

Evolve your Zero Trust Architecture: A Case Study with Cisco IT

Lessons learned from Cisco's SSE Deployment

Sanjeet Sharma
IT Security Architect

CISCO Live !

Cisco Webex App

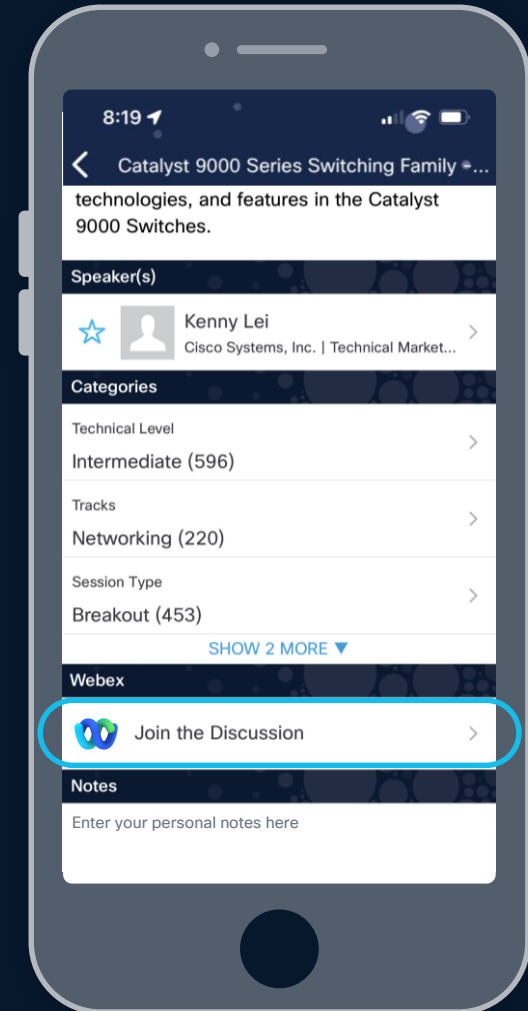
Questions?

Use Cisco Webex App to chat with the speaker after the session

How

- 1 Find this session in the Cisco Live Mobile App
- 2 Click “Join the Discussion”
- 3 Install the Webex App or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until June 13, 2025.



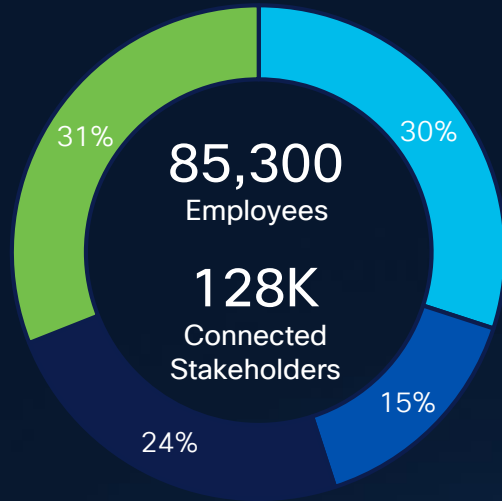
Agenda



- 01 Cisco IT at a glance
- 02 Business Landscape
- 03 Remote Access with VPNaaS
- 04 Zero Trust with Duo Network Gateway
- 05 Technical Deep Dive: ZTA
- 06 Practical Guidance for Organizations

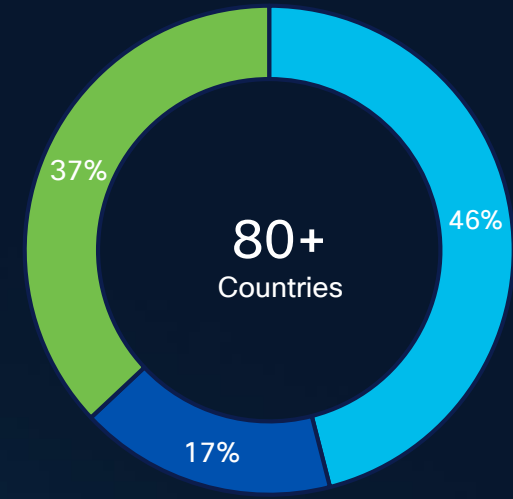
Cisco at a Glance

Employee Distribution



● Engineering ● Sales & Marketing ● Customer Experience ● Corporate Functions

Global Cisco Distribution



● Americas ● EMEA ● APJC



5,663
Routers



7,633
LAN Switches



11,164
Unified Computing
System Servers



33.5B
DNS Requests
per Day



27,684
Cisco Video Devices



71,096
Virtual Machines



61,483
Mobile Devices



130PB
Overall Usable Storage



1.52M
Webex Meetings per
Month



17.7M
DNS Threat Requests
Blocked per Day

Security Challenge Inside Cisco



8 Trillion

SIEM Events / Day
across Network
(Splunk)



50 Billion

Netflows Analyzed /
Day (Cisco Secure
Network Analytics)



47 TB

Internet Traffic
Inspected



33.5 Billion

DNS Requests / Day



2.3 Million

E-mails received / Day
(Cisco Secure Email)



12 Million

Intrusion Alerts / Day
(NGIPS)

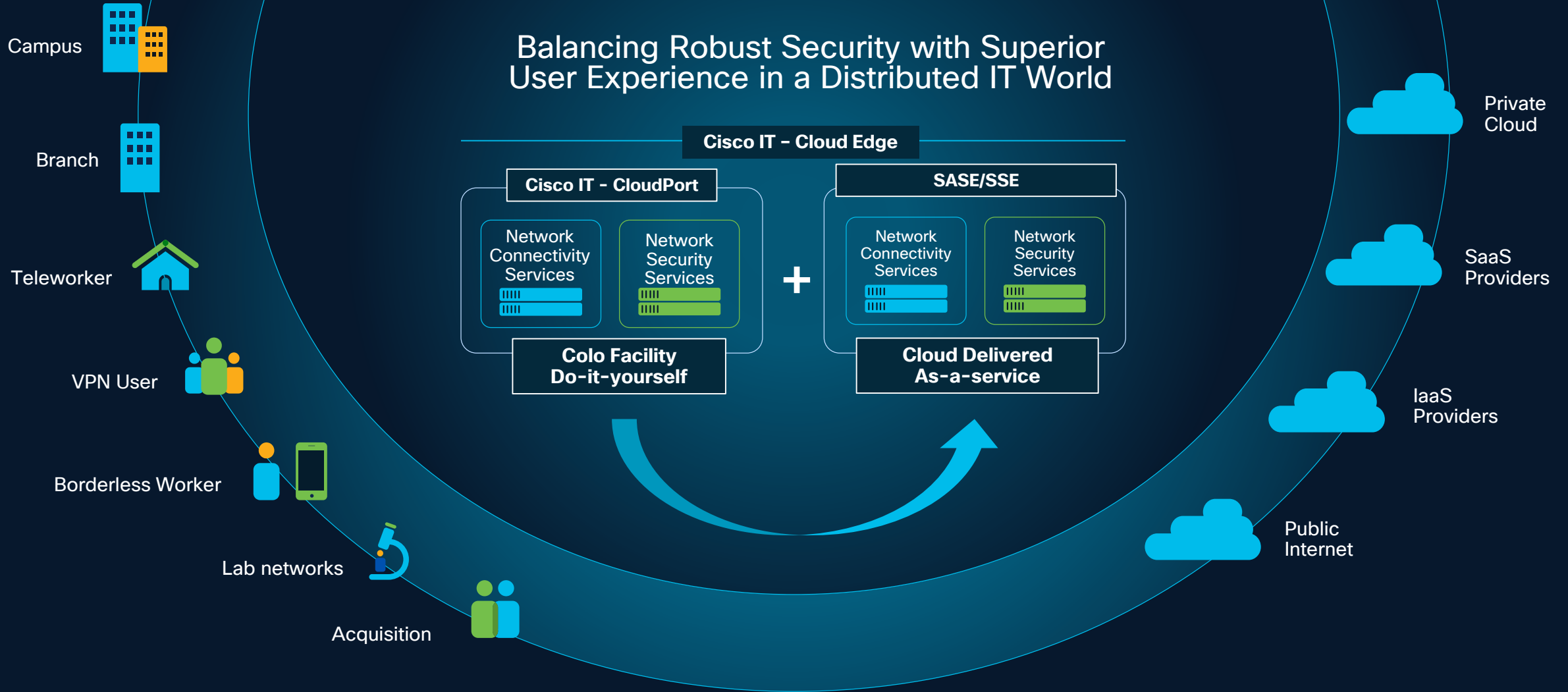


Balancing IT Priorities



Navigating the Tightrope










Balancing Robust Security with Superior User Experience in a Distributed IT World



Cisco IT- CloudPort

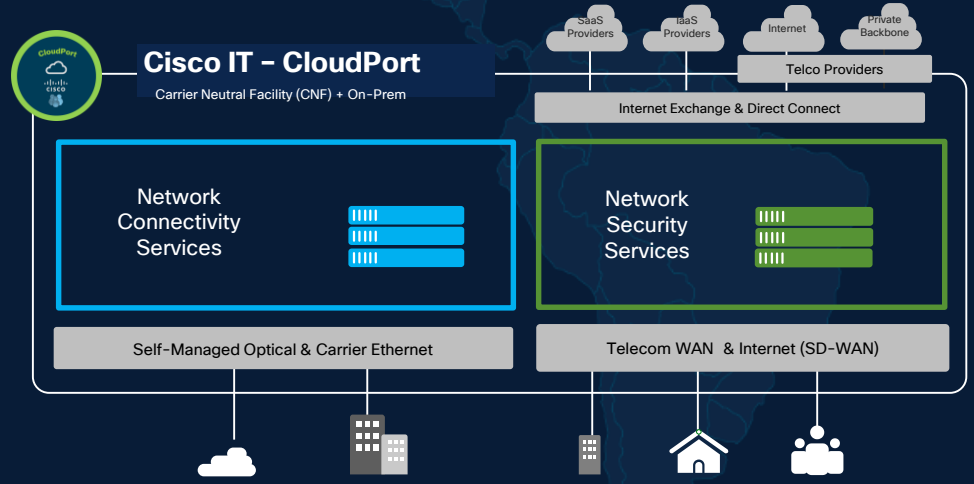
A single tenant "SASE"

Legend

-  Cisco IT CloudPort
-  Regional WAN HUB
-  100G - Ethernet
-  10G - Ethernet
-  1G - Ethernet
-  Microsoft Azure
-  Amazon Web Services
-  Google Cloud Platform
-  Cisco Private Cloud / DC



The growing trend of Public Cloud and Hybrid Work is inspiring us to strategically enhance our investment in SASE/SSE while maintaining the critical role of Cisco IT CloudPort.



