The bridge to possible

Inside Cisco IT

Powering the Next Generation Hybrid Workspace with SASE

Roel Bernaerts, PRINCIPAL ENGINEER

Cisco Webex App

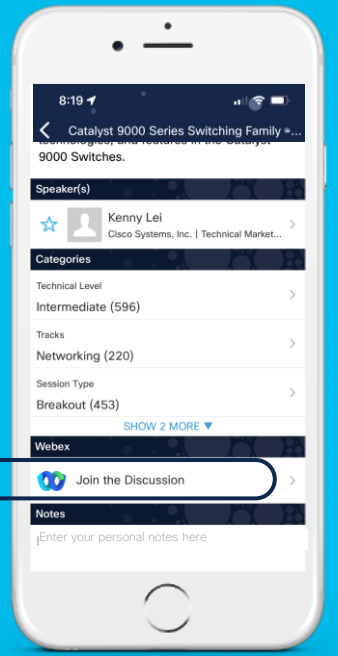
Questions?

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

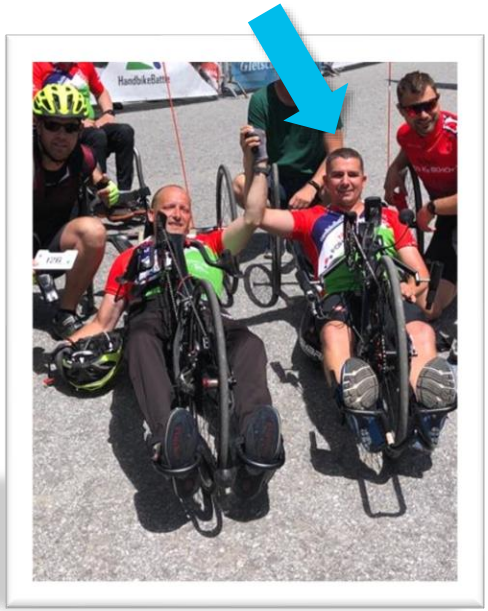
How

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 until February 24, 2023.



About me …



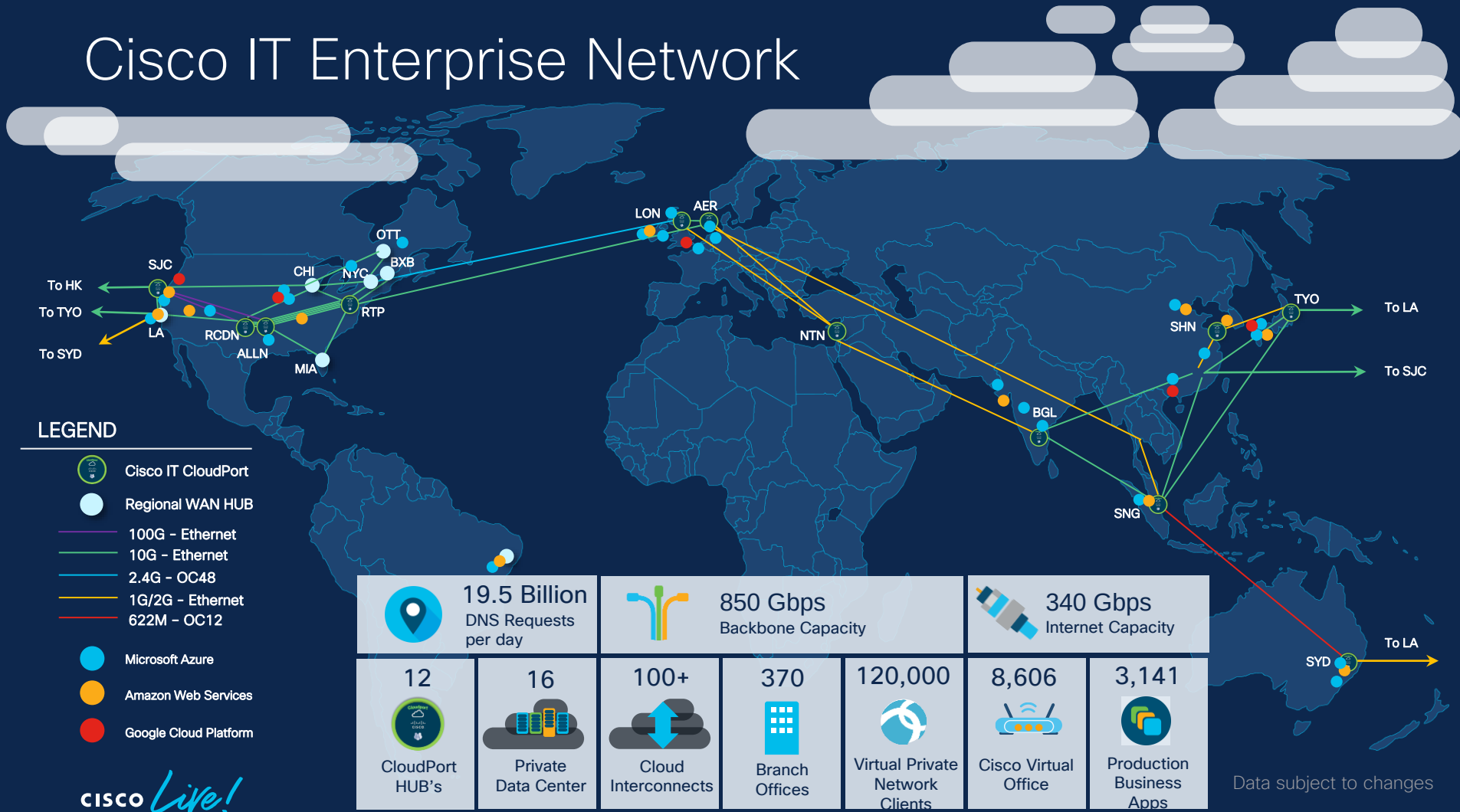
Roel Bernaerts

- 22 years at Cisco …
- Network Routing & Security
  Operations, Implementation, Design, Architecture
- Love(s)d the CLI
- Wanted to become graphic designer
- Hand bike buddy

Agenda

- What is SASE and why is it important to Cisco IT ?
- Our journey so far …
- On-Prem “SASE” HUB
- SASE Use-Case deep-dive
- What’s next for Cisco IT ?

Cisco IT Enterprise Network



LEGEND

- Cisco IT CloudPort
- Regional WAN HUB
- 100G - Ethernet
- 10G - Ethernet
- 2.4G - OC48
- 1G/2G - Ethernet
- 622M - OC12
- Microsoft Azure
- Amazon Web Services
- Google Cloud Platform

19.5 Billion DNS Requests per day

850 Gbps Backbone Capacity

340 Gbps Internet Capacity

12	16	100+	370	120,000	8,606	3,141
CloudPort HUB's	Private Data Center	Cloud Interconnects	Branch Offices	Virtual Private Network Clients	Cisco Virtual Office	Production Business Apps

Data subject to changes

cisco Live!

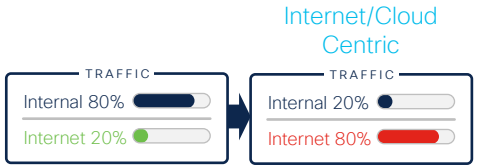
Introduction

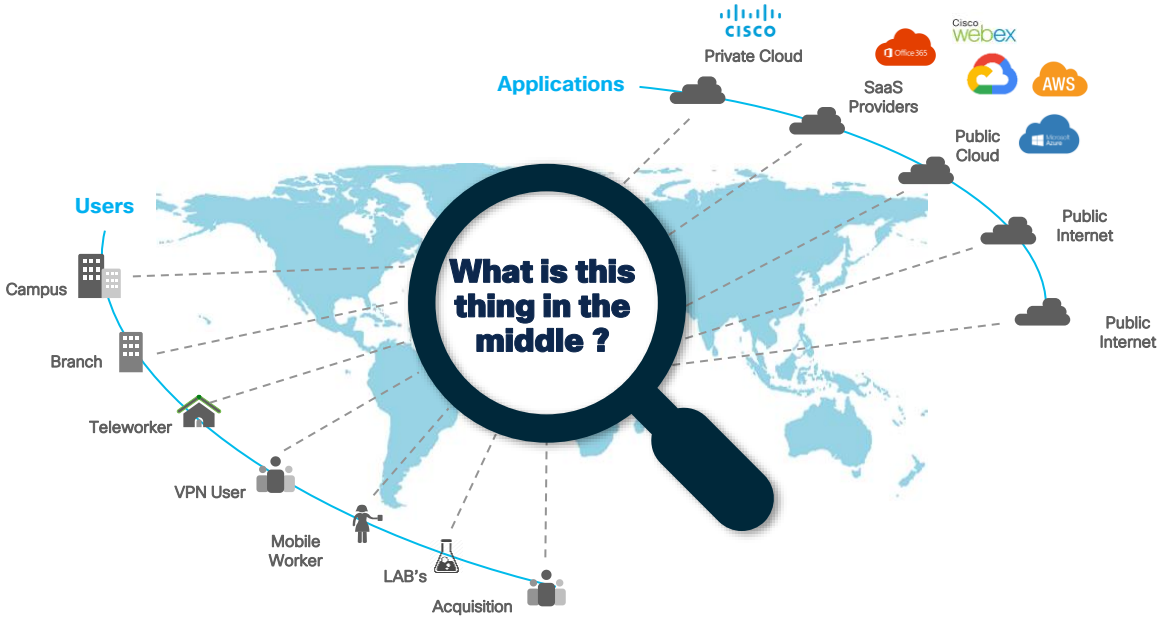
Enabling users ANYWHERE to talk to application EVERYWHERE !

