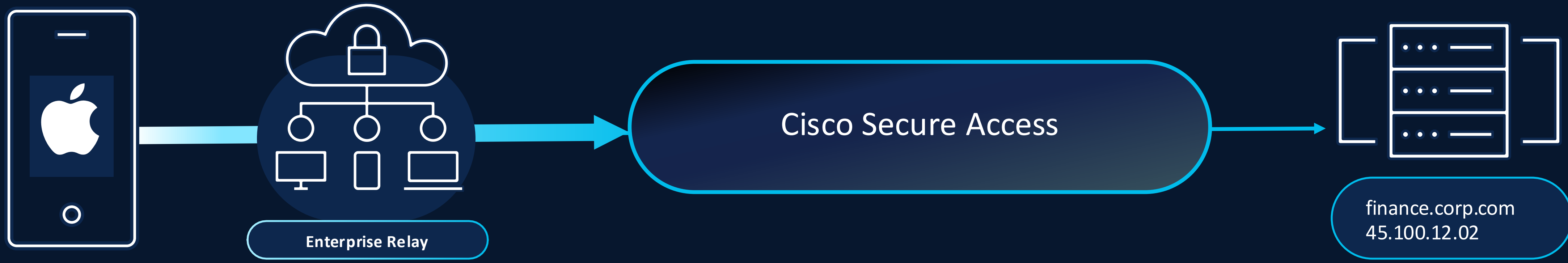
OS Native ZTA: Apple iOS and Samsung Knox



- New OS native ZTA functionality built into Apple iOS 17 and Samsung Knox 3.10
- Transparent user experience for users – no need to start or wait for VPN
- Delivers low latency and high throughput connectivity by directly intercepting traffic within the application (iOS)
- Preserves battery life by eliminating the need for device-wide, continuously running VPN connections
- iCloud Private Relay compatible (iOS)
- Built on industry leading technologies: MASQUE and QUIC
- Supports all applications, ports and protocols - not just web applications

Cisco Secure Access traffic optimization with Apple IOS

OS Native ZTA with Apple Enterprise Relay



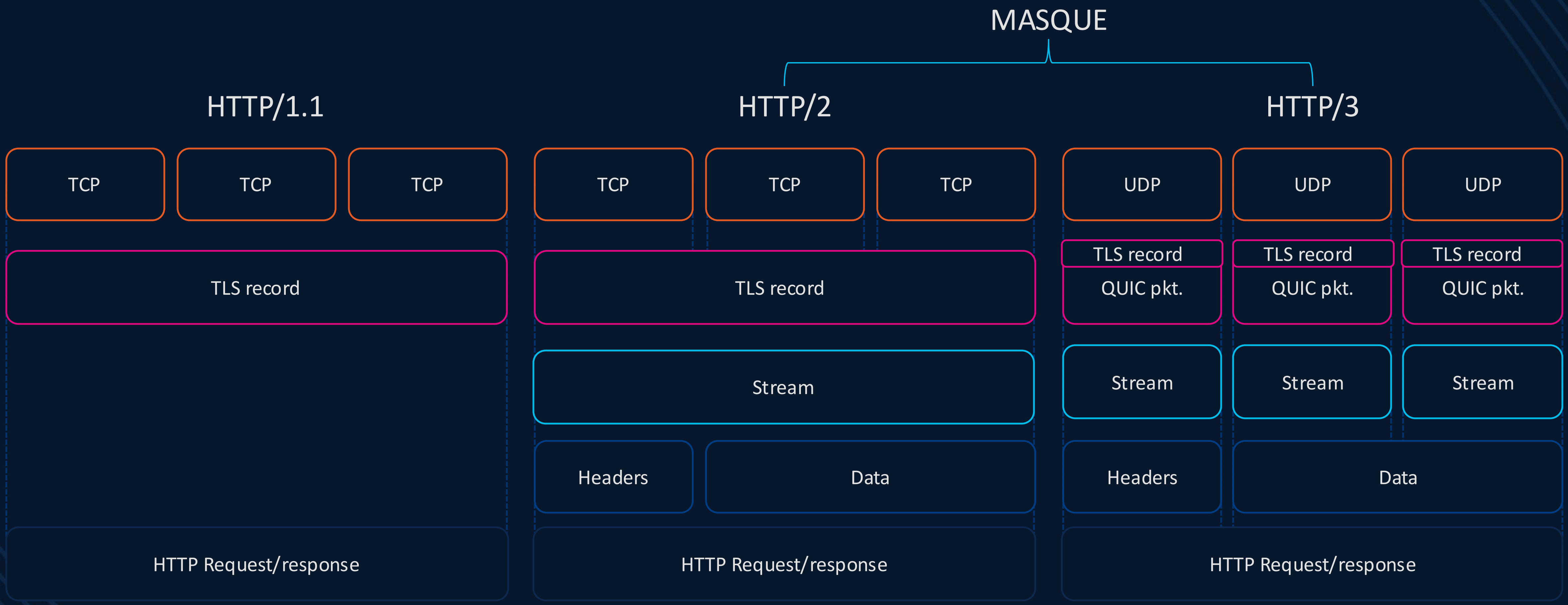
Single layer of encryption for lightning-fast, secure access and compatible with iCloud Private Relay

Traffic Flow w/o Enterprise Relay Enabled:
Device → Secure Access → Application

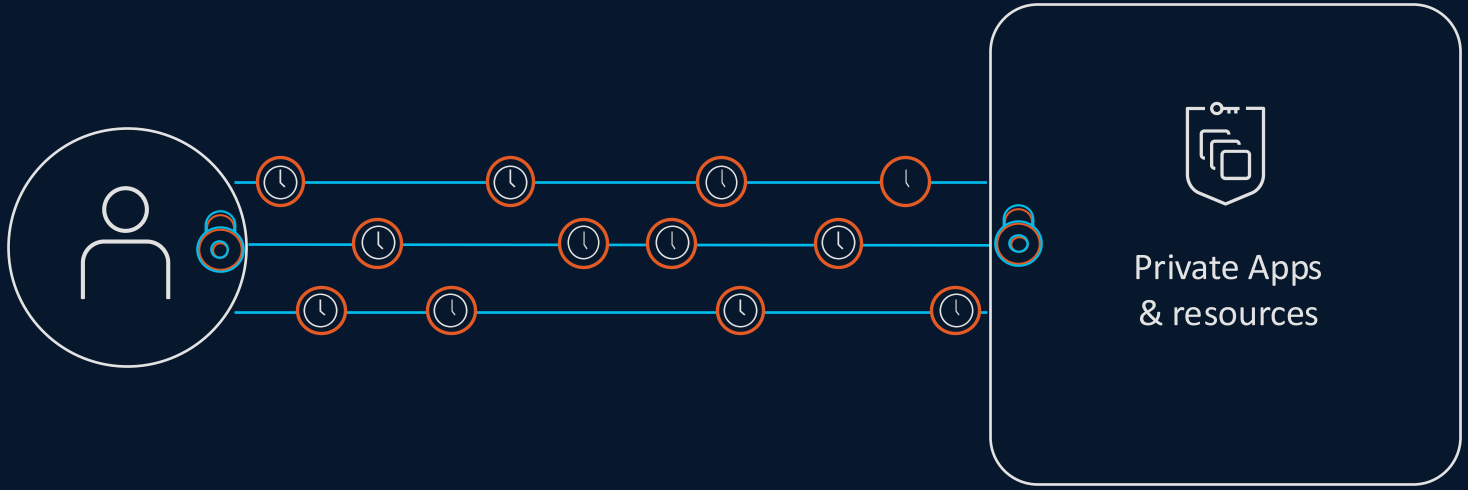
Traffic Flow w/ Enterprise Relay Enabled:
Device → Enterprise Relay → Secure Access → Application

Why MASQUE?