Evolving to Zero Trust

Zero Trust is
a mindset



Organizations should adopt a holistic zero trust approach to prevent user friction

Cisco IT Principles

Consistent user experience regardless of location

Independent of underlying network

Continuous validation of identity and trust

Identity and policy for users, devices and things

Least privilege access and micro-segmentation

Remote Workers

Office Workers

Devices & Things

VPN as a Service

Cisco Secure Access (SSE)

- 01 Cisco IT at a glance
- 02 Business Landscape
- 03 VPN as a Service
- 04 Zero Trust with Duo Network Gateway
- 05 Technical Deep Dive: ZTA
- 06 Practical Guidance for Organizations

Migration Strategy

Refresh Opportunity 6,500 Users

Cisco IT aggressively adopted Cisco Secure Access for a differentiated access VPN service to address and End of Hardware support situation

30-day migration target

Phase 1	Give users the option
Phase 2	Make SSE the default, but allow opt-out
Phase 3	SSE is the only option

Employee VPN Cisco Workforce

Cisco IT took a more prudent approach to migrate the entire workforce giving people a way out in the very early stages

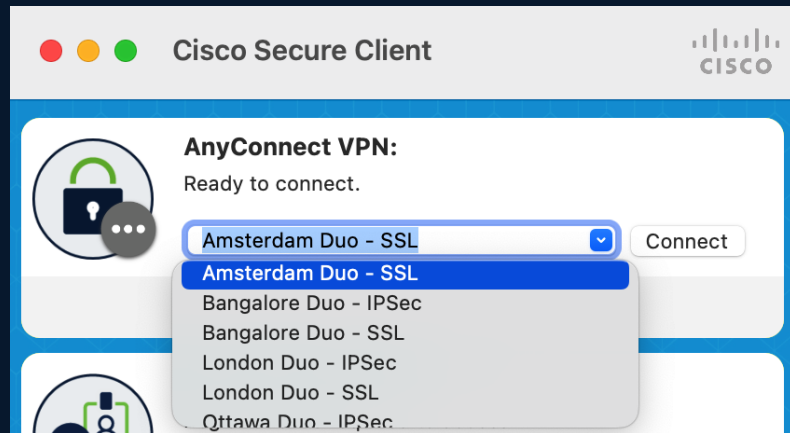
6-Month migration target

Phase 1	10K Users* 1. Give users the option 2. SSE is the only option
Phase 2	Workforce 1. Give users the option 2. SSE is the default with limited Opt-Out 3. SSE is the only option

(*) Eating our own dogfood = Make SSE the default for the people building the product

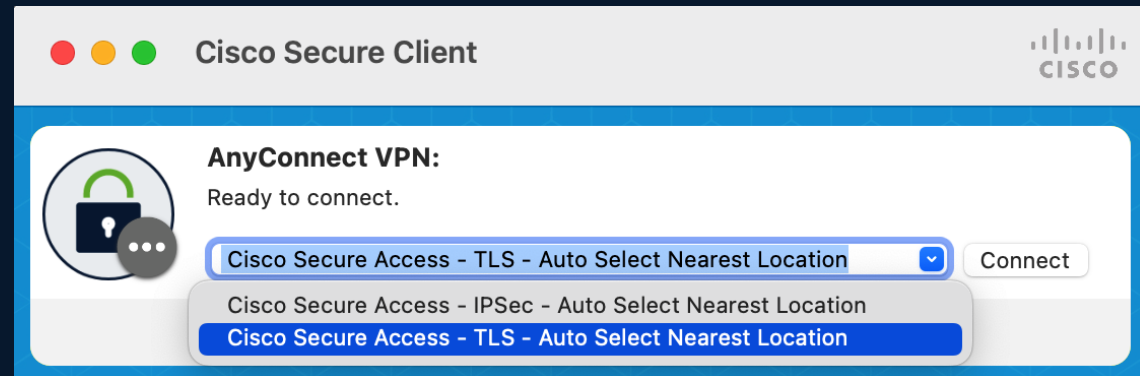
User Experience

Before



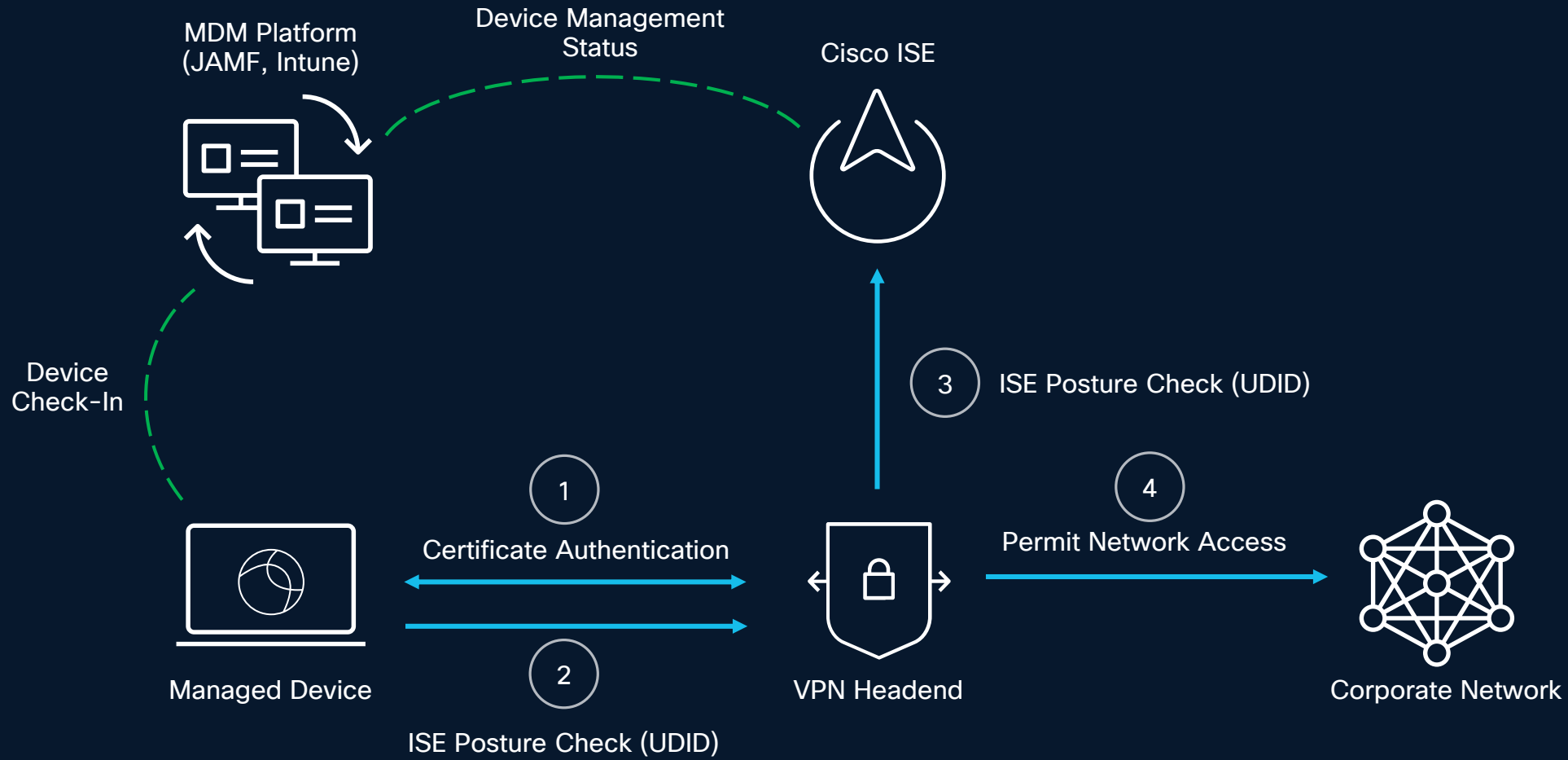
Users had to manually select one of the options from the dropdown. Many users connected to sub-optimal locations and blame VPN for poor performance.

After

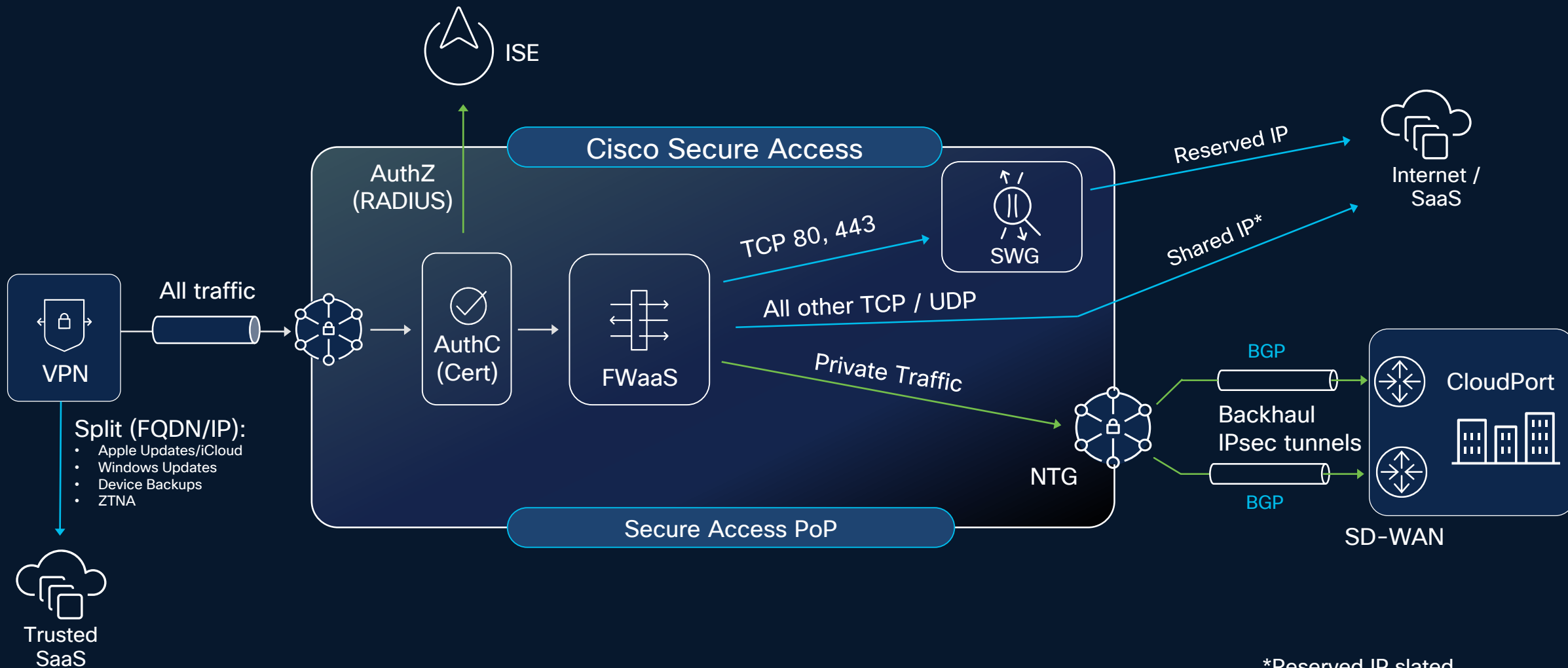


Cisco IT made the decision to only expose 2 options which both connect users to the nearest location. The regional profiles will be made available for users that need it through self-service on the client machine.