WE ARE LIVING IN A HYBRID WORLD

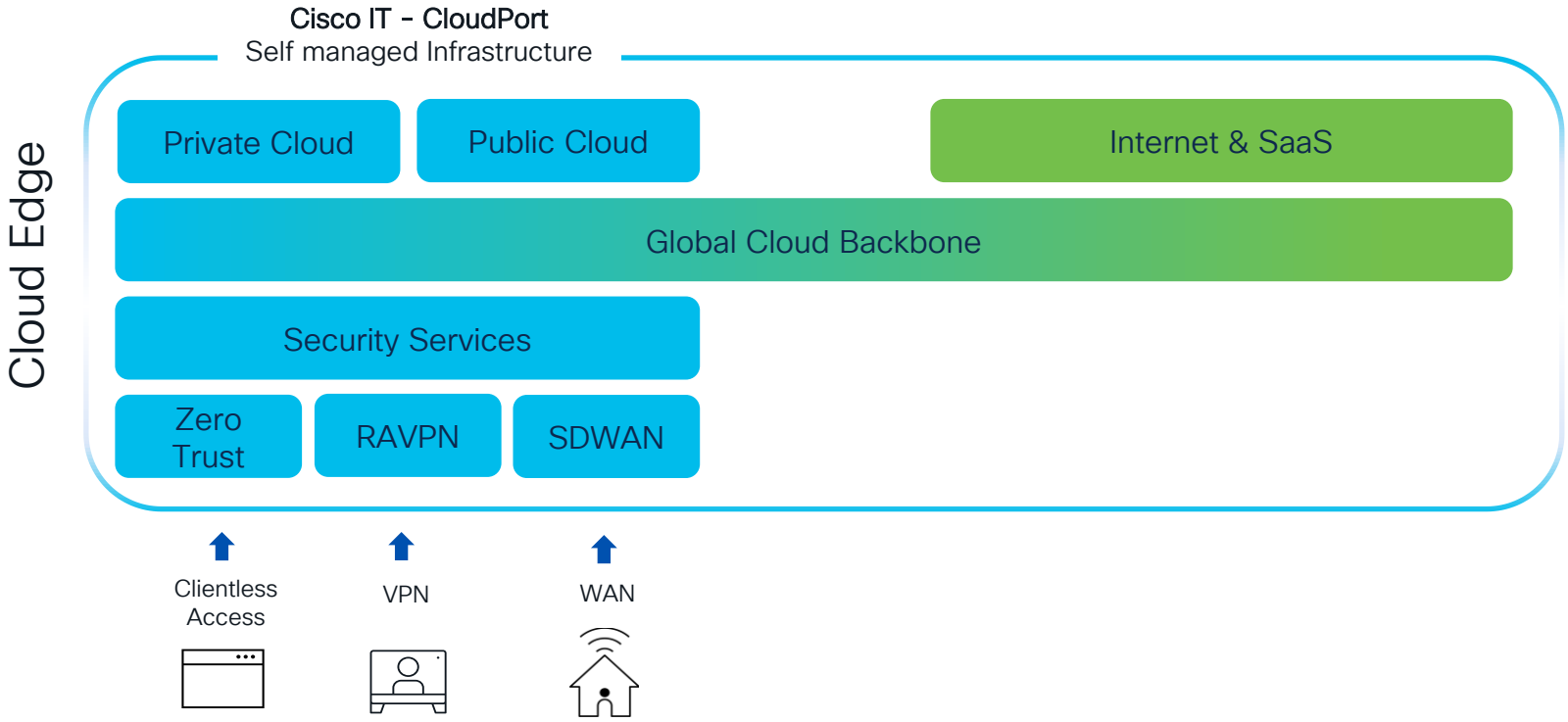
75% work from home
over 50% of the time

Business applications move to **Cloud & SaaS**

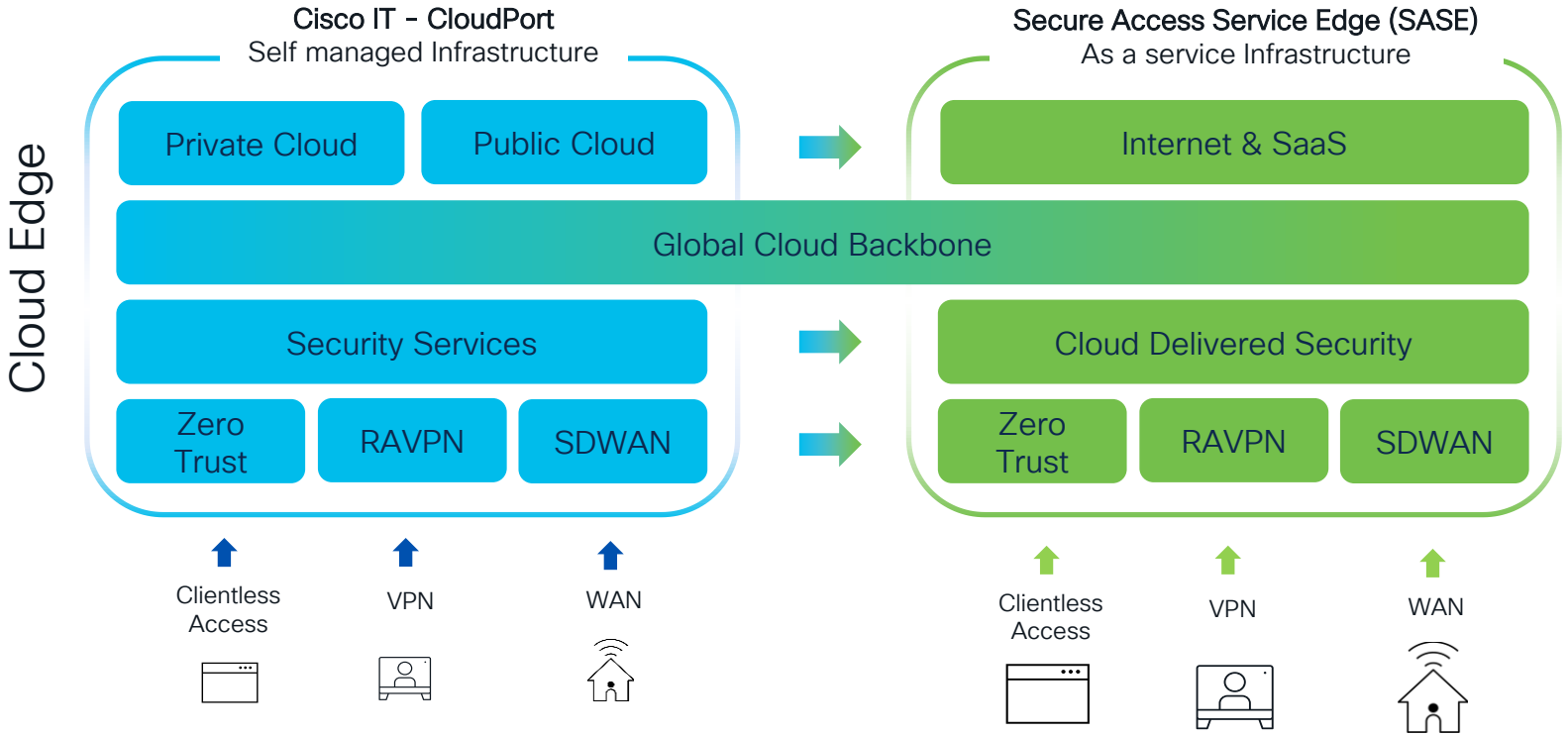




Evolving Hybrid Work platform to as a Service



Evolving Hybrid Work platform to as a Service



Why is SASE important to Cisco IT ?