HTTP formats for forward proxying



MASQUE protocol micro-segmentation



Value achieved

- Unified policy makes creating / managing user based zero trust policies easy
- Trust state is evaluated for every flow
- Least privileged access enforced for every resource
- Users only see the resources policy says they should
- Micro-segmentation directly from inside the OS at a process level

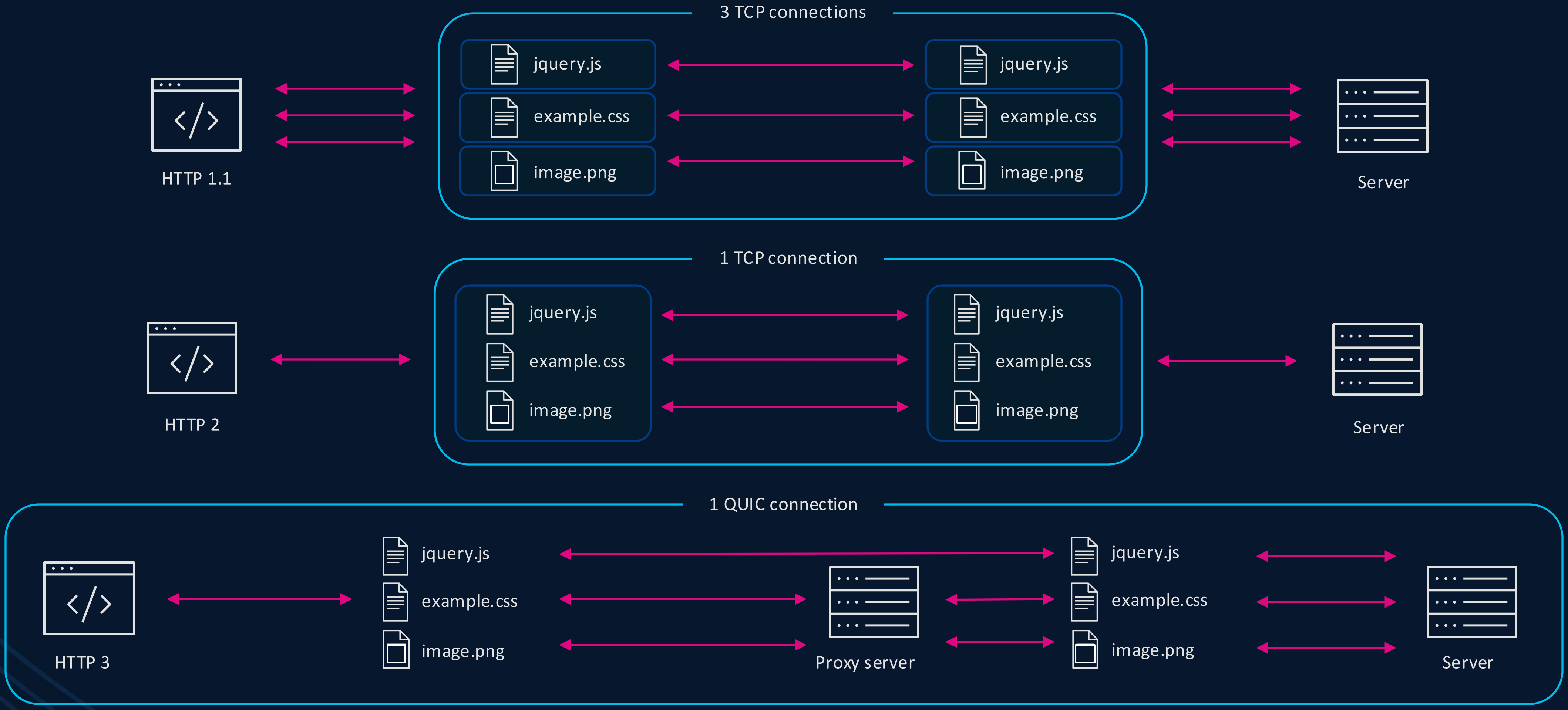
Why QUIC?

Benefits of the QUIC protocol

Fast	Better user experience than TCP/TLS for HTTP/2
Secure	Always-encrypted end-to-end security
Evolvable	Not set in stone, new versions deployed quickly
Compatible	Supports all TCP content while avoiding known TCP issues

UDP + CC + TLS + HTTP = QUIC

Connection evolution from TCP to QUIC connections



Zero Trust Access Benefits of QUIC?

- Ability to change IPs without renegotiation
- No waiting for partially delivered packets
- Not vulnerable to TCP meltdown
- No head-of-line blocking
- Can simultaneously use multiple interfaces
- Faster speeds means faster access

Vendors embracing QUIC and other next generation protocols

CISCO

Enterprise Relay (MASQUE) Zero Trust Access clients and proxies, QUIC capable firewalls

SAMSUNG

OS native Enterprise Relay (MASQUE)
Zero Trust
Access Framework

Apple

Private Relay, OS native Enterprise Relay (MASQUE)
Zero Trust Access client, kernel QUIC implementation

Microsoft

SMB over QUIC, Kernel QUIC implementation, edge browser

Google

Chrome browser, Chromium open-source, Envoy & Quiche MASQUE Proxies (50% of traffic
is QUIC)

fastly

h2o open-source MASQUE proxy used for Private Relay and Enterprise Relay ecosystems worldwide