VPN Posture Checks



VPN Full Traffic Flow

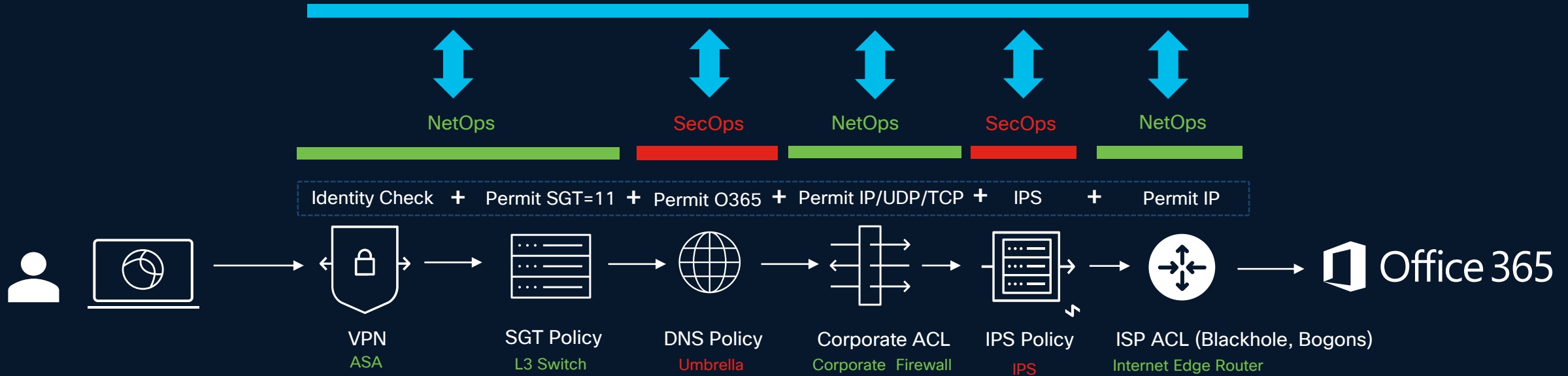


*Reserved IP slated for Q4FY25

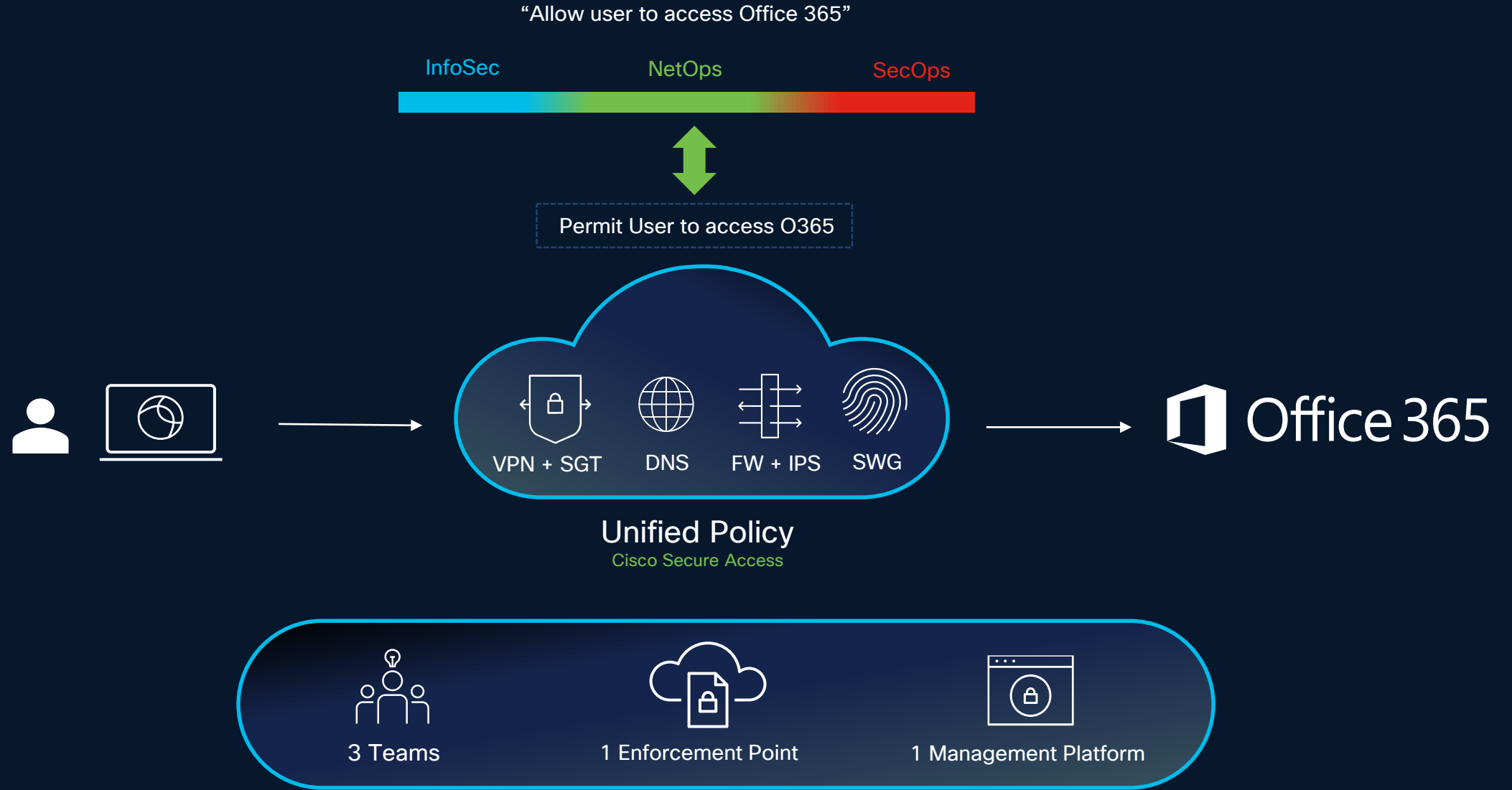
Policy in the Enterprise Network

“Allow user to access Office 365”