Business value with SASE

Solve IT business problems

Do it yourself challenges

- Complex to build and maintain
- Requires specialized skillets
- Less insights with traditional security
- Multitude of platforms and controllers
- Infrastructure heavy – shipping and cost
- Difficult to react to fast changing business needs

Optimize IT spend
Improved client experience
Outsource complexity
Enhanced security controls
Centralized insights
Business agility

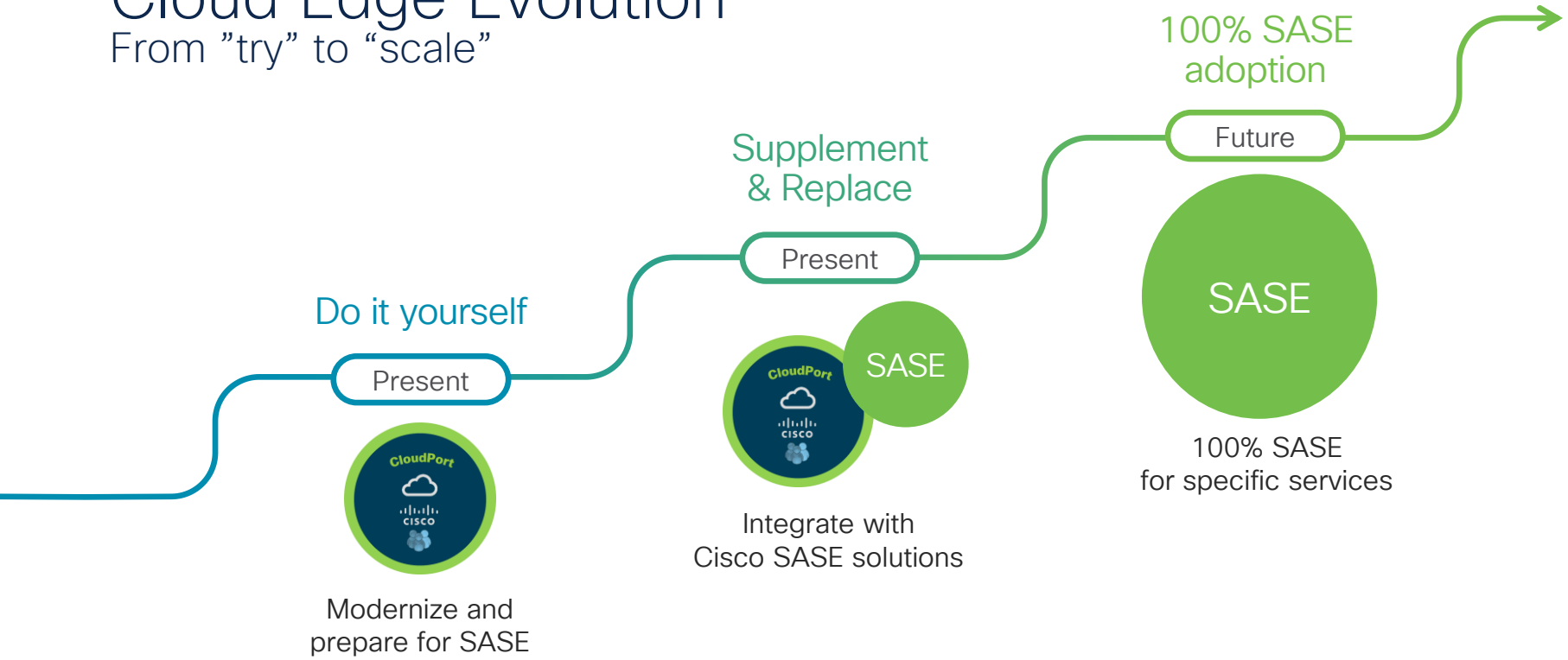
Cisco on Cisco

Be Cisco's first and best customer

- **Influence Vision & Execution**
  Help shape Cisco's SASE vision by sharing real customer business challenges and requirements
- **Make our products better**
  Evaluate new technologies & solutions early in the development process before shipping to our customers
- **Share with our customers**
  Help customers by sharing lessons learned. success stories and adoption strategies.

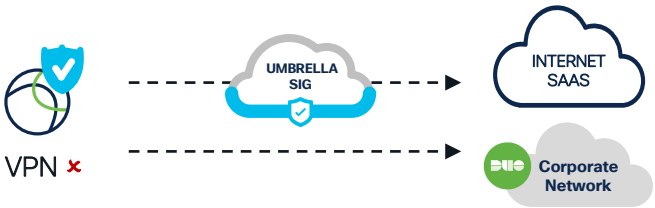
Cloud Edge Evolution

From ”try” to “scale”

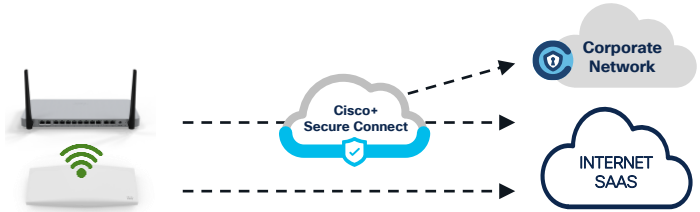


Early adoption

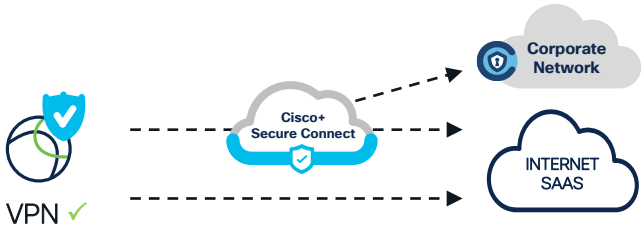
Secure Remote Worker (no-VPN)



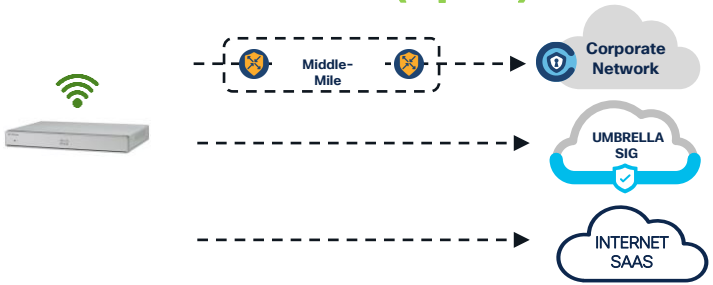
Secure Teleworker (Meraki)



Secure Remote Worker (VPN)



Secure Branch (Viptela)

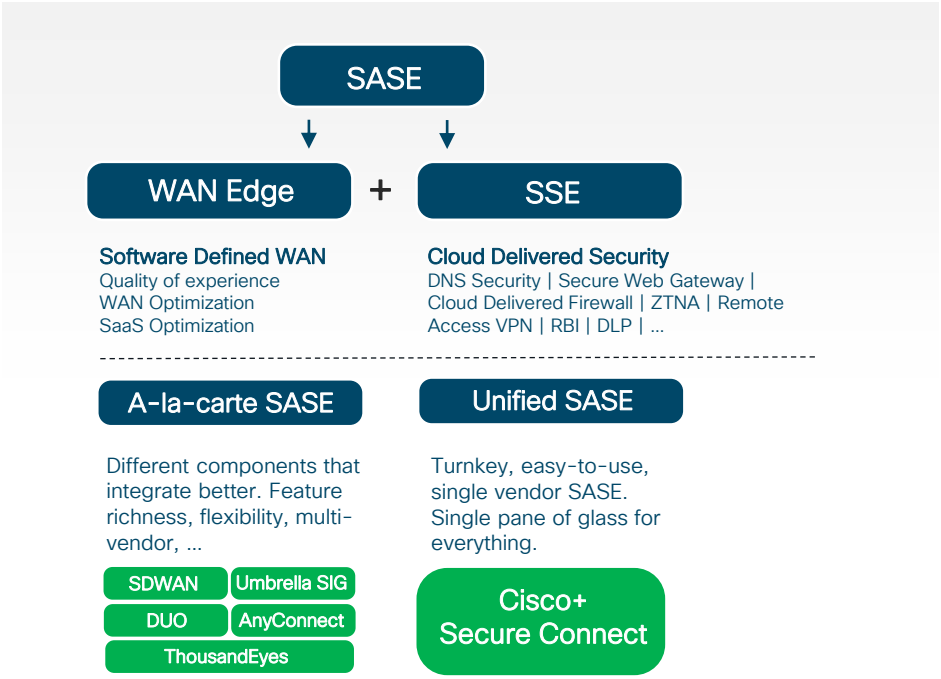


Lessons Learned

What does SASE mean ?

- Gartner, Dell'Oro, SASE providers all have different definition that can change from time to time
- Marketing often ahead of the execution
- Difficult to commit during times of uncertainty. Created some emotional resistance.
- More clarity and consistency today. First SASE wins !
- Excited about what is coming !

My ~~Cisco IT's~~ definition of SASE



Lessons Learned

(*) Neophobia – The fear of anything that is new
(**) Agoraphobia – anxious in unfamiliar environments perceive to have little control.