CLOUDFLARE

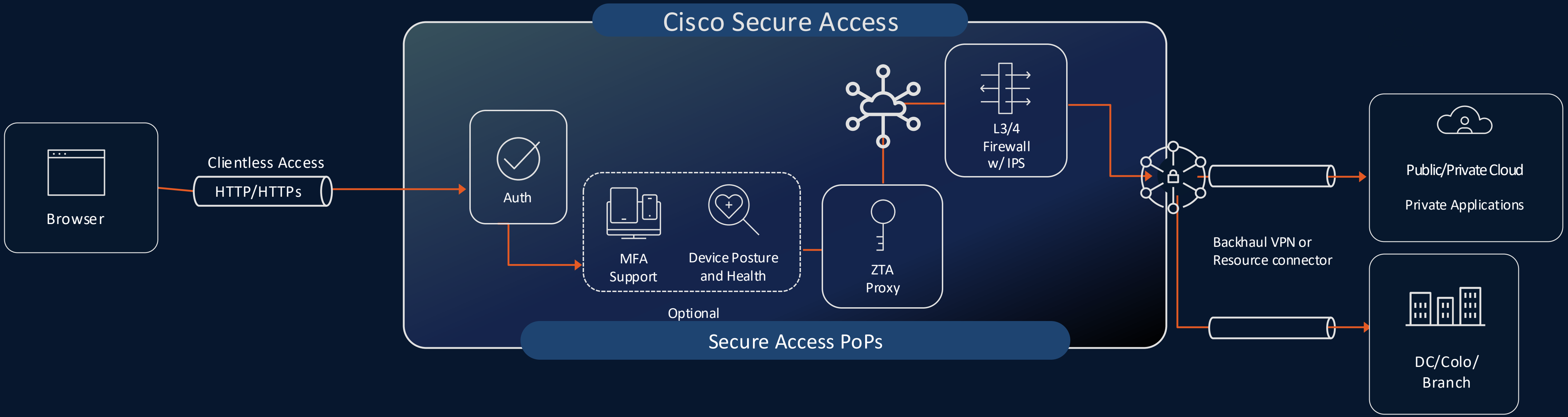
Quiche open-source MASQUE proxy used for Private
Relay worldwide. Zero Trust Access client

Akamai

MASQUE proxy used for Private Relay worldwide

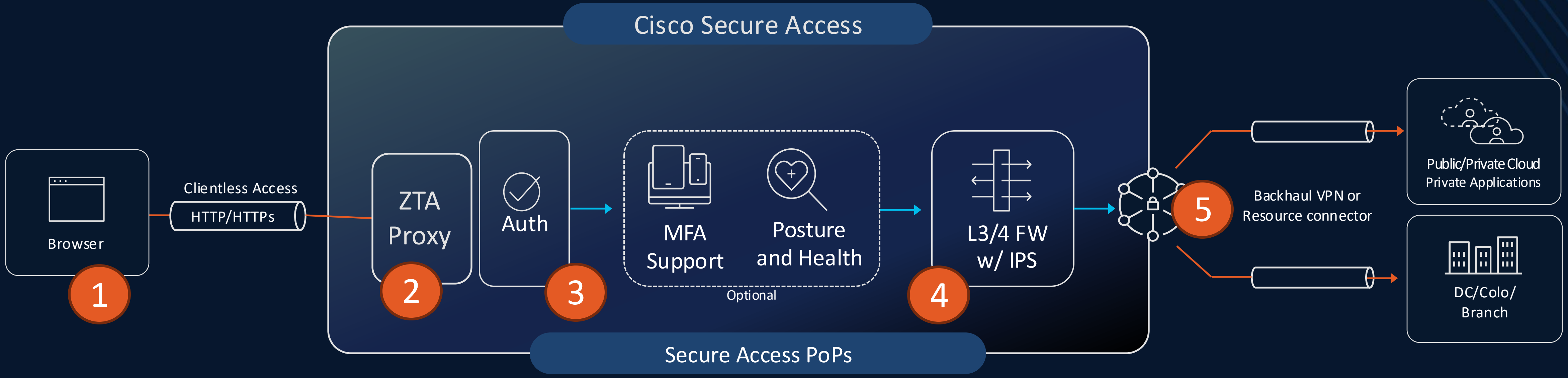
Clientless access

Clientless Zero Trust Access

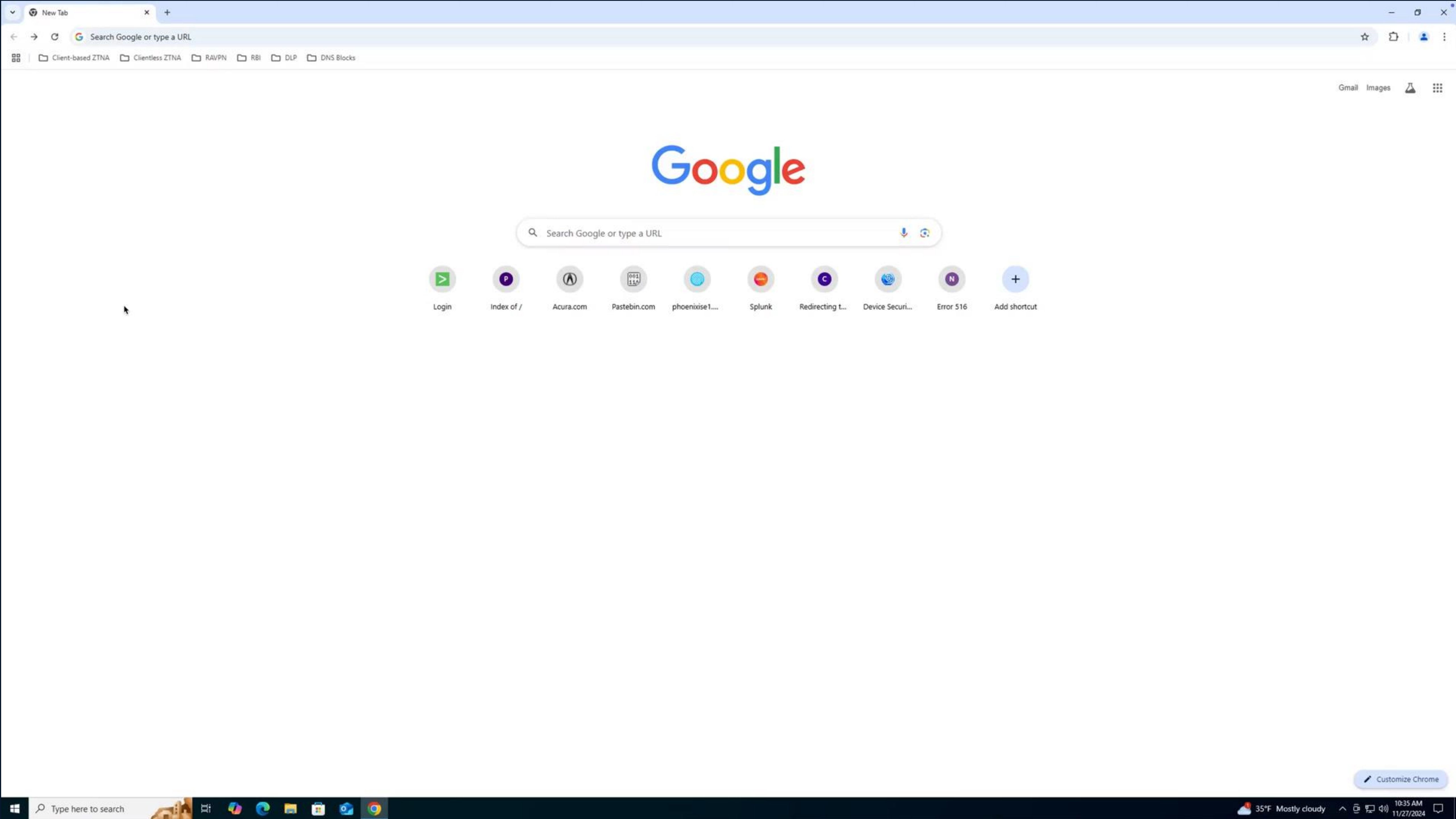


- Ideal for unmanaged devices and BYOD use-cases
- Automatically generated publicly resolvable FQDN for per app access
- Posture (optional) verification based on HTTP headers
- SAML authentication