InfoSec Architecture



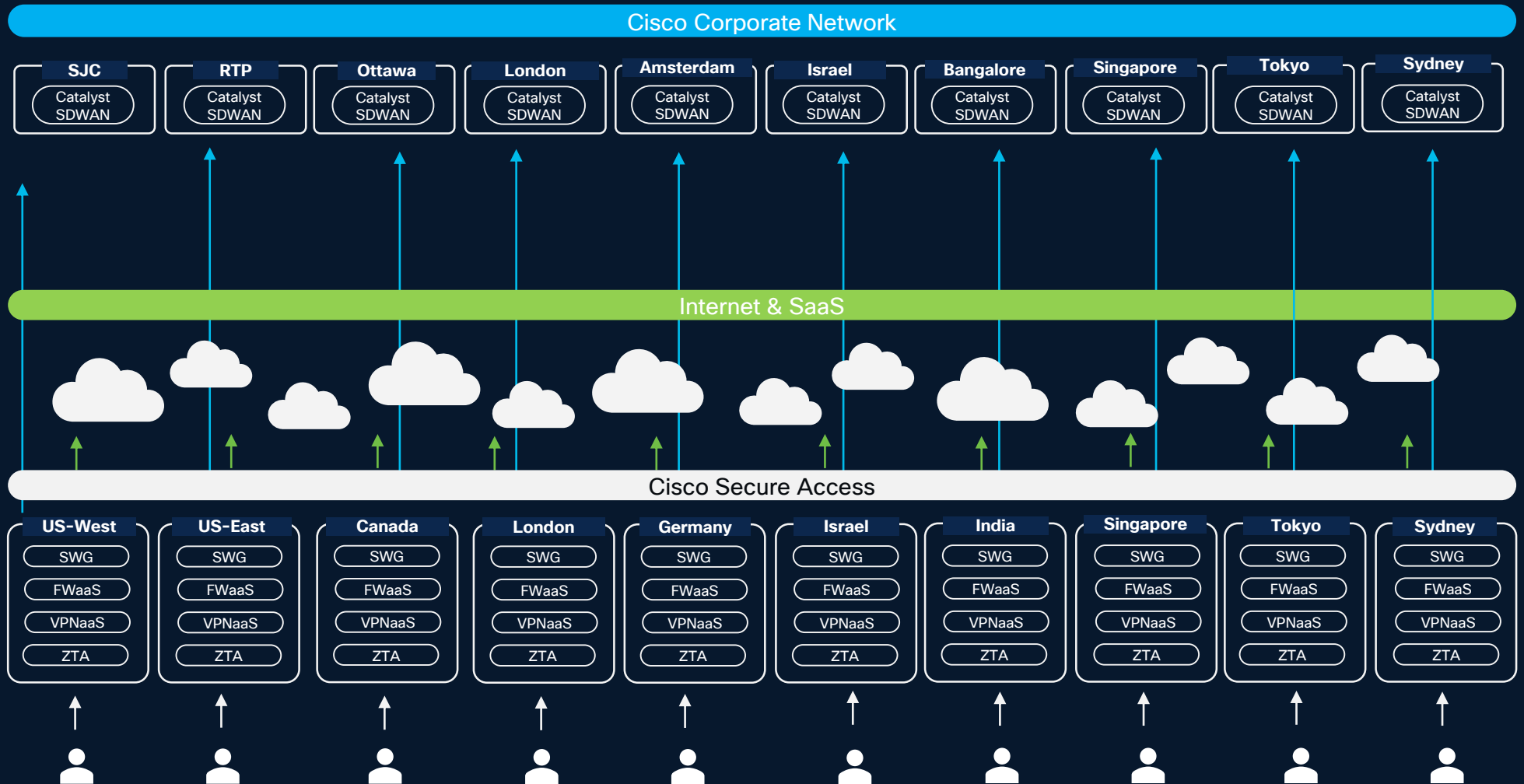
Policy in SSE



Global Architecture Overview

VPN Enablement

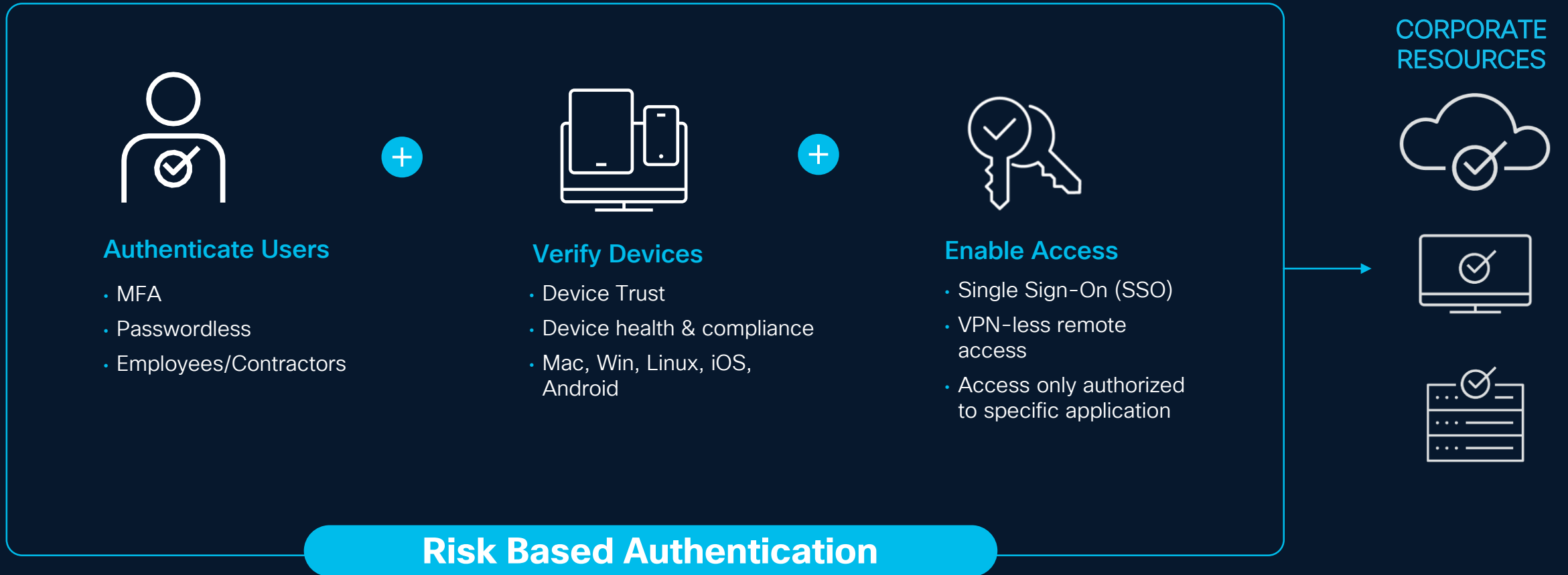
- 10 VPN Regions in strategic locations worldwide with the option to add many more in the future
- Each region has resilient and scalable connectivity to the Cisco enterprise
- Certificate-Based Authentication with RADIUS Authorization (ISE)
- Reserved IP for Secure Internet Access
- Significantly simplified security policy due to established trust and improved observability.
- Simplified IT operations by not having to manage boxes ease of troubleshooting.



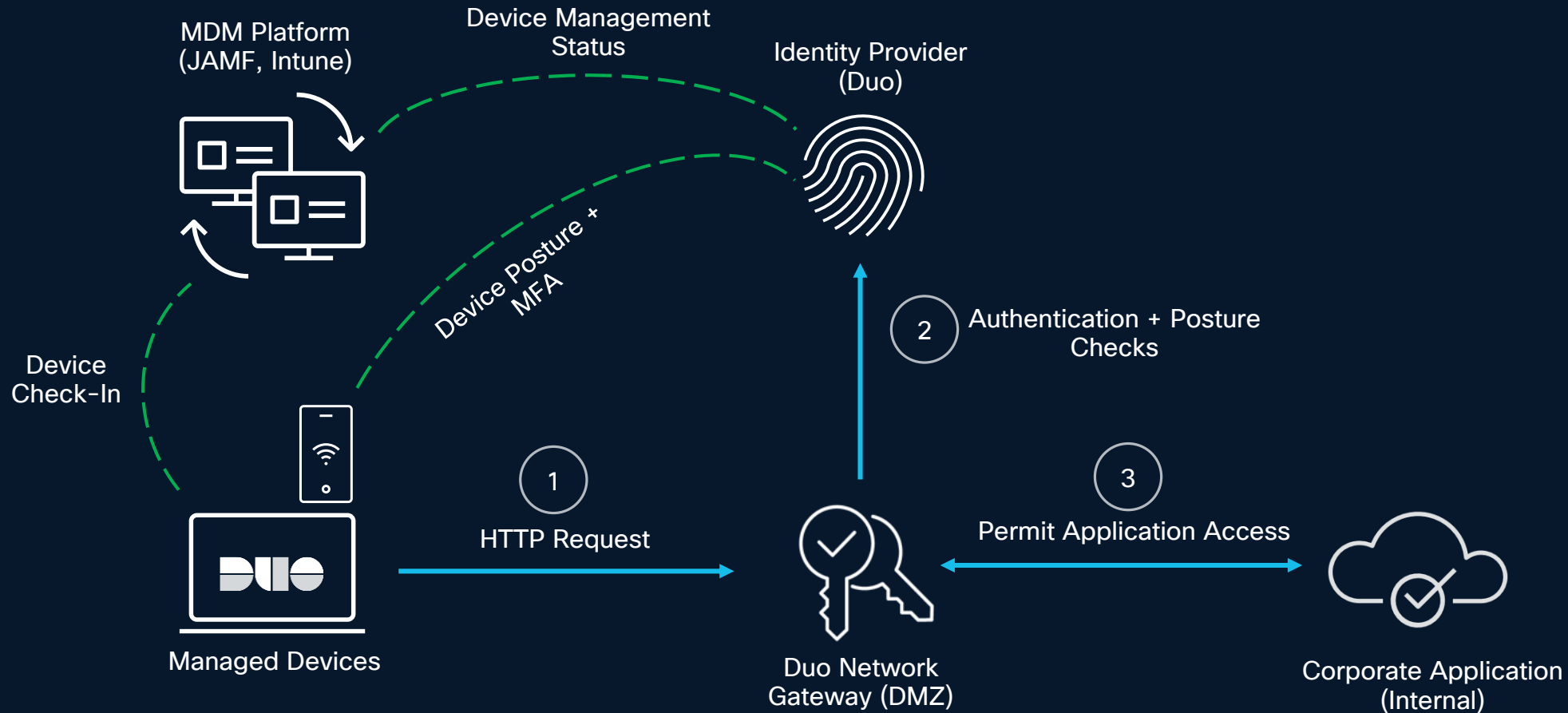
Zero Trust Access with the Duo Network Gateway

- 01 Cisco IT at a glance
- 02 Business Landscape
- 03 VPN as a Service
- 04 Zero Trust with Duo Network Gateway
- 05 Technical Deep Dive: ZTA
- 06 Practical Guidance for Organizations

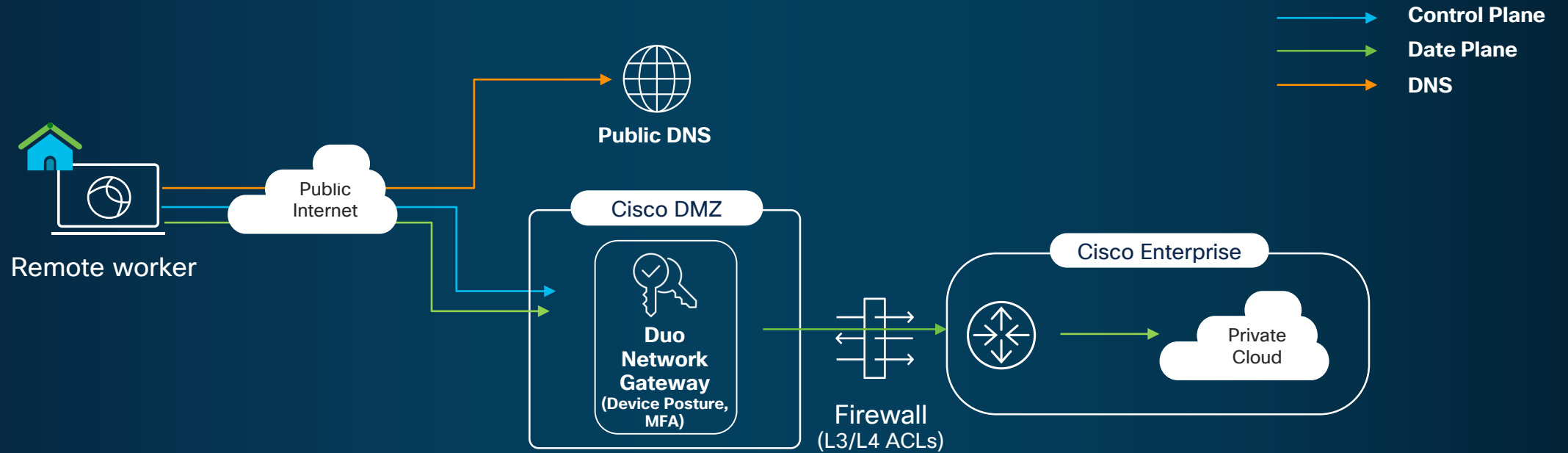
Per-App Access with Duo



Control Plane Architecture



Data Plane Architecture



Cisco's Duo Deployment



Managed Devices

Deployed Device Configs to over
170K Endpoints (Mobile/Desktop)