Mixed-Mode environments

- During the transition period there will be the legacy and SASE way of doing things
- Resistance because in the interim things can get a bit complex
- Low incentive – we have something that mostly does what it needs to do
- Focus on things that generate minimal overhead and bring immediate value
- Target specific use-cases that can be moved completely within a reasonable timeframe

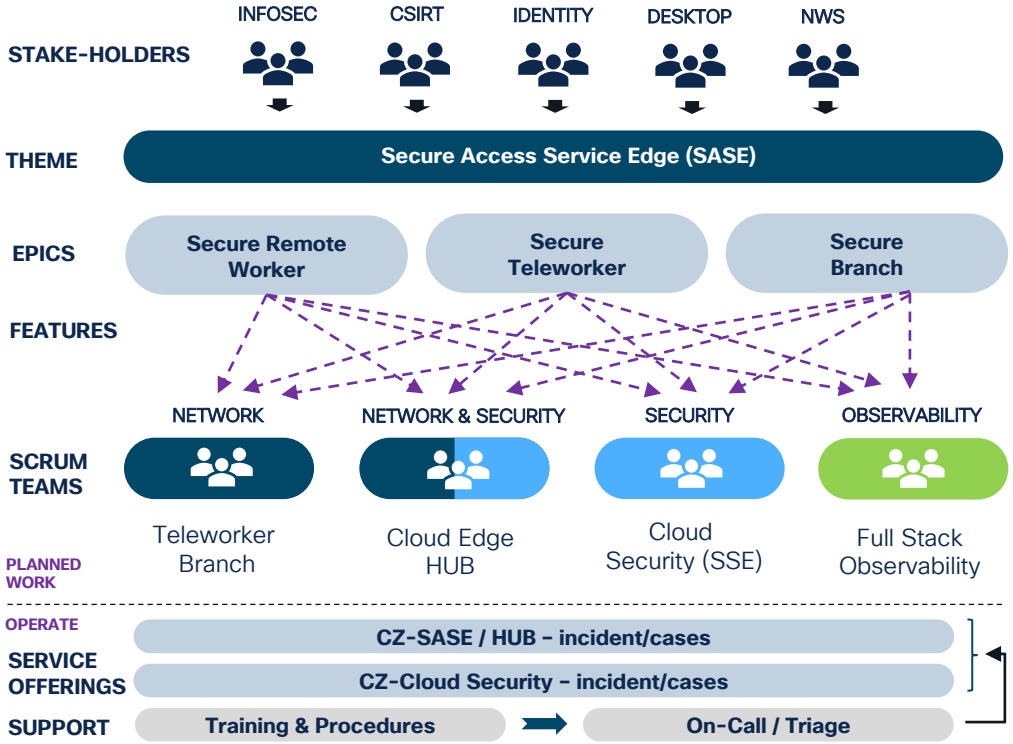
Operational readiness & outsourcing

- Neophobia(*) and agoraphobia (**) are common and in this scenario probably a good thing
- Rome wasn't built in one day – embrace some disruption and mitigate with your own tooling
- Start small and build confidence & trust
- Have a fallback plan for as long as you think you need it
- Allows resources to work on more important & critical work

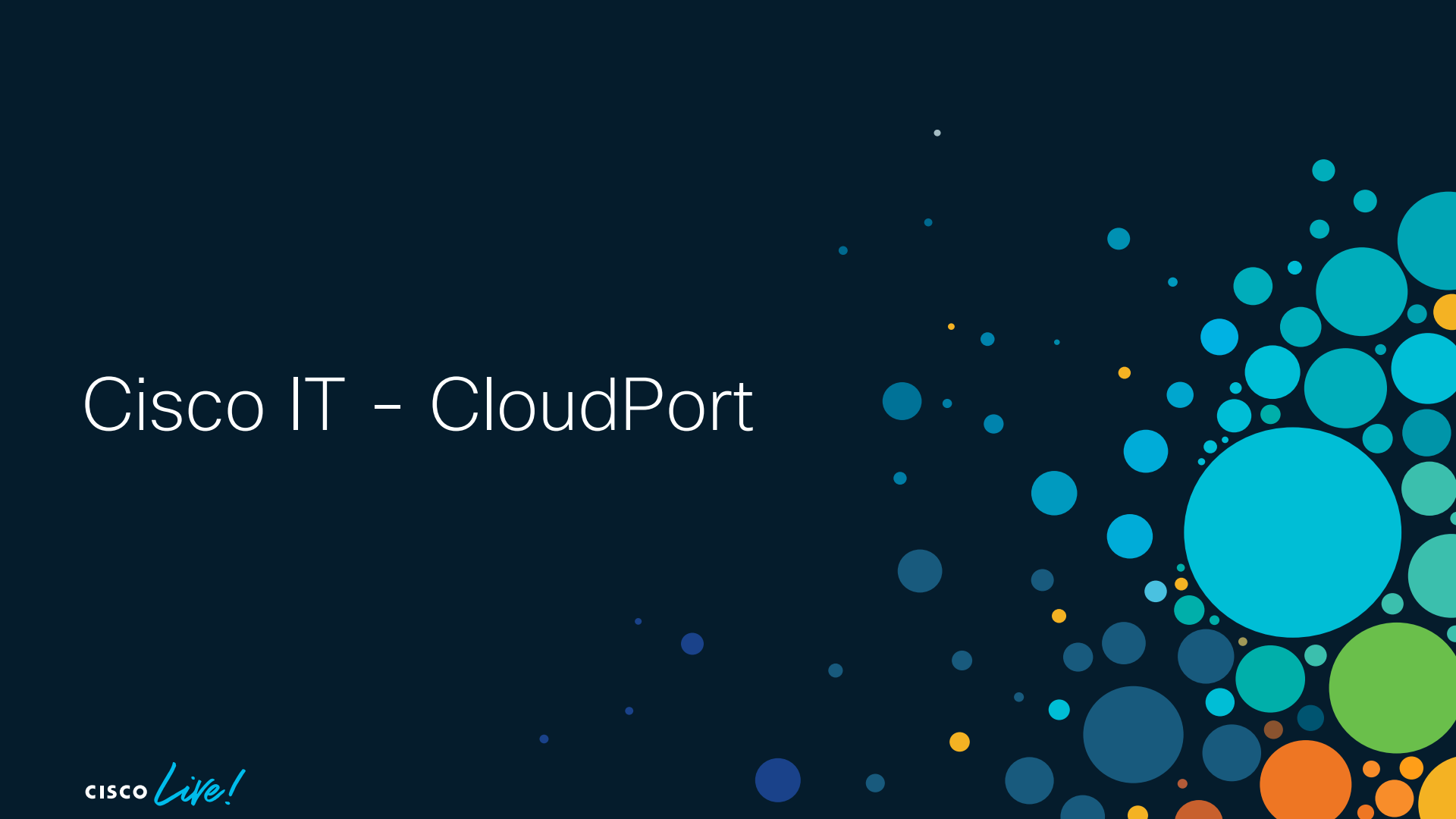
Lessons Learned

Execution & Operating model

- Networking and security needs to converge more than ever !
- Ownership distributed across many different teams
- Unique requirements & priorities that don't always align
- Tried new operating models with a smaller portion of the organization
- Agile framework that assures alignment and drives work across networking and security teams

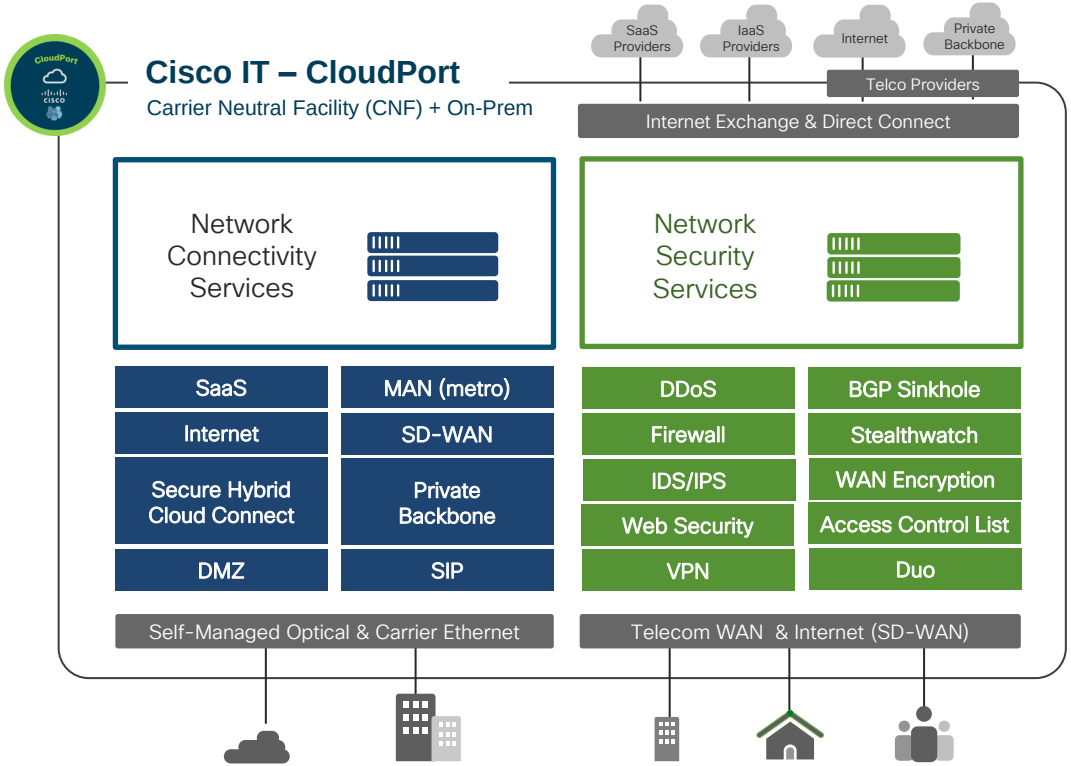


Cisco IT – CloudPort



Cisco IT -CloudPort

Single tenant “SASE”