Clientless/Browser based Access



1. Client initiates a browser connection to the application specific URL. The request gets resolved and redirected to the nearest Datacenter based upon Anycast DNS.
2. The ZTA Proxy changes the traffic source to an address within 100.64.0.0/16.
3. The request is sent for authentication and posture check
4. Once authenticated and authorized, it will redirect the request to the policy engine, where the decision is made to let the request in or not based on your set policies
5. Once decided, it will be sent to our routing engine to deliver traffic to the application correctly


New Tab
Search Google or type a URL
Client-based ZTNA
Clientless ZTNA
RAVPN
RBI
DLP
DNS Blocks
Gmail
Images
Google
Search Google or type a URL
Login
Index of /
Acura.com
Pastebin.com
phoenixise1....
Splunk
Redirecting t...
Device Securi...
Error 516
Add shortcut
Customize Chrome
Type here to search
35°F Mostly cloudy
10:35 AM
11/27/2024

Streamlining Operations

Posture

Authorization check prior to application access

Authorization and access check per session

Supported AV vendors:
Client-based ZTA

VPN-as-a-service

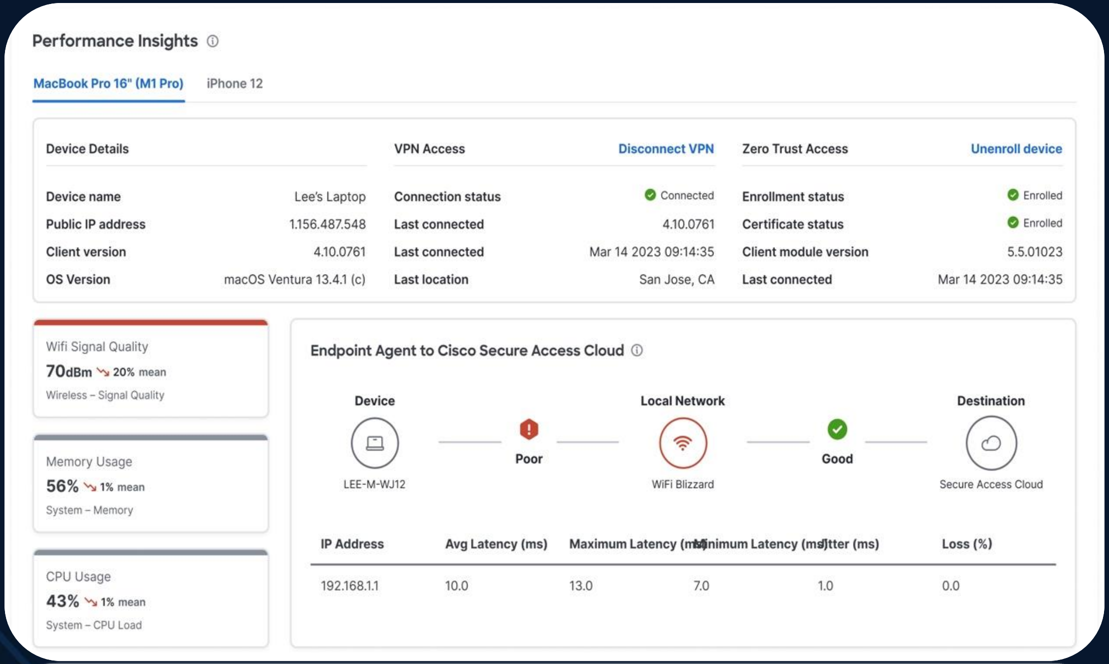
	VPNaaS	ZTA Client-based	ZTA Browser
Operating System	✓	✓	✓
Anti-Malware	✓	✓	
Firewall	✓	✓	
Disk Encryption	✓	✓	
Certificate Check	✓		
Browser Check	✓		✓
System Password		✓	
File Check	✓		
Registry Check (windows only)	✓		
Process Check	✓		

Introducing Experience Insights

User experience monitoring for applications and users

POWERED BY ThousandEyes

Monitor health and performance as users access applications and resources



Performance Insights ⓘ

MacBook Pro 16" (M1 Pro) | iPhone 12

Device Details	
Device name	Lee's Laptop
Public IP address	1.156.487.548
Client version	4.10.0761
OS Version	macOS Ventura 13.4.1 (c)

VPN Access	Disconnect VPN
Connection status	✓ Connected
Last connected	4.10.0761
Last connected	Mar 14 2023 09:14:35
Last location	San Jose, CA

Zero Trust Access	Unenroll device
Enrollment status	✓ Enrolled
Certificate status	✓ Enrolled
Client module version	5.5.01023
Last connected	Mar 14 2023 09:14:35

Wifi Signal Quality
70dBm ↘ 20% mean
Wireless – Signal Quality

Memory Usage
56% ↘ 1% mean
System – Memory

CPU Usage
43% ↘ 1% mean
System – CPU Load

Endpoint Agent to Cisco Secure Access Cloud ⓘ

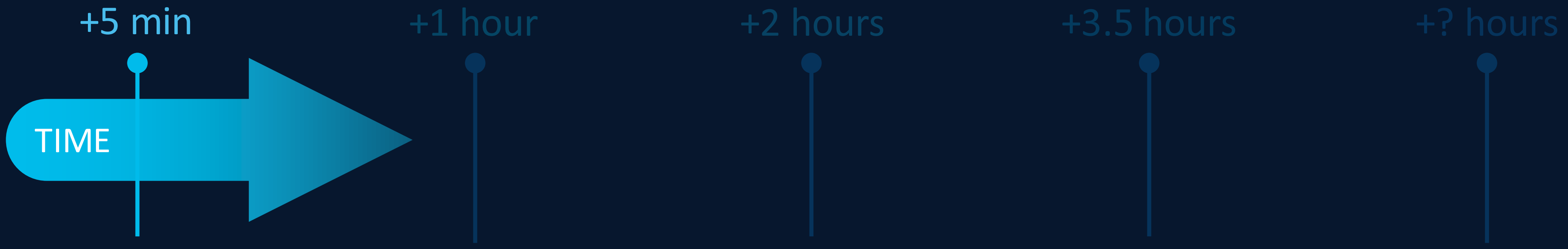
IP Address	Avg Latency (ms)	Maximum Latency (ms)	Minimum Latency (ms)	Jitter (ms)	Loss (%)
192.168.1.1	10.0	13.0	7.0	1.0	0.0

Optimize user productivity by automatically, providing details on the user's experience, enabling faster issue detection and resolution

Monitoring examples:

- Endpoint performance – CPU, memory, Wi-Fi
- Network performance – endpoint to Secure Access
- Top SaaS applications performance
- Collaboration performance monitoring
- User specific events

Decrease mean time to resolution using experience insights



Step 1

Experience Insights raises an alert. The transit ISP is experiencing an outage.