Applications Available

Borderless access for 150+
Applications



User Authentications

420K user authentications daily

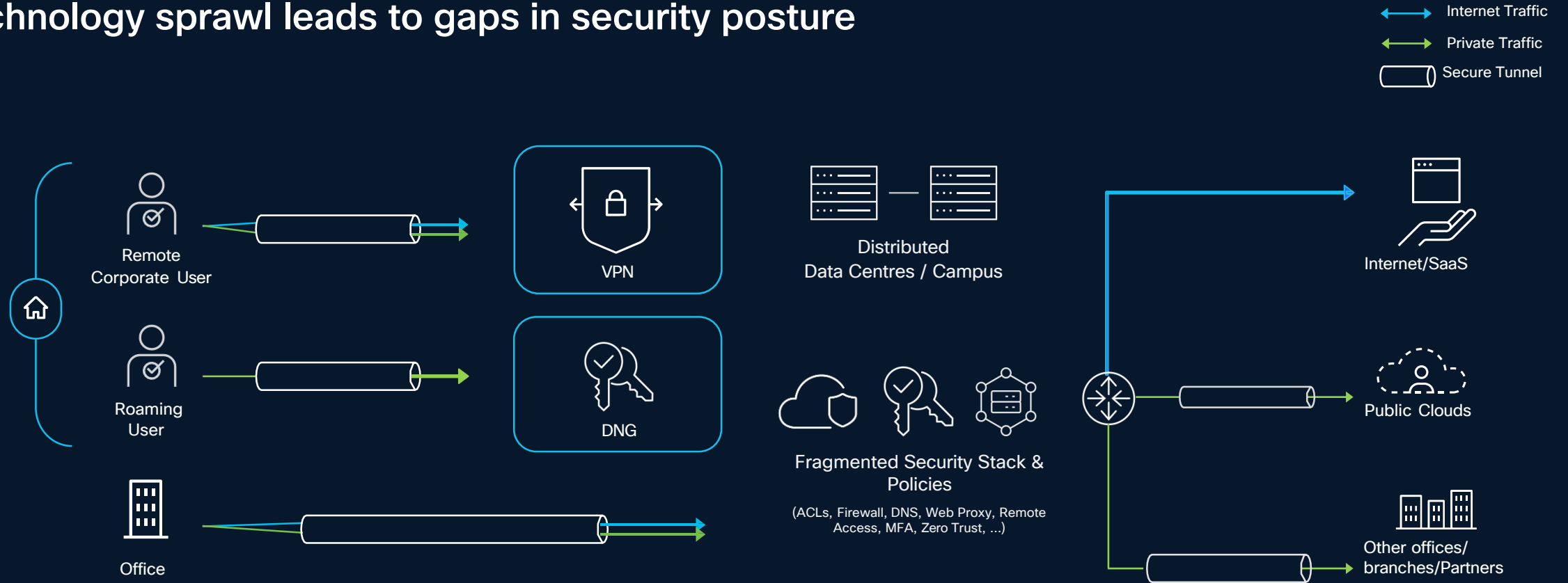


Borderless Access

Borderless access for Mac,
Windows, Linux, Android and iOS
devices

Challenge

Technology sprawl leads to gaps in security posture

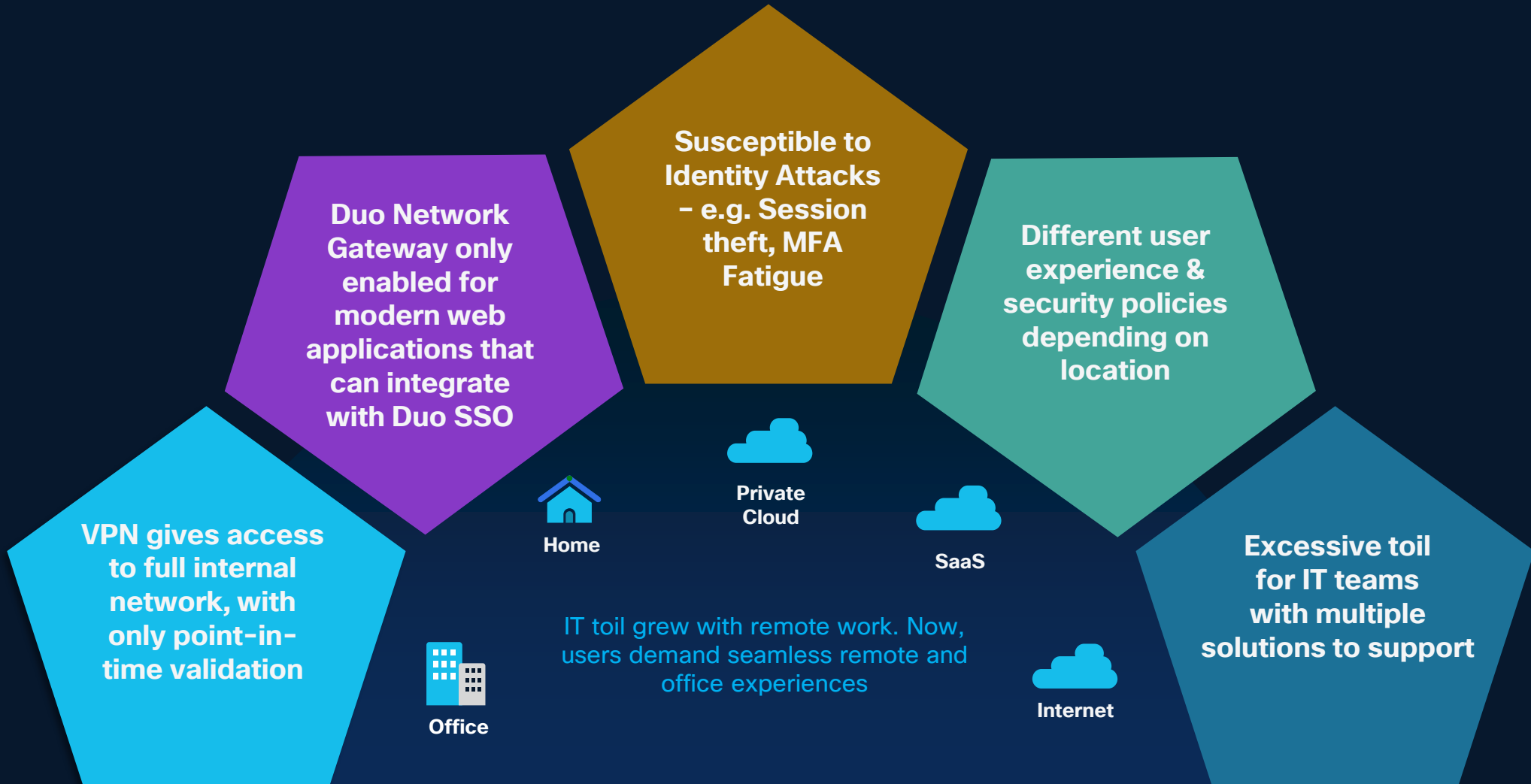


Poor user experience
Lower productivity

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

Gaps in security posture born out of
complexity and fragmentation

Hybrid Access Challenges



Evolving the Zero Trust Architecture

with Cisco Secure Access

- 01 Cisco IT at a glance
- 02 Business Landscape
- 03 VPN as a Service
- 04 Zero Trust with Duo Network Gateway
- 05 Technical Deep Dive: ZTA
- 06 Practical Guidance for Organizations



Access Approach in Cisco IT

There are 3 main security checks for accessing application resources today



User + Device Identity

For granular role-based access control



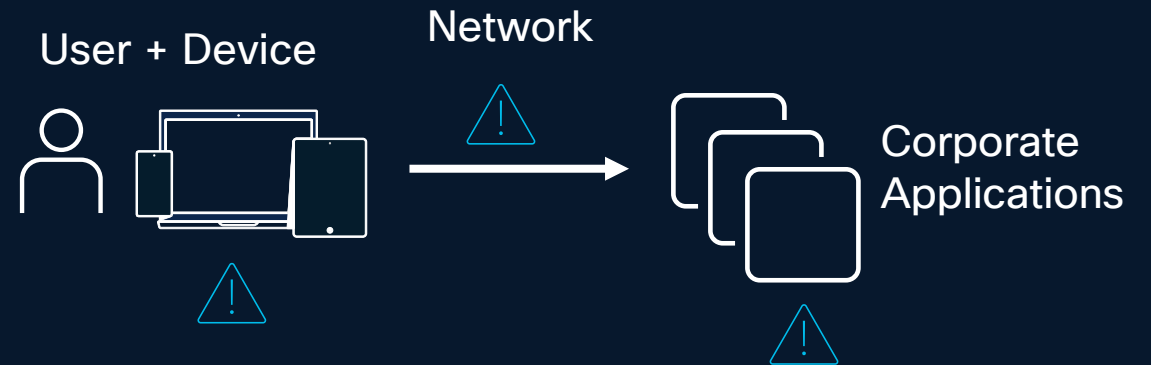
Validation of Management

Ensure endpoint is actively managed by IT via a check against the Device Management Suite



Lightweight Posture Check

Device attributes, e.g. Minimum OS, Disk Encryption, Security Agent

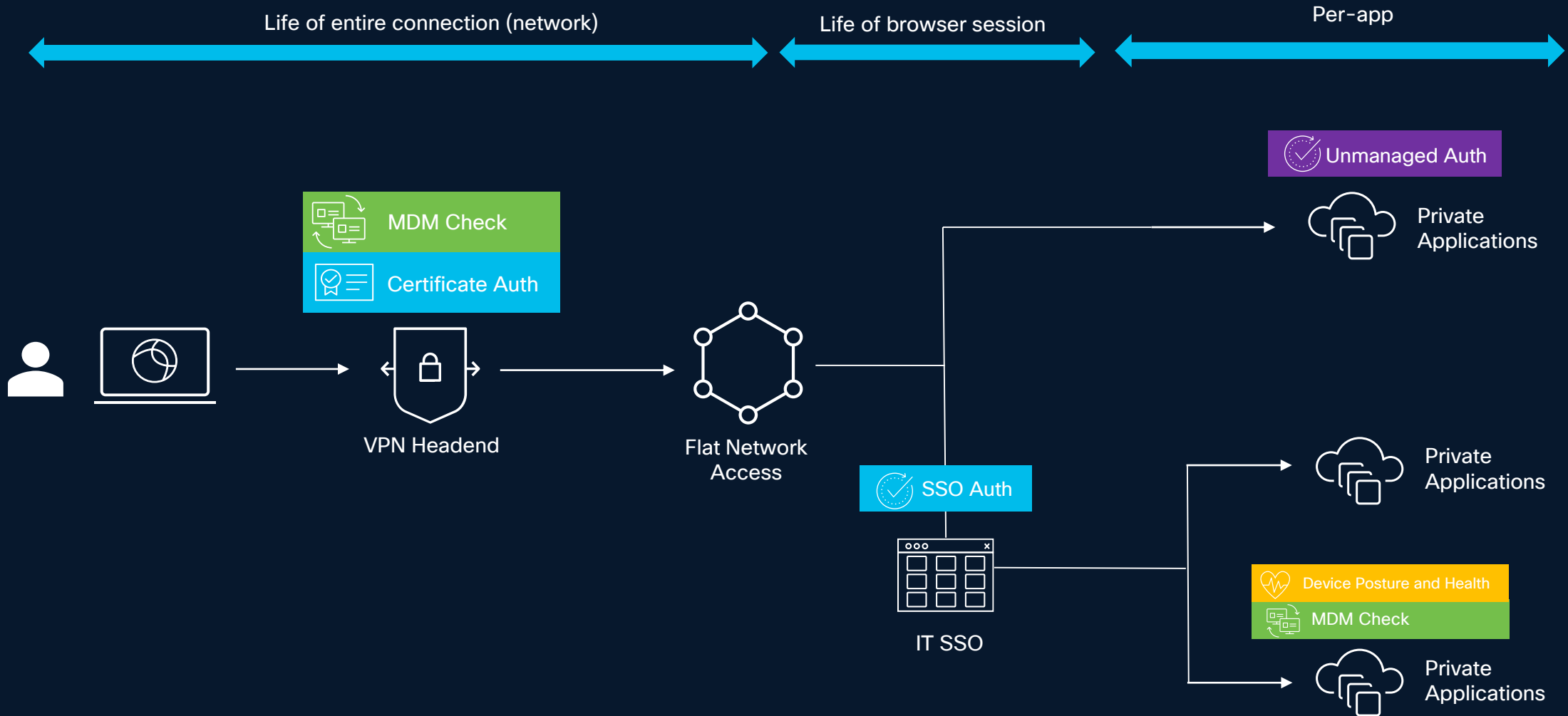


These checks are done at various stages of the connection. The goal is to have all 3 checks for any application access attempt.

