



Meraki: A Jornada para SASE



Marcelo Nunes
Strategic Sales Manager



Cassio Gomes
Technical Solutions Architect

AGENDA

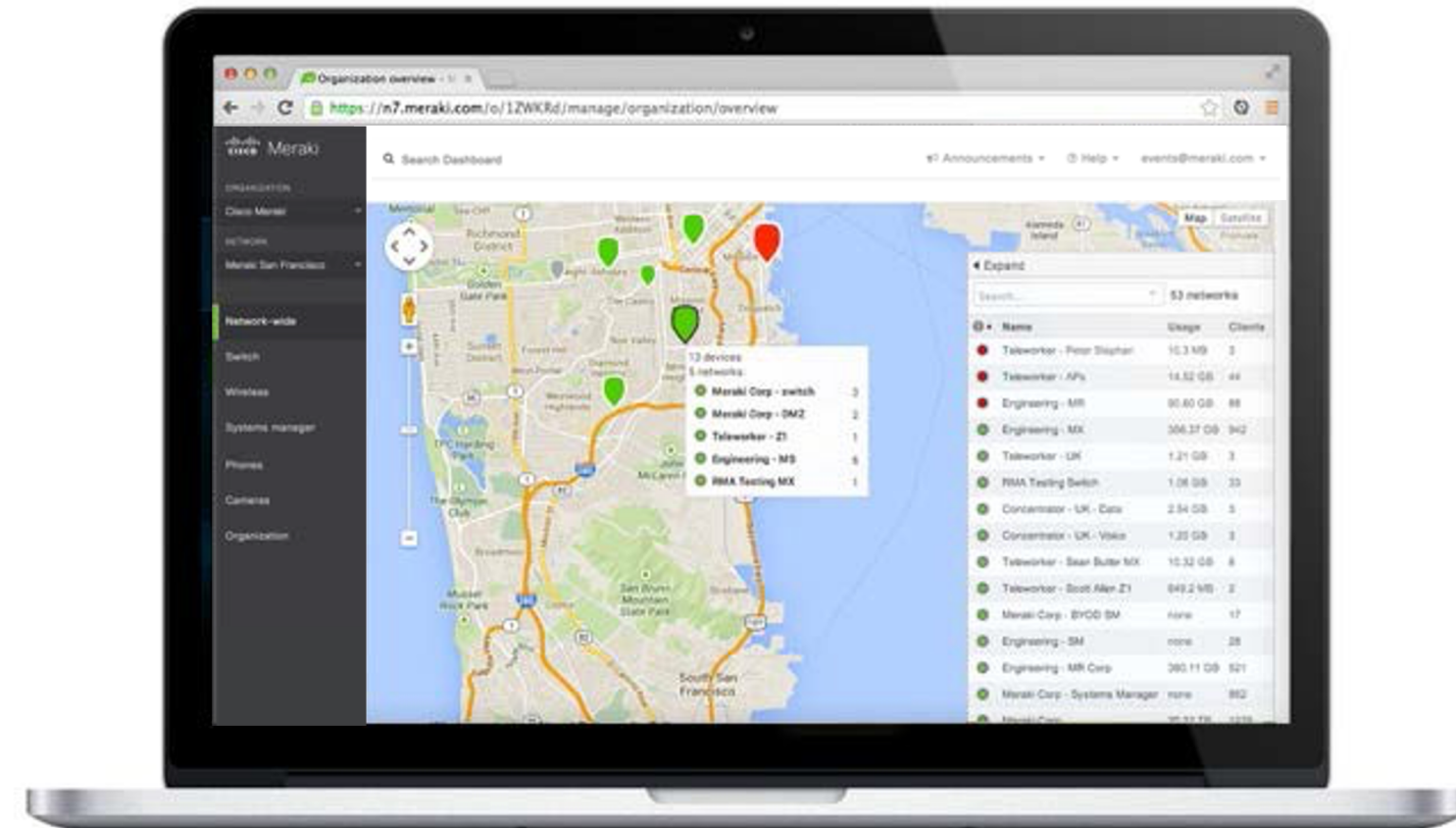
- Sobre Meraki
- SD-WAN & SASE
- Casos de Uso
- Demo



Sobre MERAKI



Marcelo Nunes
Strategic Sales Manager



Sobre a Meraki

Meraki criou uma solução de IT 100% gerenciada na Cloud que simplifica o trabalho.

Cisco Meraki acredita que simplificando a tecnologia, as pessoas podem focar no que realmente importa para o seu negócio.