Hardware & Software

Cisco Secure Firewall
ASA/FTD

NSO

ThousandEyes

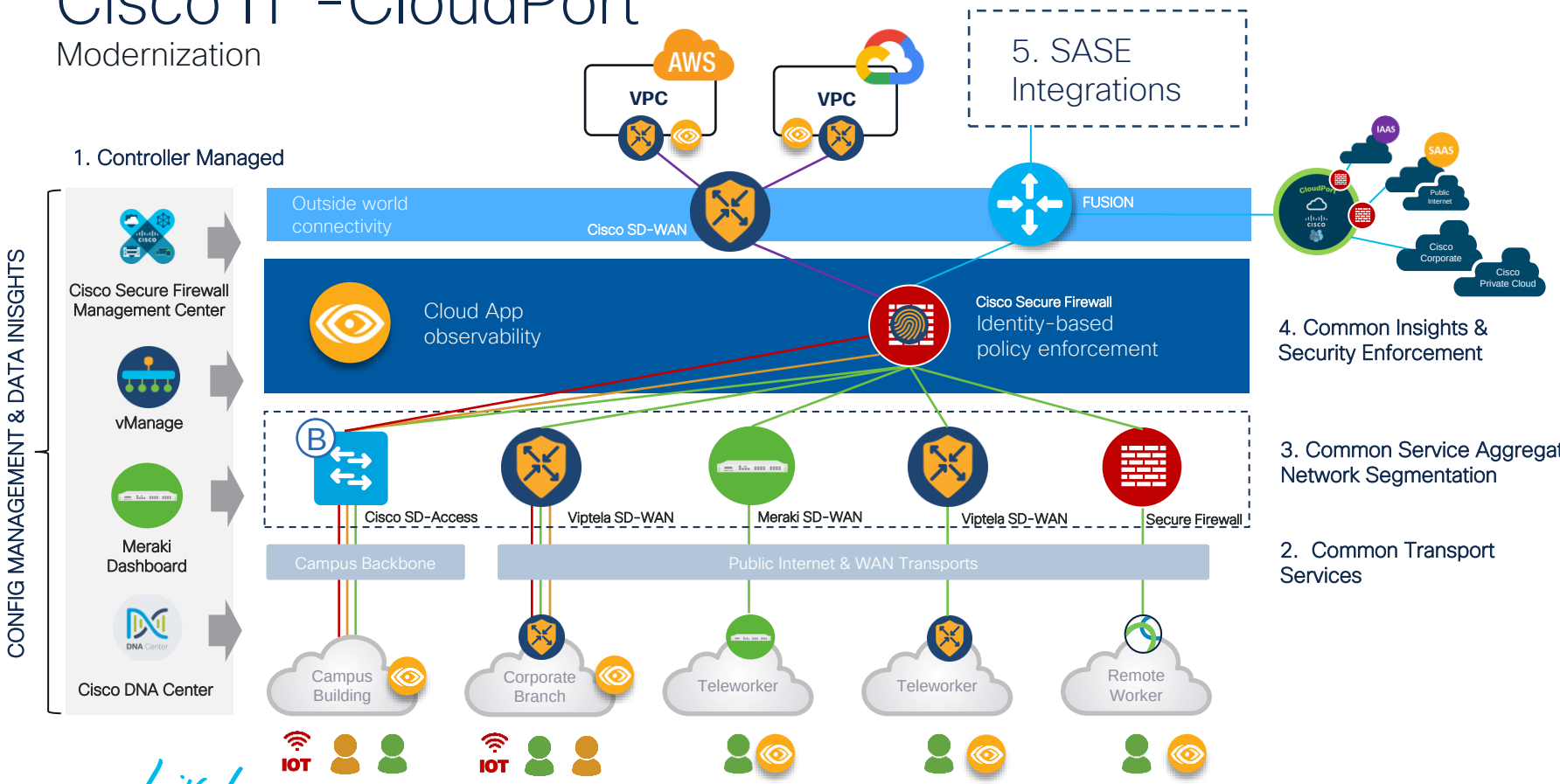
SDx
Self-built software

viptela Meraki DNA Center

Leverage products across Cisco product portfolio to offer Network & Security services in a common platform !

Cisco IT -CloudPort

Modernization



SDWAN Everywhere

Optimized Transport

Internet as primary transport

Dual DIA offices

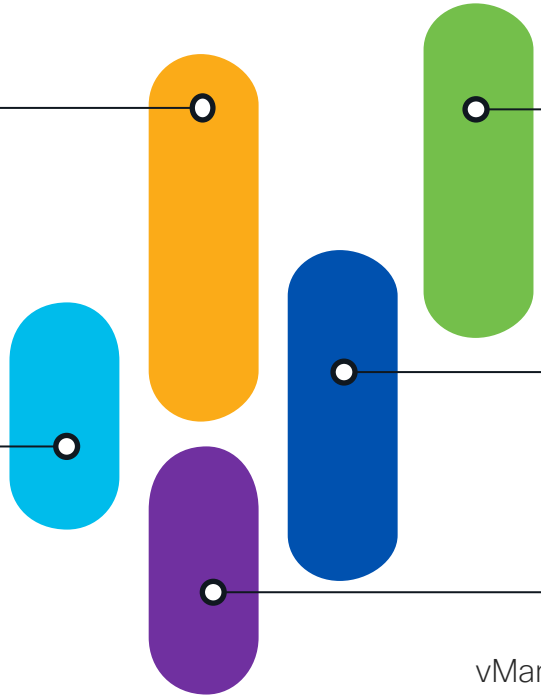
Middle-Mile optimization

WAN Optimization

Quality of service

Application aware routing

Micro- & Macro-segmentation



Hybrid Cloud Connect

SDWAN Cloud OnRamp MultiCloud

CSR1000v

Cat8000v

SaaS Optimization

SIG Auto-Tunnel integration

Cloud OnRamp for SaaS

Support simplification

Controller managed operations & change

vManage & analytics Insights & troubleshooting

Platform standardization (Cat8300/Cat8500)

Network-as-a-Service

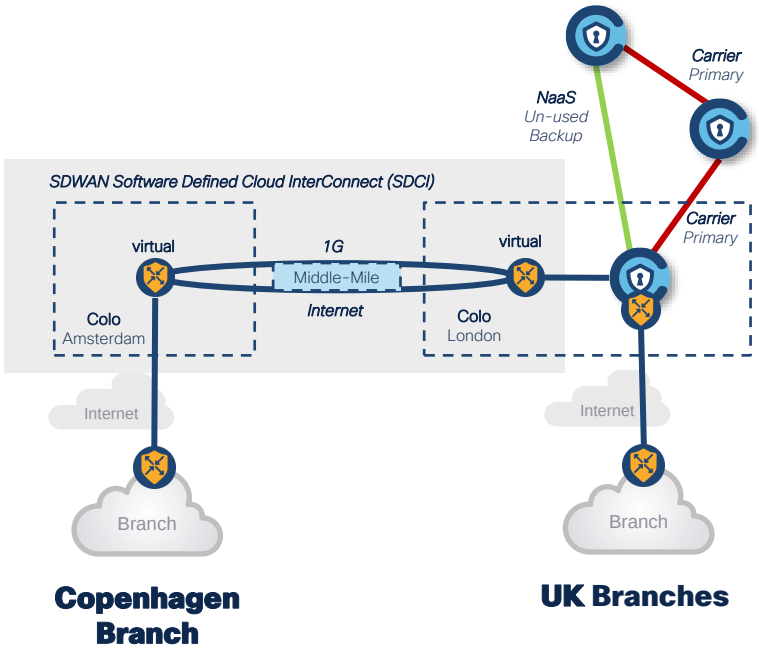
- Telco is usually in the top 3 of highest costs for an IT organization
- Cisco's backbone consist of full-stack HUB's and smaller WAN only hubs.
- Some WAN only hubs are high cost for the purpose they serve. Some circuits in the backbone are only used in failure scenario.