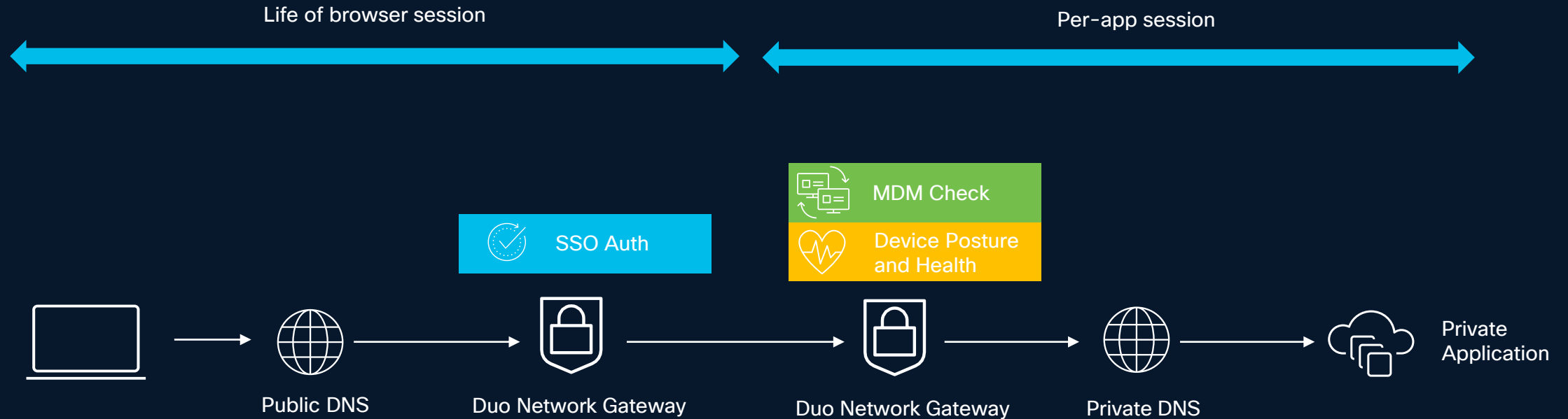


Zero Trust Philosophy is to continually validate these attributes at smaller intervals

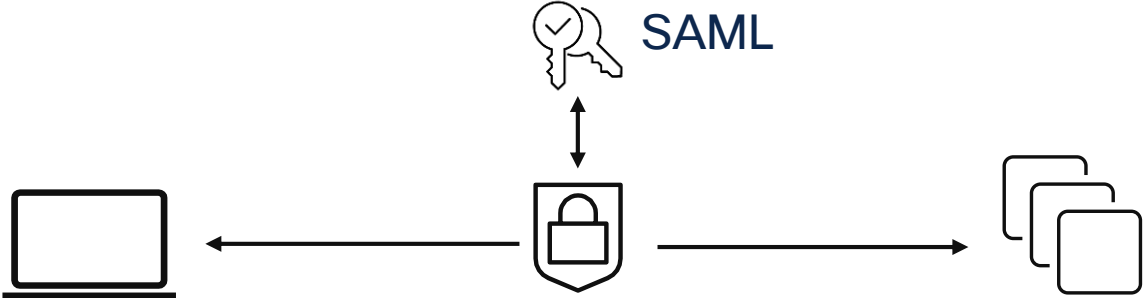
Application Access with VPN



Application Access with Duo Network Gateway



Duo Network Gateway



The DNG is a layer 7 reverse proxy – it only proxies some types of traffic, and inserts itself into the SAML Authentication layer to validate management status and device posture.

VS

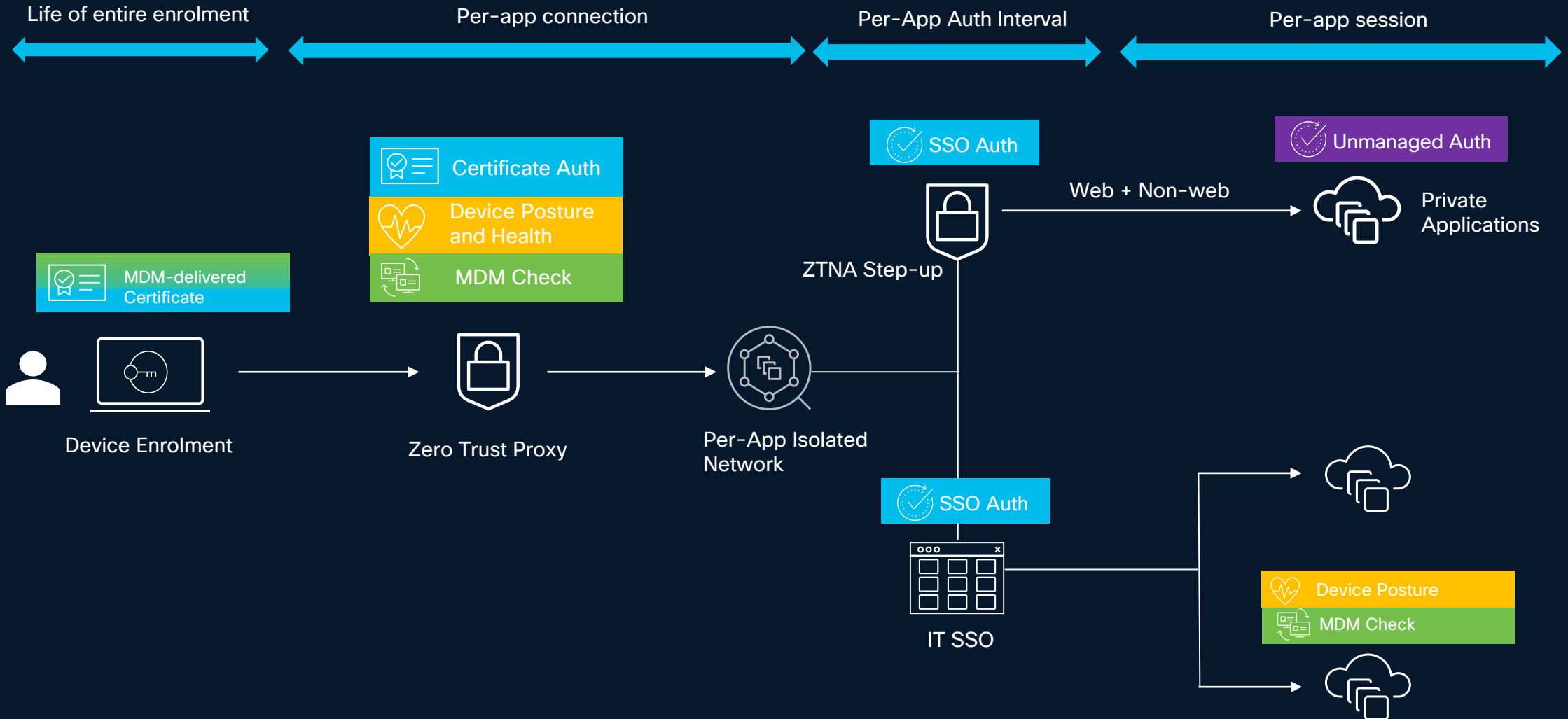
Cisco Secure Access (ZTNA)



Therefore, ZTNA is **not** a 1:1 replacement of DNG, but an evolution

ZTNA is a layer 3 forward proxy – it proxies TCP and UDP sockets to validate device identity and posture. The application still runs its own authentication.

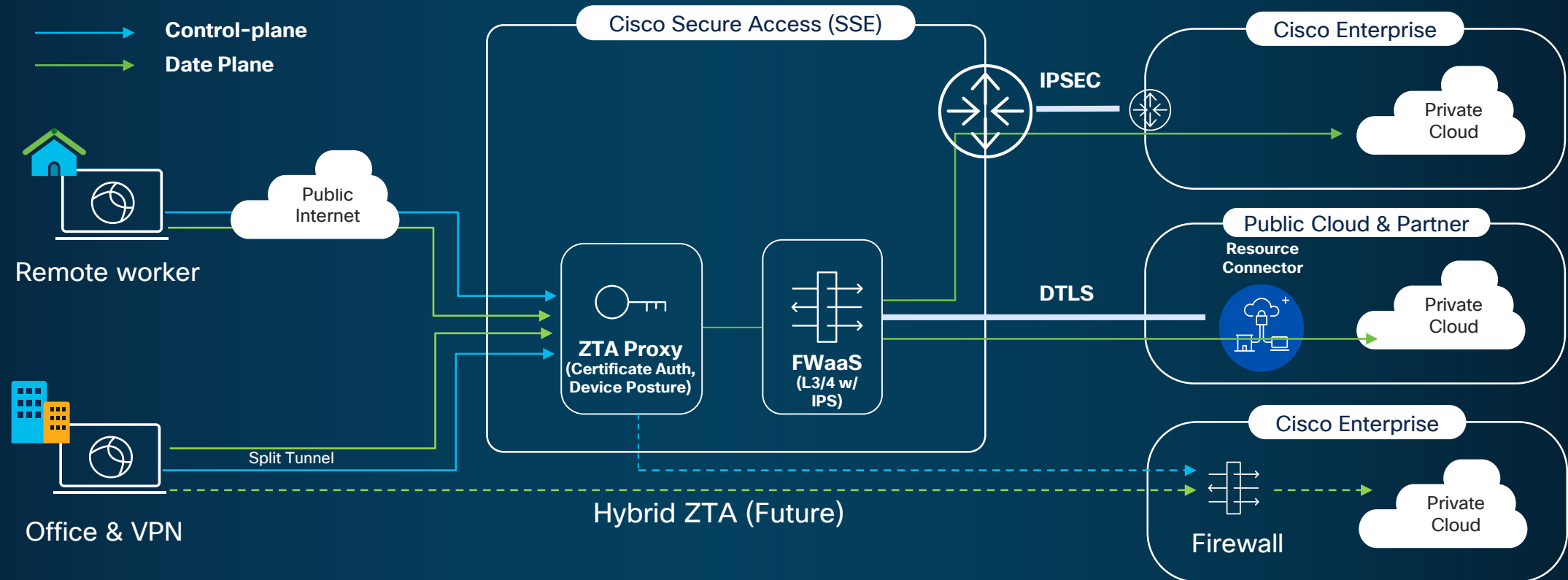
Application Access with ZTA



Architecture Overview



Cisco Secure Client
Zero Trust Access



Differentiators



TPM-Bound Keys

TPM is a hardware enclave that protects private keys. This secures ZTA clients against session/certificate hijacking (Windows, Mac, iOS, Android)



Backwards Compatible

Onboarding apps to SSE does not affect existing VPN or DNG access, allowing for seamless migration. Apps can be gradually onboarding to an increased user base, and any failures allow fallback to the underlying network (VPN/Public).