Step 2

Help desk ticket is raised

Step 3

Issue is routed to NOC

Step 4

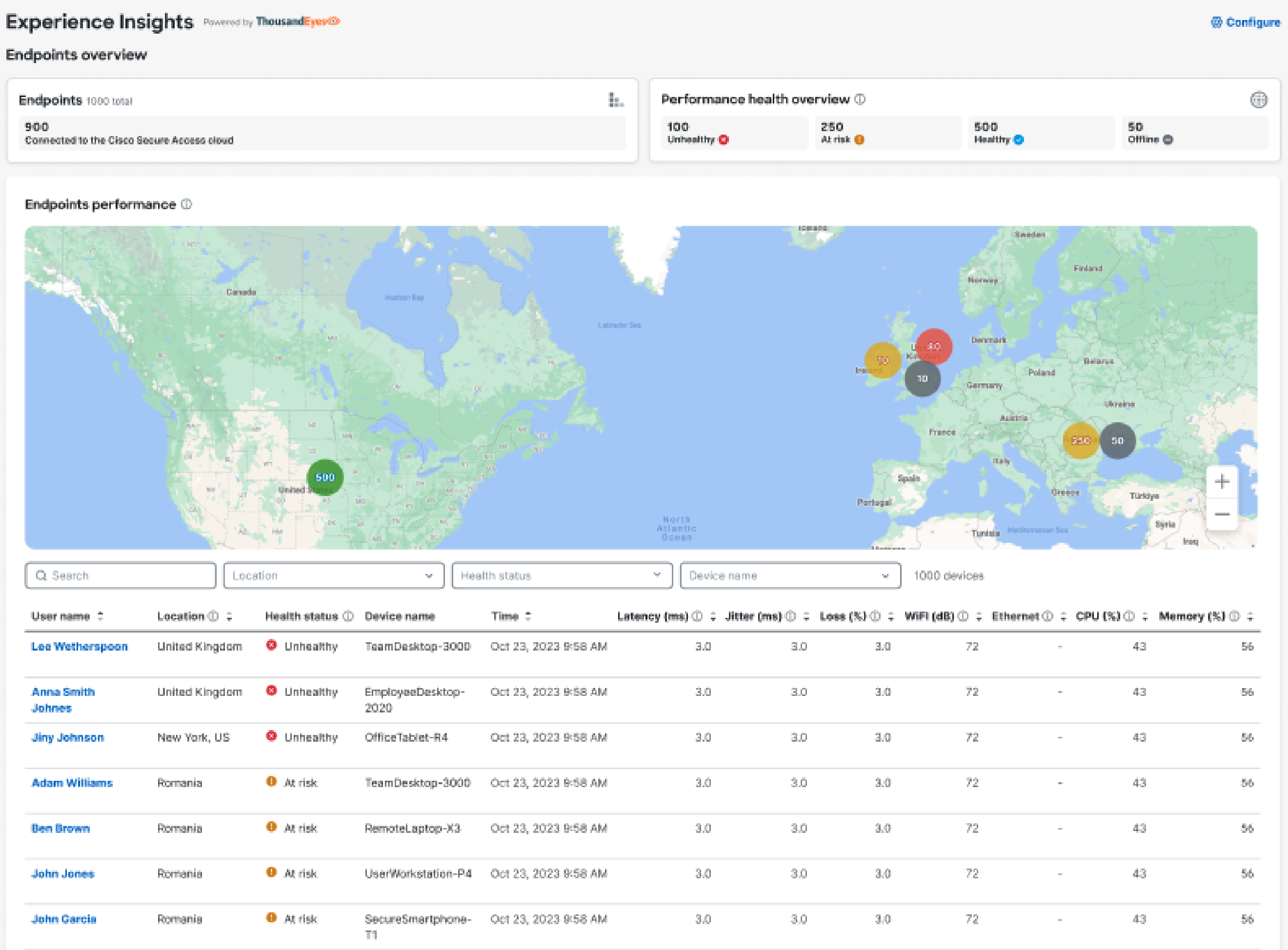
NOC investigates each hop in the path

Step 5

NOC never identifies root cause because it lies within the transit ISP, where they no visibility. Instead, they struggle with performance degradation until it is resolved by an outside party.