SDWAN Software Defined Cloud InterConnect (SDCI)

- bring up virtual SDWAN nodes in Colo facilities
- Optimized Middle-Mile connectivity to on-prem

Software defined capacity

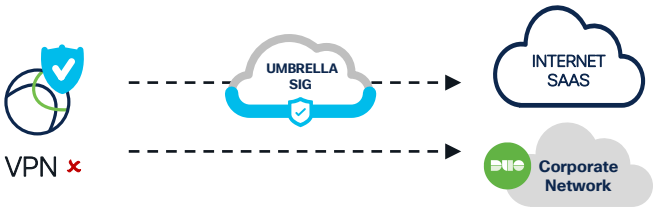
Replace expensive idle/backup circuits with cost-effective, high-speed and reliable connectivity delivered by Colo providers



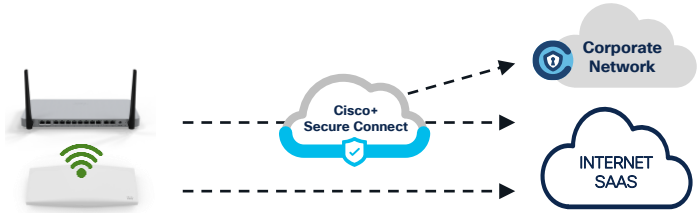
SASE Use-Cases

Use-cases

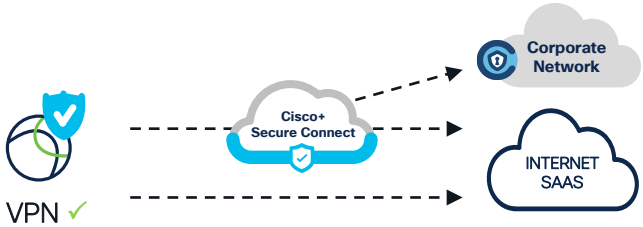
Secure Remote Worker (no-VPN)



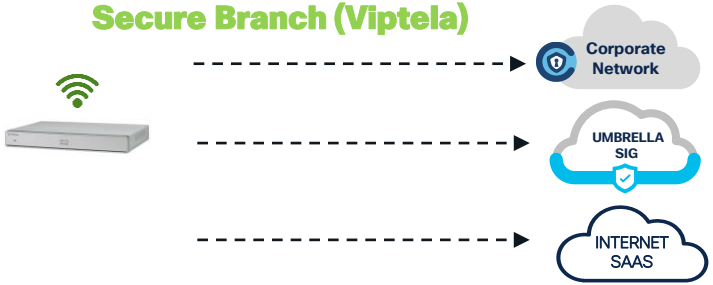
Secure Teleworker (Meraki)



Secure Remote Worker (VPN)

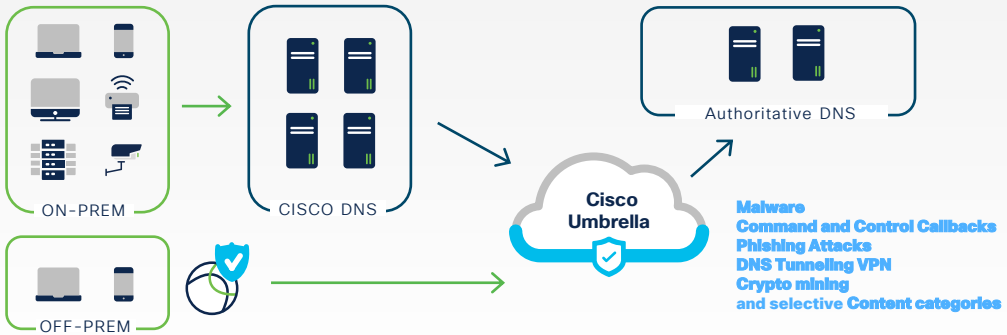


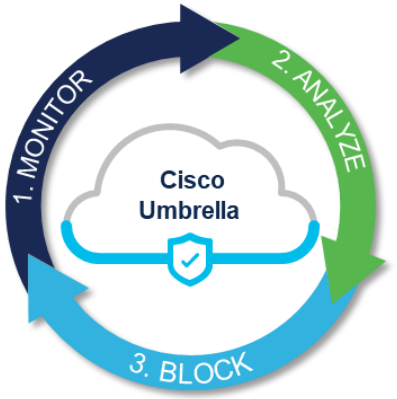
Secure Branch (Viptela)



Umbrella DNS Security

Importance of DNS security often underestimated
First step in connecting to the internet
Used by all devices, in nearly all internet connections





19.5b
DNS Queries per day off sourced from the Cisco network and endpoints

22m
DNS blocks per day

1000x
Amount of threat intelligence in Umbrella vs Infosec home grown system

30 min
Average time of the change requests to enable enterprise wide policy changes

110k
Umbrella clients enabled in 2 weeks

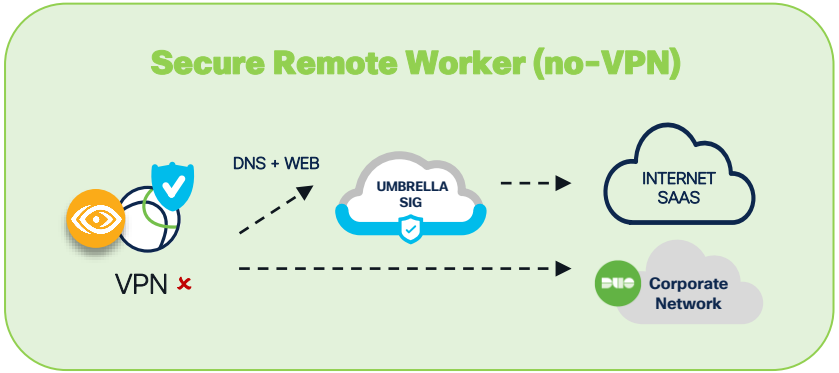
3
End client installation cases

<10 cases
For False Positives per Month

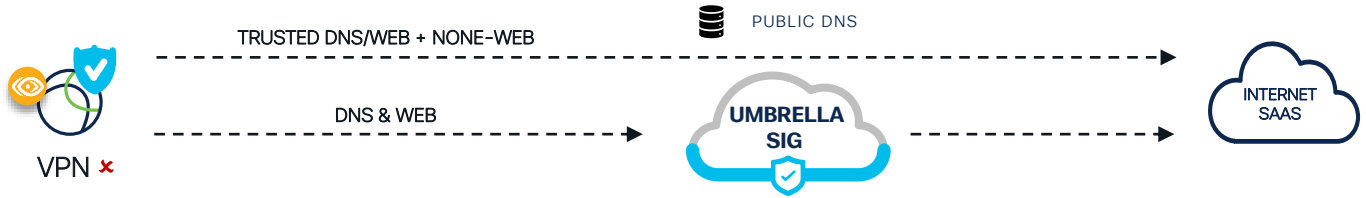
Secure Remote Worker (no-VPN)
Use-Case summary

Protect users at home when not connected to VPN

- When users work from the internet, they are only protected by security on the endpoint itself
- With AnyConnect VPN integrated with Umbrella SIG, users can be protected even when not on VPN
- DNS protection and advanced Web protection
- Client experience monitoring via ThousandEyes endpoint agents

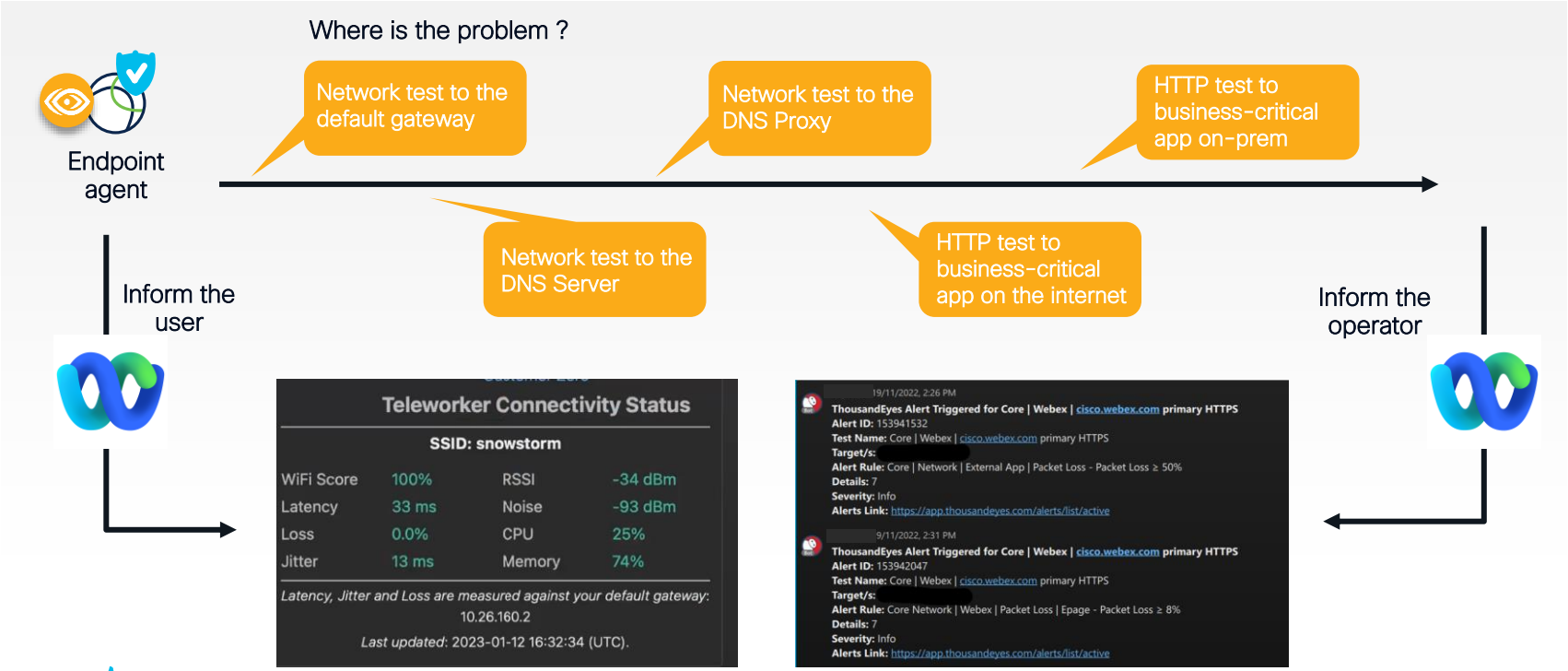


Secure Remote Worker (no-VPN)