A Meraki foi Fundada em 2006, adquirida pela Cisco em 2012, se tornou líder no mercado de IT, com mais de 230.000 clientes, e 8 milhões de dispositivos online ao redor do mundo.

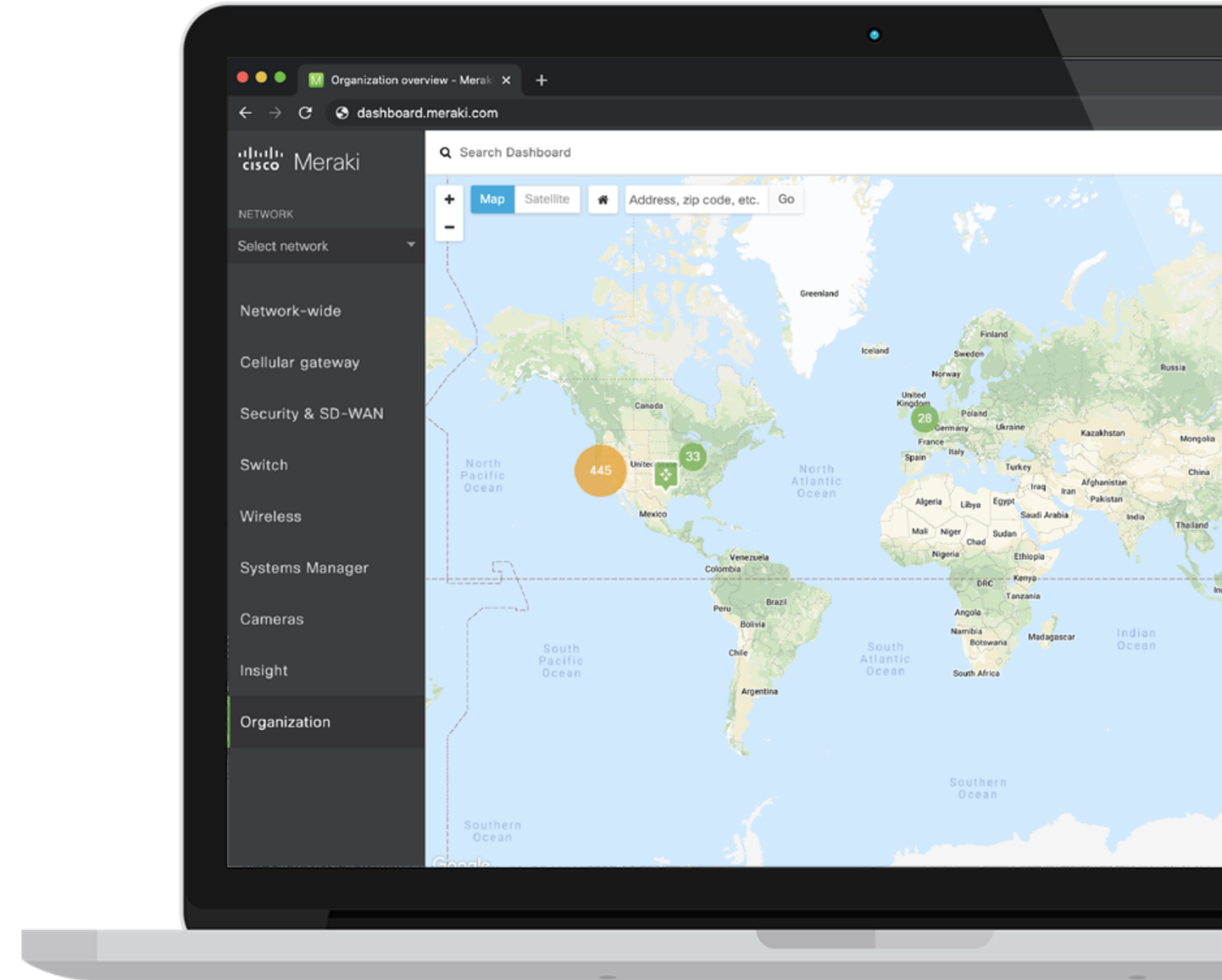
O portfolio Cisco Meraki inclui, Wireless, Switching, Security, e Câmeras.