Single dashboard experience

Monitor user digital experience without separate agents or management portals



Experience Insights Powered by ThousandEyes

Configure

Endpoints overview

Endpoints 1000 total

900
Connected to the Cisco Secure Access cloud

Performance health overview

100	250	500	50
Unhealthy	At risk	Healthy	Offline

Endpoints performance

Search | Location | Health status | Device name | 1000 devices

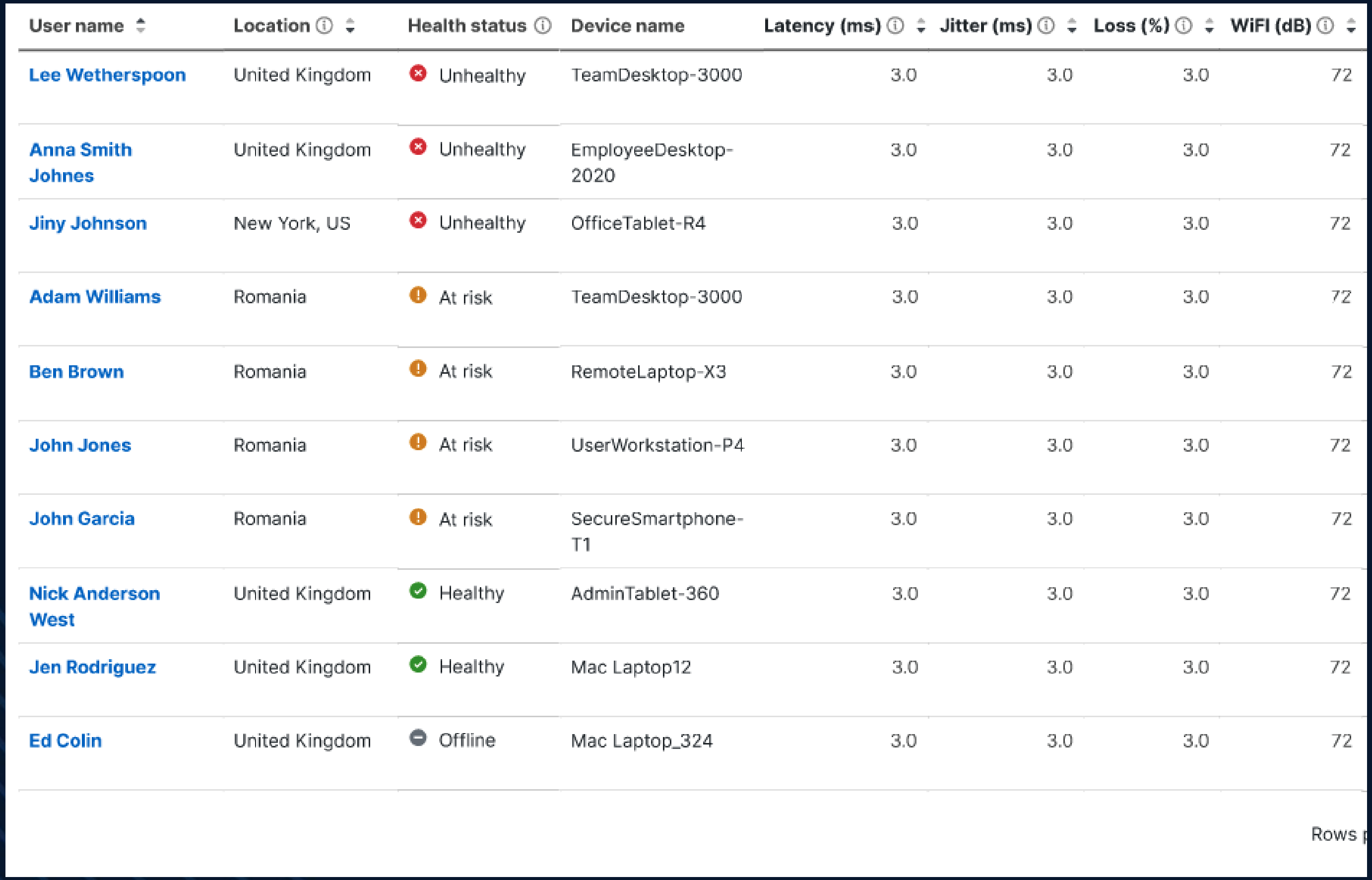
User name	Location	Health status	Device name	Time	Latency (ms)	Jitter (ms)	Loss (%)	WiFi (dB)	Ethernet	CPU (%)	Memory (%)
Lee Wetherspoon	United Kingdom	Unhealthy	TeamDesktop-3000	Oct 23, 2023 9:58 AM	3.0	3.0	3.0	72	-	43	56
Anna Smith Johnes	United Kingdom	Unhealthy	EmployeeDesktop-2020	Oct 23, 2023 9:58 AM	3.0	3.0	3.0	72	-	43	56
Jiny Johnson	New York, US	Unhealthy	OfficeTablet-R4	Oct 23, 2023 9:58 AM	3.0	3.0	3.0	72	-	43	56
Adam Williams	Romania	At risk	TeamDesktop-3000	Oct 23, 2023 9:58 AM	3.0	3.0	3.0	72	-	43	56
Ben Brown	Romania	At risk	RemoteLaptop-X3	Oct 23, 2023 9:58 AM	3.0	3.0	3.0	72	-	43	56
John Jones	Romania	At risk	UserWorkstation-P4	Oct 23, 2023 9:58 AM	3.0	3.0	3.0	72	-	43	56
John Garcia	Romania	At risk	SecureSmartphone-T1	Oct 23, 2023 9:58 AM	3.0	3.0	3.0	72	-	43	56

Experience Insights…

- Can identify disruptions in numerous third-party applications
- Is part of the Cisco Secure Access dashboard
- Includes ThousandEyes Embedded Endpoint Agent as a module in Cisco Secure Client

See every endpoint, regardless of location

Gain a complete view of the user experience, even for remote and hybrid workers



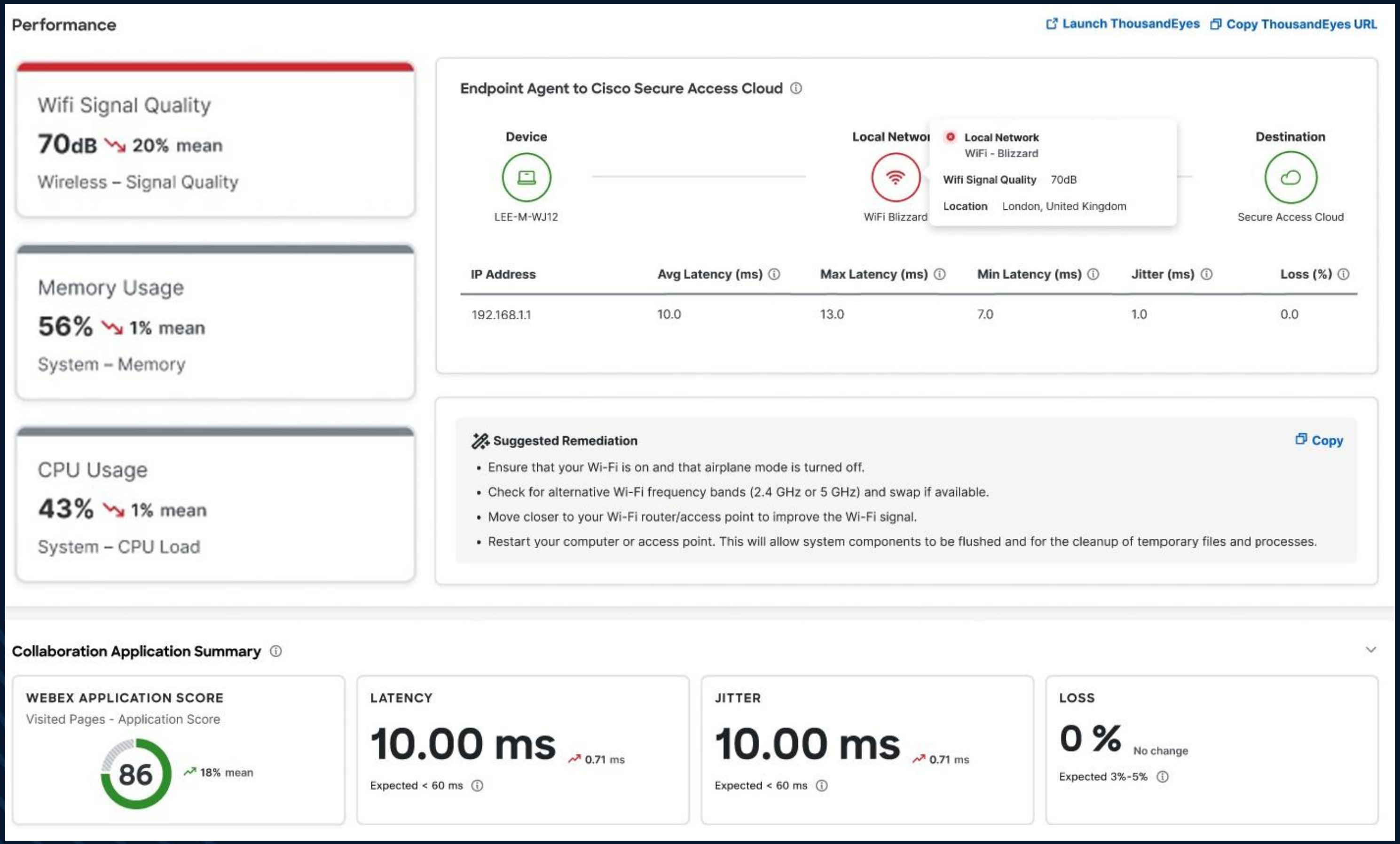
User name	Location	Health status	Device name	Latency (ms)	Jitter (ms)	Loss (%)	WiFI (dB)
Lee Wetherspoon	United Kingdom	Unhealthy	TeamDesktop-3000	3.0	3.0	3.0	72
Anna Smith Johnes	United Kingdom	Unhealthy	EmployeeDesktop-2020	3.0	3.0	3.0	72
Jiny Johnson	New York, US	Unhealthy	OfficeTablet-R4	3.0	3.0	3.0	72
Adam Williams	Romania	At risk	TeamDesktop-3000	3.0	3.0	3.0	72
Ben Brown	Romania	At risk	RemoteLaptop-X3	3.0	3.0	3.0	72
John Jones	Romania	At risk	UserWorkstation-P4	3.0	3.0	3.0	72
John Garcia	Romania	At risk	SecureSmartphone-T1	3.0	3.0	3.0	72
Nick Anderson West	United Kingdom	Healthy	AdminTablet-360	3.0	3.0	3.0	72
Jen Rodriguez	United Kingdom	Healthy	Mac Laptop12	3.0	3.0	3.0	72
Ed Colin	United Kingdom	Offline	Mac Laptop_324	3.0	3.0	3.0	72