1. ENDPOINT	2. DOMAIN MANAGEMENT	3. DNS POLICY	4. WEB POLICY	5. SECURITY OPERATIONS
▪ Cisco AnyConnect VPN with **Umbrella Secure Roaming** module ▪ Desktop team creates a **software package** and makes it availablele to entitled users ▪ Package includes the **Umbrella Org ID** information ▪ **Umbrella Root Certificate** installed via Mobile Device Management (MDM)	Bypass trusted or "broken" domains from redirection ▪ **Internal Domains** Resolve against client DNS and do not proxy *Local Domain suffix added automatically. Cisco Internal domains.* ▪ **External Domains** Resolve against Umbrella DNS and do not proxy Trusted applications such as O365, box, WebEx, …	Configure the DNS Policy ▪ Identity ▪ Security Setting Malware, C&C, Phising, Cryptomining, DNS Tunnel VPN. ▪ Content category filtering Application Settings ▪ Allow/Blocklist ▪ Block Page ▪ Logging ▪ Intelligent proxy **Powerful toolset to protect at the DNS layer !**	Configure the Web Policy ▪ Rulesets (Allow, Warn, Block, Isolate) ▪ File inspection / ThreatGrid ▪ File Type Control ▪ SAML ▪ Logging ▪ Security Settings ▪ Inspection *Selective decryption* **Powerful toolset to protect at the Web layer !** **More powerful when inspection is enabled !**	▪ Pro-actively test policy decisions with **policy tester** ▪ Monitor what is being blocked and why in **activity reporting** ▪ Export logs through **Log Management** ▪ Query Umbrella's database to gain insights via **Smart Search**

Visibility puts you in control
ThousandEyes



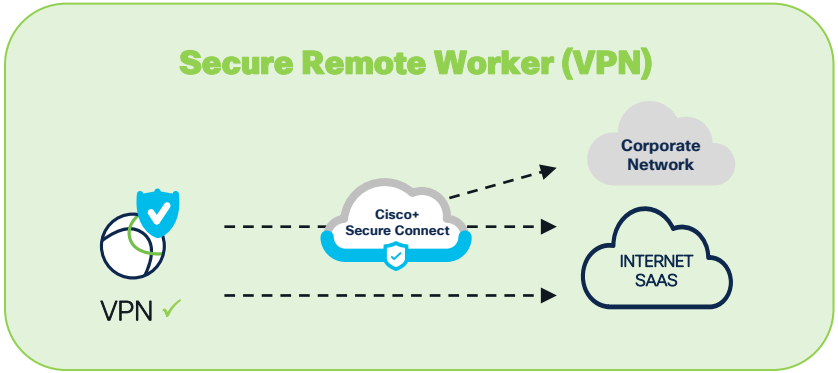
Secure Remote Worker (no-VPN)
Lessons Learned

• Potential performance improvements with DNS and better footprint – but overhead of inspection Mixed feedback from clients	Fine tune the policy to balance security versus connectivity. Takes some time to find a good middle ground
• Unexpected blocks for business related sites (SWG) due to certificate & cipher problems	Selective bypass until the underlying issue is resolved. Easier to solve for the things you own.
• Troubleshooting performance issues has become even more challenging	ThousandEyes endpoint agent helps to define if the issues is at home, Umbrella or the internet
• Good for security operations –lacking on network operations	See above
• There can be some initial pains – especially with inspection	Start with a small community with mixed job profiles Fine tune policy and expand.
• Domain management can be challenging	Feature request – better traffic steering capabilities at the client (Intelligent proxy)

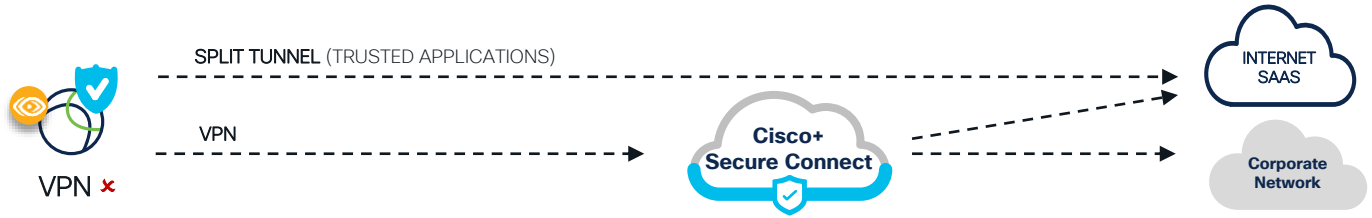
Secure Remote Worker (VPN)
Use-Case summary

Remote Access VPN as a service

- Deploying and maintaining on-prem VPN infrastructure can be resource intensive
- Cisco+ Secure Connect delivers RAVPN as a service with a few clicks of a button
- Provides secure internet access and protected access to private resources
- Consistent policy when on- and off- vpn



Secure Remote Worker (VPN)



1. ENDPOINT	2. DOMAIN MANAGEMENT	3. SAML / USERS	4. REMOTE ACCESS	5. BACKHAUL+ POLICY
▪ Cisco AnyConnect VPN with **Umbrella Secure Roaming** module ▪ Desktop team creates a **software package** and makes it availablele to entitled users ▪ Package includes the **Umbrella Org ID** file ▪ **Umbrella Root Certificate**	Bypass trusted / "broken" domains and private resources from redirection ▪ **Internal Domains** Resolve against client DNS and do not proxy ▪ **External Domains** Resolve against Umbrella DNS and do not proxy	Configure **SAML** & **Users/Groups** ▪ Org. wide SAML configuration (DUO,Okta, PingID, ...) ▪ Import users (Azure, AD, manual, ...) DUO allows access only for **approved** users connecting from **trusted** devices !	Configure **Remote Access VPN settings** ▪ Select regions ▪ IP's, DNS, Domain suffix ▪ Traffic Steering policy Split exclude Split include ▪ Basic client settings ▪ Assign Users & Groups ▪ Endpoint compliance Update **Roaming Computer settings** ▪ Trusted Network Detection	Build **backhaul connections** to the corporate network to reach private resources ▪ Add a new tunnel ▪ Select the far end platform (ASA,FTD, Meraki, Viptela, ...) ▪ Define which IP addresses are behind the tunnel ▪ Configure the far end Restrict access to private resources by **firewall policy** ▪ Allow- or block list policy

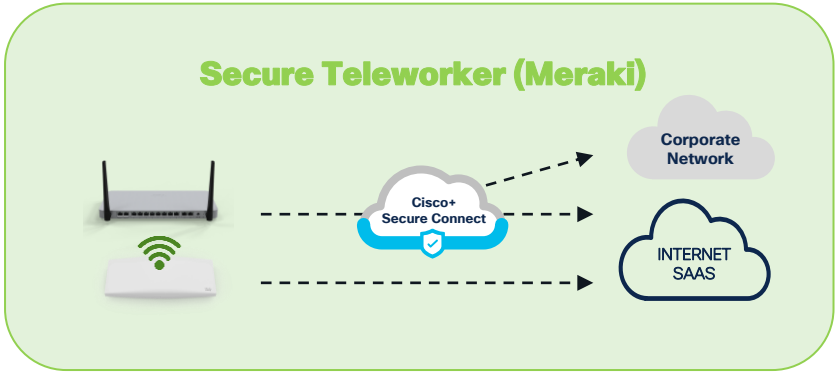
Secure Remote Worker (VPN)
Lessons Learned

• Multiple places to maintain policy for traffic steering decisions	Try to keep it simple. Keep traffic inside the tunnel when possible
• Endpoint compliance is limited today. Inconsistent with ISE on Prem	VPN protection with DUO SAML. Feature request for ISE
• When issues happen – limited ways for the user to work around that him/herself	Start without protection when on VPN (TND) and use on-prem security stack. Turn on protection after proving steady state
• Corporate network routing policies pose restrictions for backhaul connectivity (IP mobility & disaster recovery)	Build it the “SASE-way” – solve routing issues on-prem when integrating
• Scalability– number of users supported and backhaul capacity	Use for smaller scale use-cases.