Secure Network

Instead of authorizing the whole application/browser session, SSE posture checks are evaluated separately for each TCP/UDP socket, providing a much more robust and secure zero trust framework. No exposure to public internet, or even internal IPs.

Cisco Secure Access Policy Creation

Cisco IT - ZTNA Posture Requirements

Client-based

Applied criteria

Operating system

- Windows, Latest version (Updated dynamically) allowed
- Android, 14.0.0 and latest version allowed only on Knox enabled Samsung devices
- iOS, Latest version (Updated dynamically) allowed
- Mac OS X, 13.6.5, 13.6.4... [Show more](#)

Firewall

- Require firewall to be running on the endpoint
- Require firewall to be running on the endpoint

Endpoint security agent

- Require an endpoint security agent to be running on the endpoint
- Allowed endpoint security agents: [Show more](#)
- Require an endpoint security agent to be running on the endpoint
- Allowed endpoint security agents: [Show more](#)

System password

- Require system password for the endpoint
- Require system password for the endpoint

Disk encryption

- Require Any disk encryption product on the endpoint
- Require Any disk encryption product on the endpoint

Associated rules

Rule Name
ZTNA-C - Trusted Applications
ZTNA-C - Untrusted Applications - Step Up Required

[View more in Policy](#)

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](#)

[Cisco Secure Client](#) [Manage DNS Servers \(5\)](#)

Zero Trust | Virtual Private Network | Internet Security

Enrollment methods

Before users can access resources using client-based Zero Trust Access, their endpoint devices must be enrolled. Manage enrollment methods for your organization here. [Help](#)

Windows and macOS devices enroll using: **SSO Authentication** | **Certificates**

Android and iOS devices enroll using SSO Authentication only.

Traffic Steering

Use traffic steering to configure your traffic to either go through Zero Trust or bypass it. [Help](#)

[Destination](#)

[command-center.cisco.com](#)

[Add Destination](#)

Private Resource | **Modified**

[Command Center](#) | Automatically on Nov 28, 2024

Rule name

ZTNA-C - Trusted Applications

Rule order: 9

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.

[CED-SecureAccess-MVP](#)

To
Specify one or more destinations.

[Cisco Trusted Applications](#)

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: **Cisco IT - ZTNA Posture Requirements** | Requirements: **Operating System, Firewall, Endpoint security agent, System password** + 1 More

Private Resources: **Cisco Trusted Applications** 3

Detailed App Utilization Discovery

App Discovery read-only
Download CSV

[Back to Dashboard](#)

FILTERS

LABEL Unreviewed ✕

Filter by Identity

Label Select All

Unreviewed (27131)

Approved (0)

Not Approved (0)

Under Audit (0)

Controllable Apps

All Controllable Apps

Advanced Controls

Risk Select All

Very High

High

Medium

Low

Very Low

Category Select All

Ad Publishing

Anonymizer

Application Development and Testing

Application Protocol

Backup & Recovery

Business Intelligence

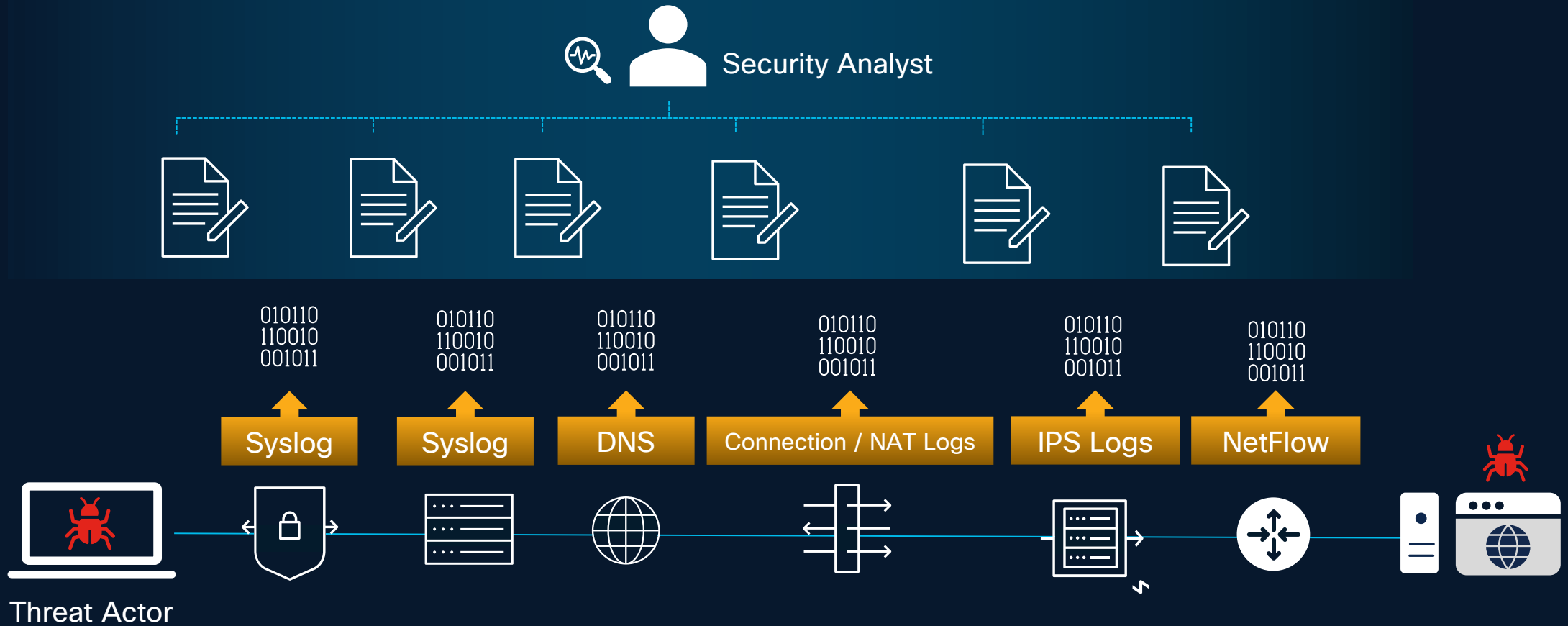
Cloud Broker

27131 Total Applications ⚙️

Application	Risk Score	Identities	DNS Requests	Total Web Traffic	Firewall Events	Blocked F	Label
YouTube Media	Low	106598	1,173,686,184	191.7 TB total traffic 191.6 TB 127.5 ...	104,073,543		Unreviewed Control this app ⚠️
Webex Teams Collaboration	Medium	145972	8,481,276,199	68.5 TB total traffic 67.0 TB 1.5 TB	623,506,857		Unreviewed Control this app ⚠️
Akamai Intelligent Edge Platform Content Delivery Network	Low	92471	20,136,139,065	44.4 TB total traffic 44.4 TB 13.7 GB	6,750,042		Unreviewed Control this app ⚠️
NETFLIX Media	Medium	11424	94,691,523	17.3 TB total traffic 17.3 TB 11.3 GB	9,174,112		Unreviewed Control this app ⚠️
Facebook Social Networking	Medium	96027	617,197,551	17.2 TB total traffic 17.1 TB 42.5 GB	34,749,362		Unreviewed Control this app ⚠️

Security Analysis in Enterprise Network

Disparate Data Sources, Complex Correlation



Unified Activity Logging

All logging is now centralized, eliminating the need for building tooling to do attribution across products.

Security investigators can easily see who accessed what, when, how, and identify any concerns.



Integrate with other data sources to write proactive security plays

DNS Security

Event Details [X]

Action
● Allowed

Time
Feb 5, 2025 10:28 AM

Rule Name
[For all Internet access](#)

Source
[Redacted]

Rule Identity
[Redacted]

Internal IP Address
[Redacted]

External IP Address
[Redacted]

Destination
[play.google.com](#)

Categories
Ecommerce/Shopping, Movies, Software/Technology, Computers and Internet
[Dispute Categorization](#)

Resource/Application
Google Play Store

Application Category
Software Repository

DNS Type
NS

Firewall

Event Details [X]

Action
● Allowed

Time
Feb 5, 2025 11:27 AM

Rule Name
[SIA - AD Users to Internet \(223770\)](#)

Source
[Redacted]
Cisco_Employee (SGT-10)

Source IP
[Redacted]

Destination IP
[Redacted]

Source Port
28853

Destination Port
443

Categories
Computers and Internet
[Dispute Categorization](#)

Resource/Application
Google Play

Application Category
Software Repository

File Status (Disposition)
-

File Transfer Direction
C2S

Identified Threat
-

Malware Analysis Defended

Web Security

Event Details [X]

Action
● Allowed

Time
Feb 5, 2025 11:27 AM

Rule Name
[SIA - AD Users to Internet](#)

Source
[Redacted]
CED-SecureAccess-MVP
Cisco_Employee (SGT-10)

Rule Identity
[CED-SecureAccess-MVP](#)

Internal IP Address
-

External IP Address
[Redacted]

Destination
[https://play.google.com](#)

Hostname
[play.google.com](#)

Categories
Software/Technology, Computers and Internet
[Dispute Categorization](#)

Resource/Application
Google Play Store

Application Category
Software Repository

Egress IP Address
151.186.181.29 (Reserved)

Egress Data Center
London, GB

Zero Trust Access

Event Details [X]

Connection Method
ZTNA Client-based

Time
Feb 4, 2025 10:04 PM

Action
Allowed

Access details

Identity
[Redacted]

Resource/Application
Tableau

Destination
[Redacted]

Destination IP
[Redacted]

Destination Port
443

Resource Connector Group
-

Ingress Region
US (East)

Tunnel Type
HTTP2

Transaction ID
c3a90176-6914-4d94-88d7-8367832fda20

Cisco IT Value Cases

Better Security



- Uplift from VPN to an isolated network per app, with strong identity
- Can secure unmanaged apps without needing intervention from app owner
- Continuous validation with better logging/visibility

Secure the Data Center – only the ZTA proxy has network access

User Experience



- Allow users access to wider range of apps without the need for VPN
- Better performance due to cloud availability and no HTTP redirects
- No difference in experience whether on 'trusted' network or not.