Rows

- Pervasive visibility into every endpoint
- Identify disruptions quicker
- Diagnose root cause faster

Simplify troubleshooting

Consolidated view of network and security events to make troubleshooting easier



Performance

Launch ThousandEyes | Copy ThousandEyes URL

Wifi Signal Quality
70dB ↘ 20% mean
Wireless – Signal Quality

Memory Usage
56% ↘ 1% mean
System – Memory

CPU Usage
43% ↘ 1% mean
System – CPU Load

Endpoint Agent to Cisco Secure Access Cloud ⓘ

Local Network
WiFi - Blizzard
Wifi Signal Quality 70dB
Location London, United Kingdom

IP Address	Avg Latency (ms) ⓘ	Max Latency (ms) ⓘ	Min Latency (ms) ⓘ	Jitter (ms) ⓘ	Loss (%) ⓘ
192.168.1.1	10.0	13.0	7.0	1.0	0.0

Suggested Remediation | Copy

- Ensure that your Wi-Fi is on and that airplane mode is turned off.
- Check for alternative Wi-Fi frequency bands (2.4 GHz or 5 GHz) and swap if available.
- Move closer to your Wi-Fi router/access point to improve the Wi-Fi signal.
- Restart your computer or access point. This will allow system components to be flushed and for the cleanup of temporary files and processes.

Collaboration Application Summary ⓘ

WEBEX APPLICATION SCORE
Visited Pages - Application Score
86 ↗ 18% mean

LATENCY
10.00 ms ↗ 0.71 ms
Expected < 60 ms ⓘ

JITTER
10.00 ms ↗ 0.71 ms
Expected < 60 ms ⓘ

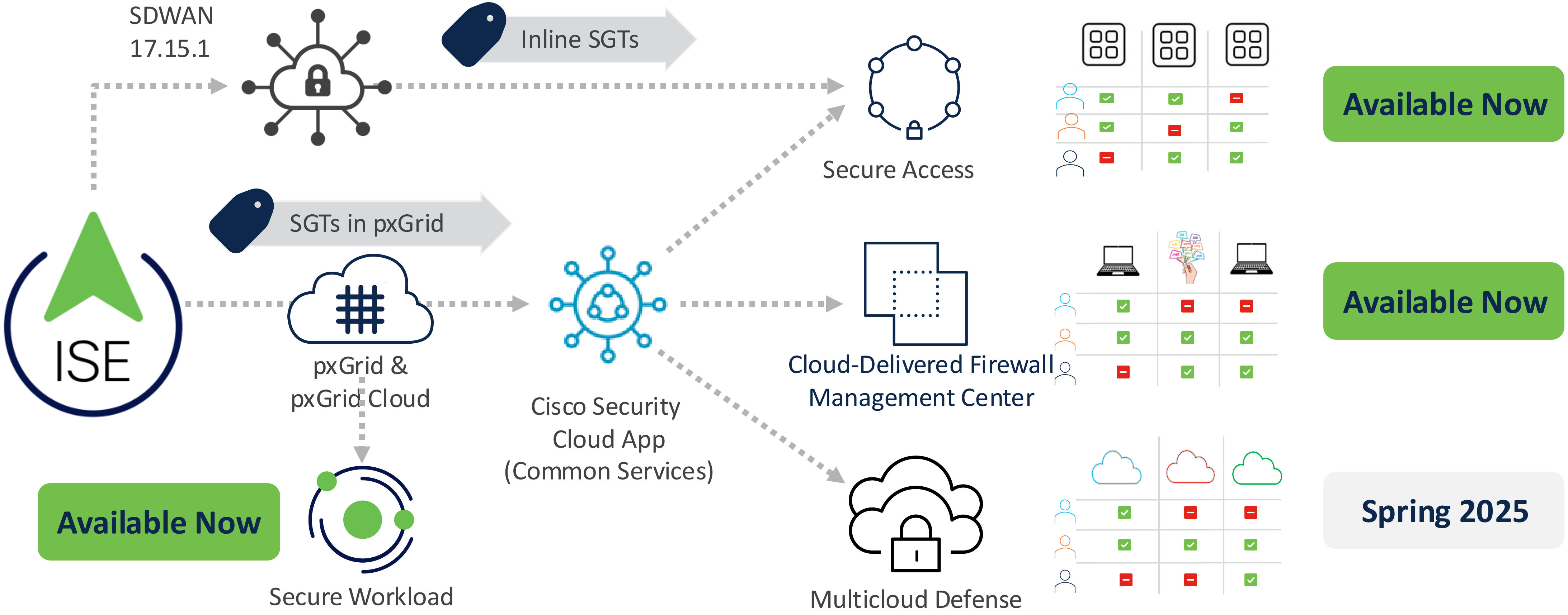
LOSS
0 % No change
Expected 3%-5% ⓘ

Reduce Mean Time to Resolution

- Understand global workforce experience
- Pinpoint issues from user to application
- Share insights across multiple domains (IT, security, help desk)