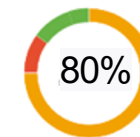
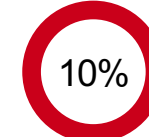
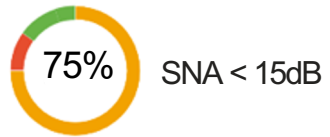


The Meraki Platform

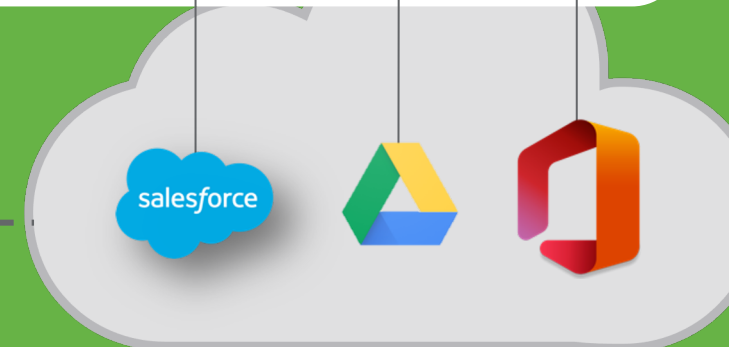
A Complete Cloud-Managed IT Portfolio from a Single Pane of Glass

 MR Wireless Access Points	 MS Ethernet Switches	 MX Security & SD-WAN Appliances	 MG Cellular Gateways
 MI Insight [Application & WAN]	 SM Endpoint Management	 MV Smart Cameras	 MT Sensors IoT





Client



Meraki Health

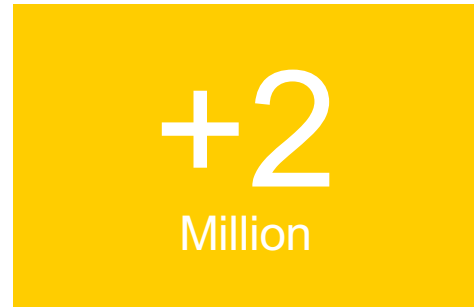
70% of organizations want a **single infrastructure vendor** (Gartner)