Onboard most – not some – applications onto ZTA

IT Operations

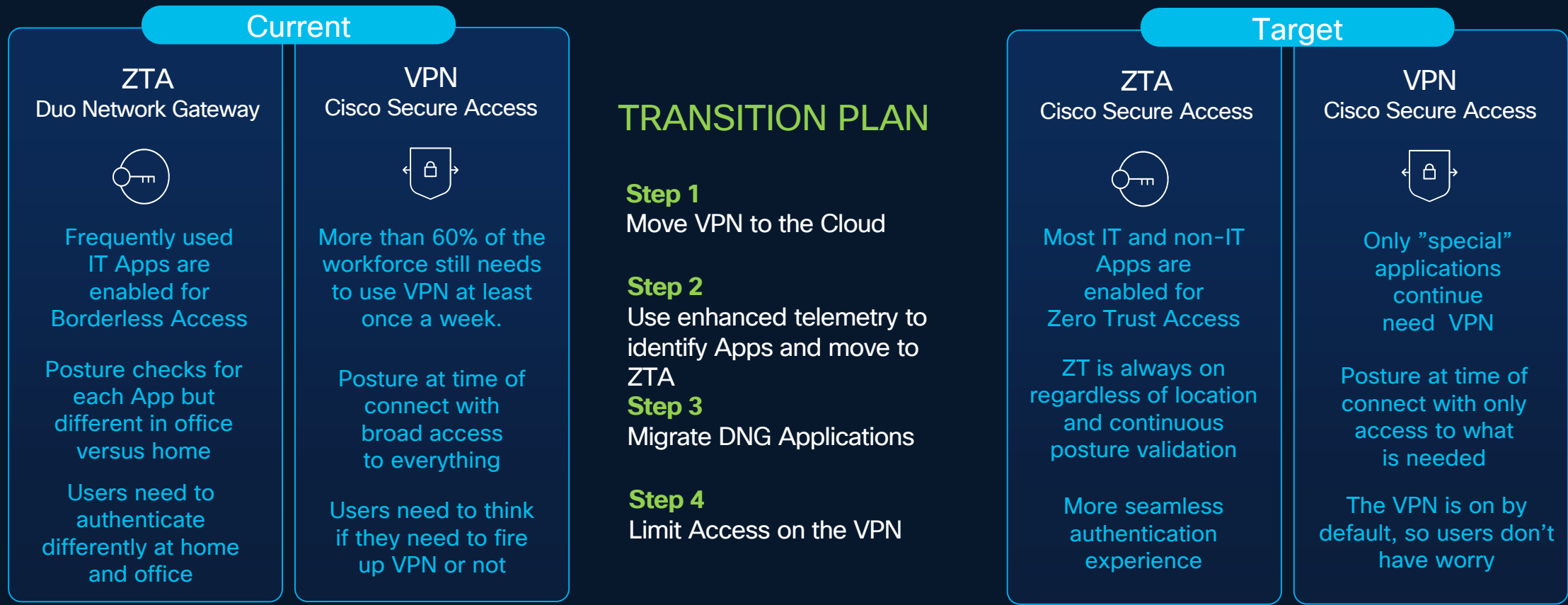


- Simplified network design compared to DNG
- No separate policies for DNG vs internal Duo apps
- No lifecycle management of on-premises VMs

IT simplification by consuming as a cloud service

The North Star Vision

VPNs aren't vanishing, by Zero Trust Access is Stealing the Show



TRANSITION PLAN

- Step 1**
Move VPN to the Cloud
- Step 2**
Use enhanced telemetry to identify Apps and move to ZTA
- Step 3**
Migrate DNG Applications
- Step 4**
Limit Access on the VPN

Lessons Learned

Practical Guidance for Organizations

- 01 Cisco IT at a glance
- 02 Business Landscape
- 03 VPN as a Service
- 04 Zero Trust with Duo Network Gateway
- 05 Technical Deep Dive: ZTA
- 06 Practical Guidance for Organizations



Lessons Learned

01

Strategic Vision

Develop a company wide NorthStar vision and business outcomes

Before

Different teams try to adopt SSE in isolation to address their specific challenges

After

Teams work closely together to achieve maximum business value

02

Executive Sponsorship

Ensure strong, sustained leadership commitment and prioritization

Before

Operational work tends to be prioritized over forward-looking innovation

After

Stop managing On-Prem and IT wide prioritization of work and resources

Lessons Learned

03

Form a virtual team with representatives from all parts of IT and Security

Cisco's integrated platforms unite network and security products, fostering closer collaboration between IT and security teams

Device Experience

IT Helpdesk

Information Security

★ IT Design & UX

IT Communications

Security Operations

Identity & Access Management

Workplace

Network Operations



Lessons Learned

04

Speed vs. Risk

Balance innovation speed with willingness or need to take risk

Being Customer Zero does not mean we sacrifice on user experience and security. At the end of the day – the job of IT is enabling our users to perform their job.

Move fast when needed

Cisco enabled the IT workforce for VPN, accelerated by an end-of-life hardware situation

A more prudent approach where it matters

Cisco IT enabled applications for ZTA in phases

Risk assessment and mitigation

Cisco IT invested time in understanding and documenting risks, finding ways to mitigate them before moving to the next phase

Steering Committee Go / No-Go decision

We communicated the risks of moving forward and the business impact of slowing down up the leadership chain, ensuring that all decisions had visibility at the VP level

Complete your session evaluations



Complete a minimum of 4 session surveys and the Overall Event Survey to be entered in a drawing to win 1 of 5 full conference passes to Cisco Live 2026.



Earn 100 points per survey completed and compete on the Cisco Live Challenge leaderboard.



Level up and earn exclusive prizes!



Complete your surveys in the Cisco Live mobile app.

Continue your education



Visit the Cisco Showcase for related demos



Book your one-on-one Meet the Engineer meeting



Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs



Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

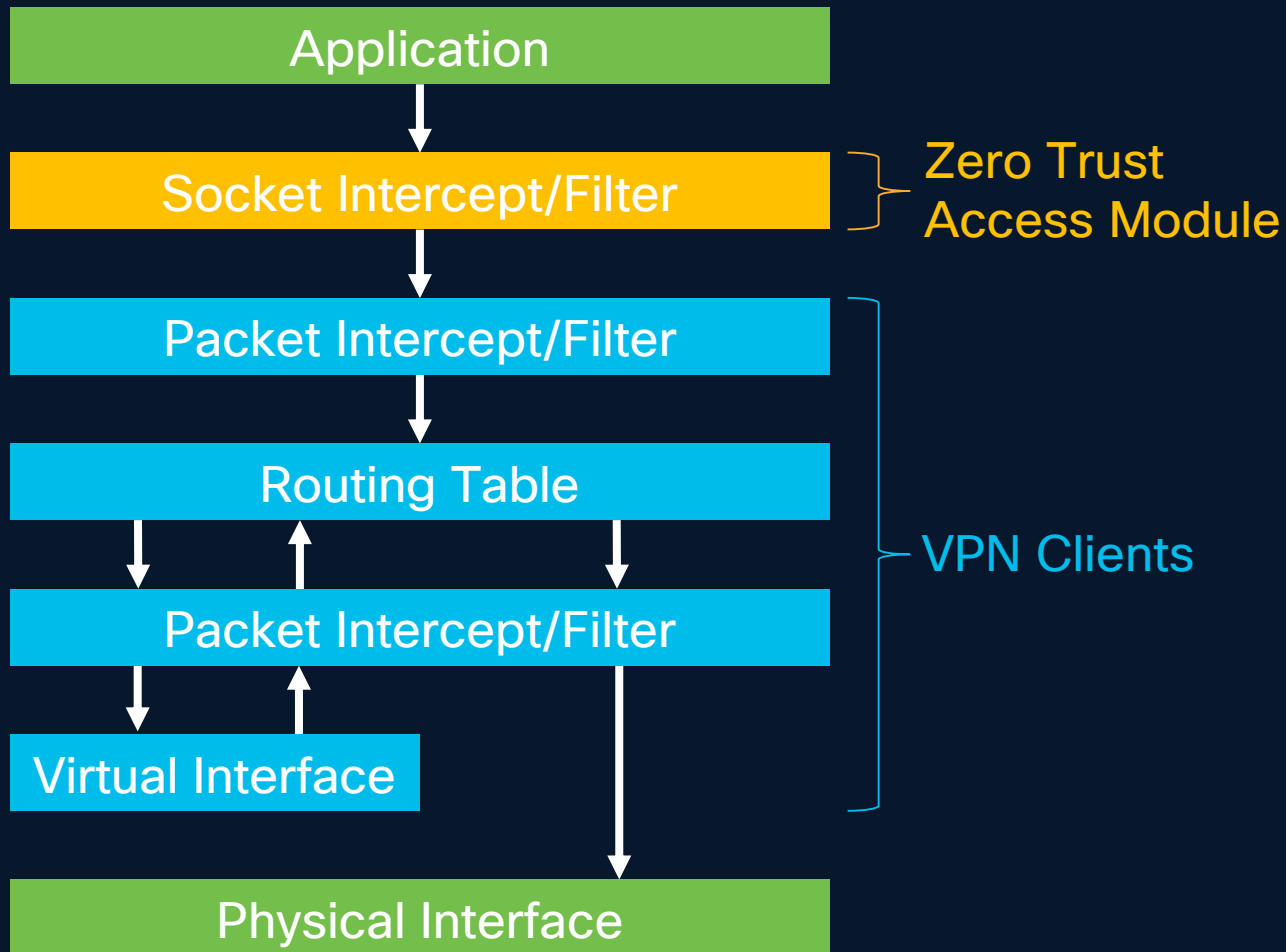
Contact me: Webex Chat or find me at the conference

Thank you

CISCO Live !



Cisco Secure Client: 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