Putting it all together

ISE and Cisco Security Cloud Services



✓	✓	🟥
✓	🟥	✓
🟥	✓	✓

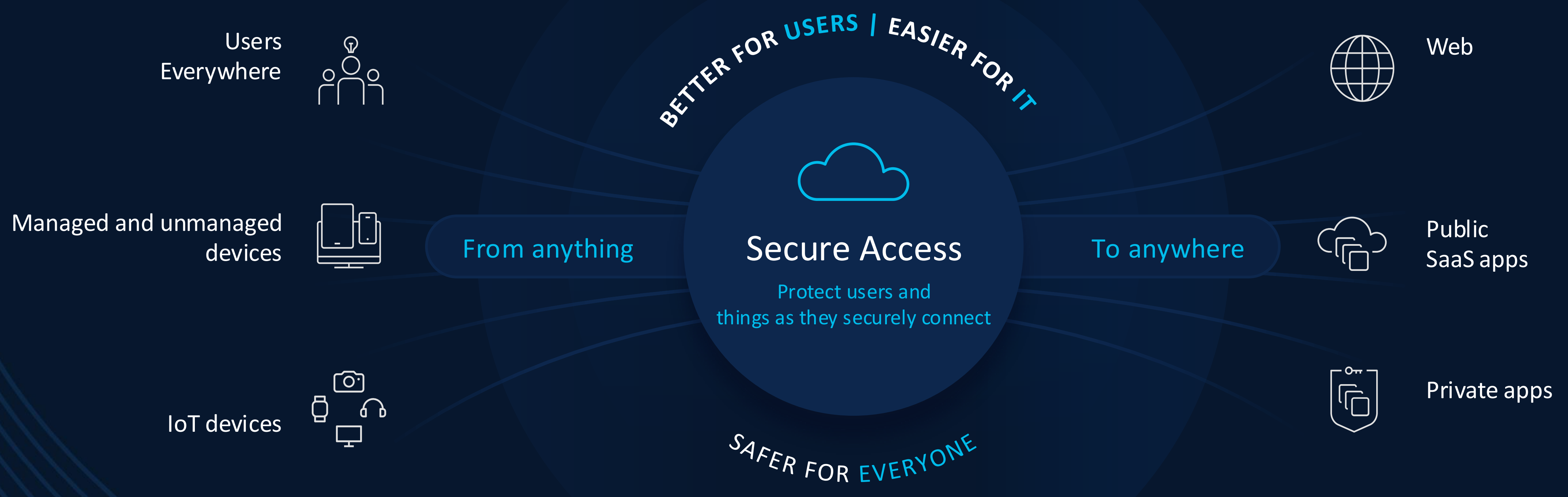
✓	🟥	🟥
✓	✓	✓
🟥	✓	✓

✓	🟥	🟥
✓	✓	✓
🟥	🟥	✓

Security Group Tags (SGTs) are the common language used across campus, remote, cloud, and firewall policies

Modernize your defense with Cisco Secure Access

Converged cloud-native security grounded in zero trust



Users Everywhere

Managed and unmanaged devices

IoT devices

From anything

Secure Access

Protect users and things as they securely connect

To anywhere

Web

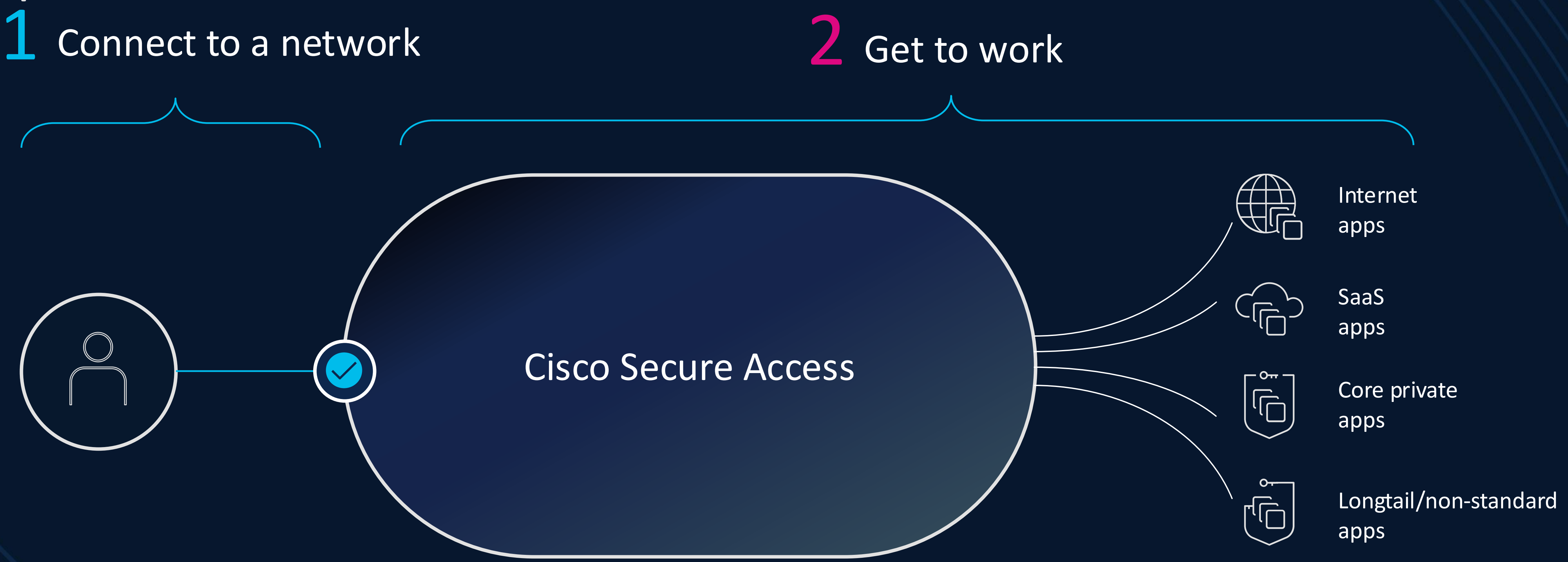
Public SaaS apps

Private apps

BETTER FOR USERS | EASIER FOR IT

SAFER FOR EVERYONE

Cisco Secure Access: Simple, frictionless user experience



Note: Supports both client and clientless ZTNA connectivity cisco