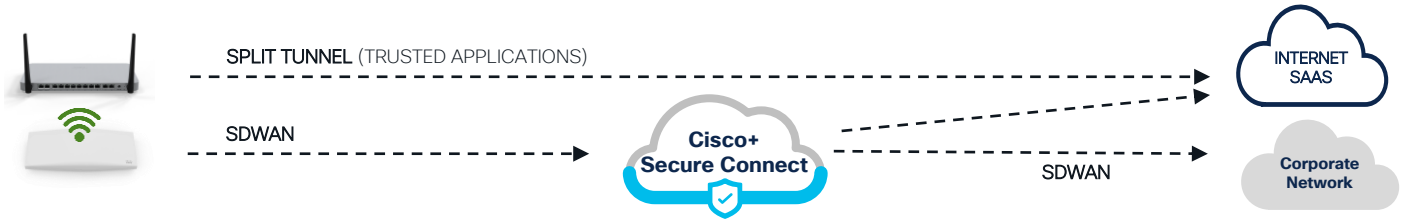
Secure Teleworker (Meraki)
Use-Case summary

Meraki SDWAN – as a service

- Entitled users need a hardware-based solution for working from home
- Cisco+ Secure connect allows to very easily integrate Meraki SDWAN
- Access to private resources via a Meraki SDWAN backhaul connectivity
- Secure internet Access via SIG
- Unified policy with VPN users



Secure Teleworker (Meraki)



1. CLAIM & CONFIG	2. SPLIT TUNNEL	3. ONBOARDING	4. BACKHAUL	5. POLICY
Client receives the hardware ▪ Claim serial number ▪ Licensing ▪ Firmware upgrades **Basic configuration** ▪ WAN ▪ IP Addressing ▪ VLAN's ▪ DHCP ▪ WIFI ▪ …	**Local internet breakout** - Send trusted applications direct to internet ▪ **Protocol / IP based** ▪ **Application**	Build SDWAN **tunnels** between **client devices** and C+SC ▪ Configure API Keys ▪ Map networks to HUB ▪ Enable VPN membership per VLAN ▪ Middle-Mile connectivity established automatically Enable Umbrella DNS protection ▪ DHCP Policy ▪ Group Policy (MX) ▪ Firewall & Traffic shaping (MS)	Build SDWAN **Tunnels** between **on-prem** devices and C+SC ▪ High Availability ▪ Map Networks to HUB ▪ Enable VPN membership ▪ Routing configuration	Create/confirm **identities** ▪ DNS : Network Devices ▪ Web : Internal Networks Add **identities** to existing **policies**

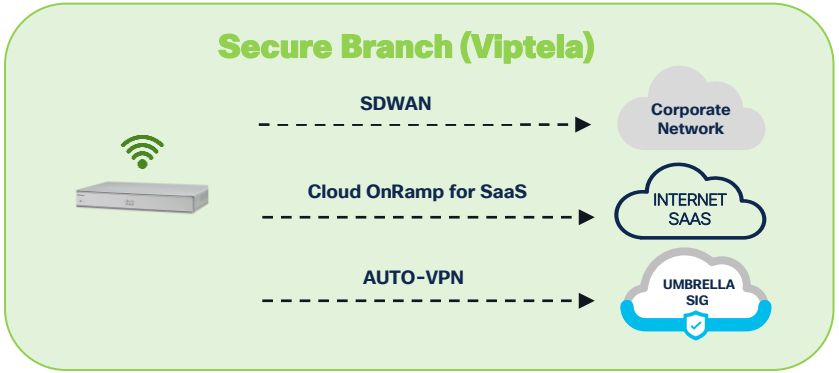
Secure Teleworker (Meraki)
Lessons Learned

• Inconsistent traffic steering for direct to internet between VPN and Meraki	Creates complexity – try to avoid inconsistencies
• Feature differences between router (MX) and Access-Point (MS)	Wireless access-points required to be able to bypass internal domains from DNS interception
• Limited routing capabilities on Meraki for integrating with On-Prem (active/active, BGP,…)	Use IPSEC Tunnels for backhaul tunnels (Viptela SDWAN)
• Works well for Teleworker. Less feature rich than Viptela SDWAN (micro/macro segmentation)	Feature enhancements requested

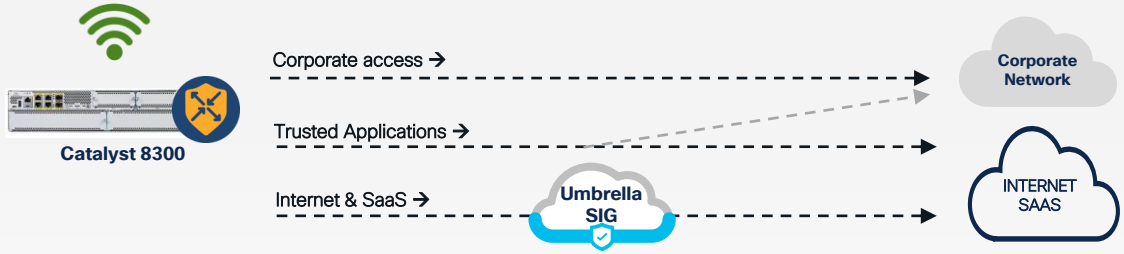
Secure Branch (Viptela)
Use-Case summary

Optimize SaaS applications experience

- A lot of traffic is backhauled to central locations impacting user experience
- Performance based routing of trusted applications direct to internet
- Bring users closer to applications while keeping Cisco Secure



Secure Branch (Viptela)



1. WAN Optimization

Most efficient use of available capacity ! Internet as primary transport !

An SD-WAN enables multiple WAN links to be centrally controlled and managed, providing optimization through the monitoring of packet loss, jitter, and latency on the various transport links.

2. SaaS Optimization & Secure Internet

Cloud OnRamp SaaS

Direct to internet for trusted applications (Performance-based)

- Intelligent identification of standard applications
- Direct internet access (DIA) by default
- Fall-back to 2nd DIA / L2VPN in case of performance issues

Umbrella Auto-Tunnel

Bring users closer to applications

- Benefit from much larger SASE footprint
- Avoid excessive backhaul
- Benefit from better peering

Secure Branch (Viptela)
Lessons Learned

• Application recognition failures resulting in Internet traffic routing to the internet	Install latest protocol packs, integrate with SaaS providers to supplement NBAR/AVC
• Application recognition failures resulting in On-Prem traffic routing to the internet	Data-Policy to force traffic over the SDWAN VPN
• Adds another layer of complexity to troubleshoot when things don't work as expected	Network Path Insights !! Ability to capture traffic and detailed view of AVC/routing decisions
• Sometimes difficult to see where traffic is going.	IT can be found .. Not too intuitive.

Remember… SASE is a journey

- Very excited about what is next !
- Be Cisco's first and best customer
- Adopt SASE at scale when/where it makes sense
- Decrease dependency on on-prem infrastructure
- Strengthen partnerships and combine efforts

Cisco on Cisco

Cisco Blogs

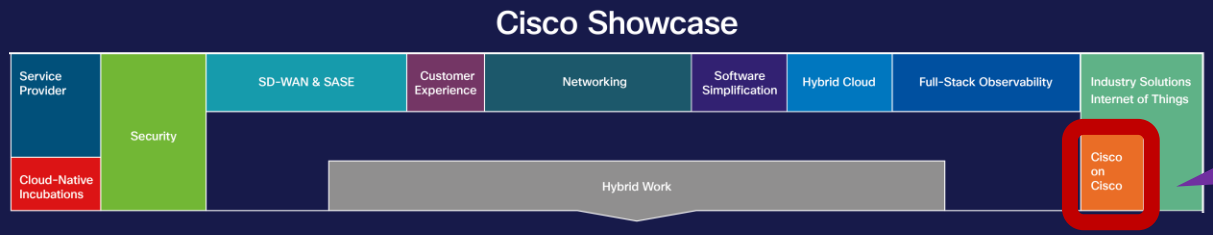
https://blogs.cisco.com/tag/sase
https://blogs.cisco.com/tag/ciscoit
https://blogs.cisco.com/tag/customer-zero

Cisco Live Content Library

Search for "Inside Cisco IT"

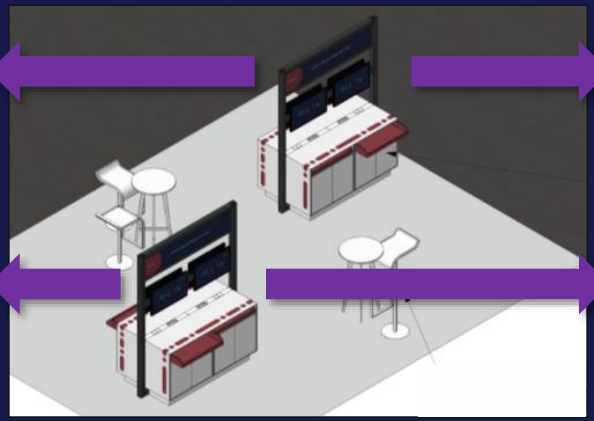
cisco Live!

World of Solutions



Powering the Hybrid Office

Collaboration Experience



Remote Work: From Home to Anywhere

Behind the Curtain with Cisco IT

Complete your Session Survey

- Please complete your session survey after each session. Your feedback is very important.
- Complete a minimum of 4 session surveys and the Overall Conference survey (open from Thursday) to receive your Cisco Live t-shirt.

- All surveys can be taken in the Cisco Events Mobile App or by logging in to the Session Catalog and clicking the "Attendee Dashboard" at https://www.ciscolive.com/emea/learn/sessions/session-catalog.html

Continue Your Education

Visit the Cisco Showcase for related demos.

Book your one-on-one Meet the Engineer meeting.

Attend any of the related sessions at the DevNet, Capture the Flag, and Walk-in Labs zones.

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


cisco
The bridge to possible
Thank you
cisco Live!


CISCO Live!
ALL IN