A peek at the numbers

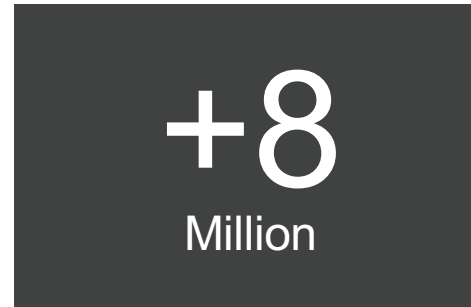
Platform statistics



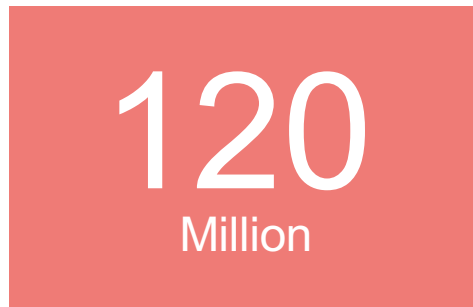
New Customers



Customer
Networks



Network
Devices Online



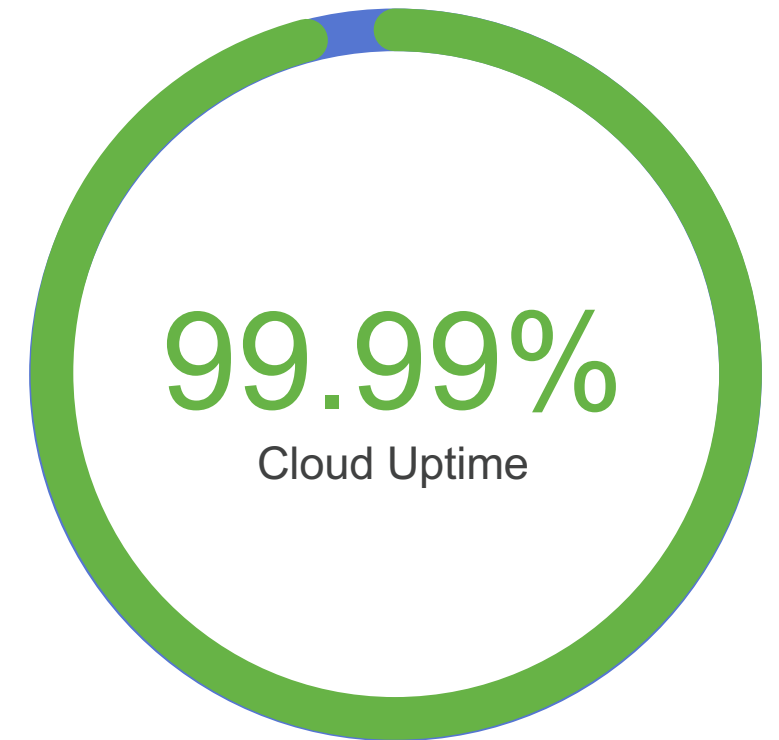
External API Daily
Requests

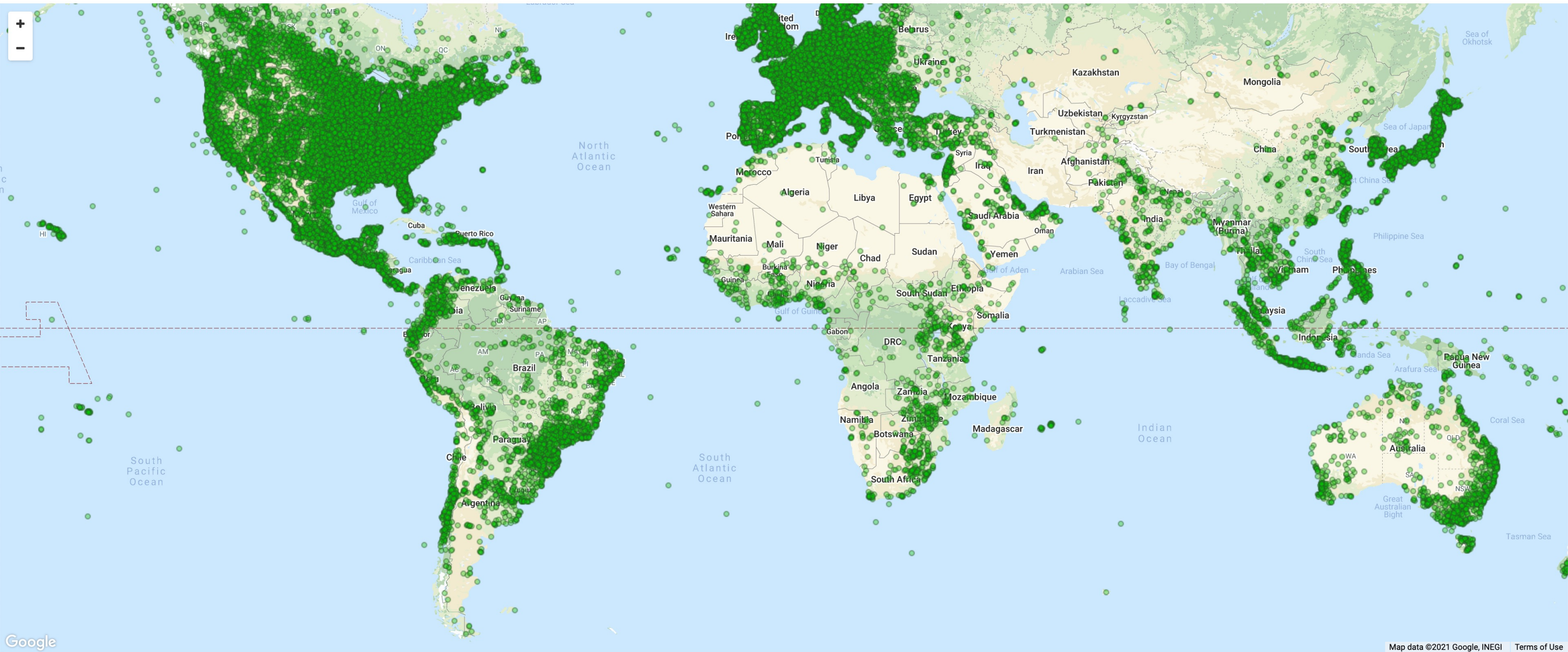


Daily End
User Devices



Daily Splash
Pages Served

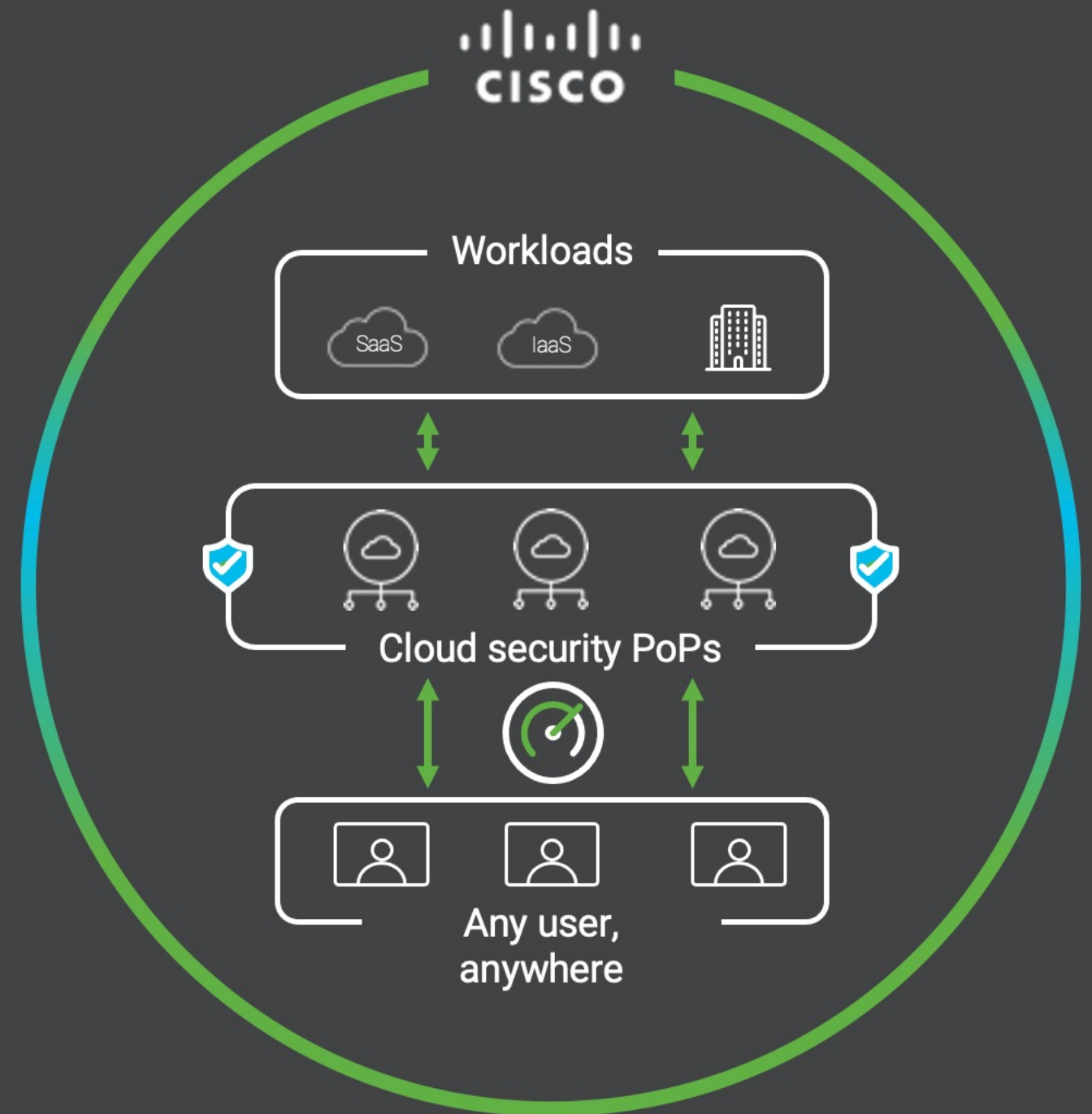




SD-WAN & SASE



Cassio Gomes
Technical Solutions Architect



WHY SD-WAN

WAN & Bandwidth Transitions

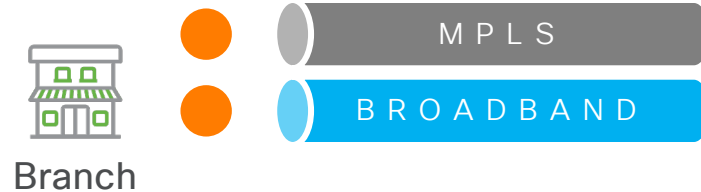


- **Increasing bandwidth** demands
 - Continued **cloud migration** of applications and resources
 - Increasing use of **video & VoIP**
- Private legacy WAN links are coming under **increasing strain**
- Other **WAN technologies are maturing** to become viable for enterprise consideration
 - Broadband
 - Fiber
 - Cellular

WHY SD-WAN: Reducing reliance on MPLS

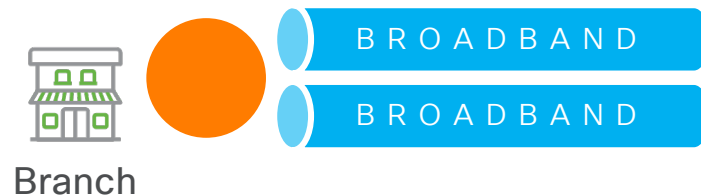
Cost-Effective & MPLS-like Enterprise WAN Options

AUGMENTED MPLS



- Supplement an existing MPLS network with broadband for increased bandwidth
- Offload traffic from MPLS to broadband with policy-based routing dynamic path selection

BROADBAND-BROADBAND

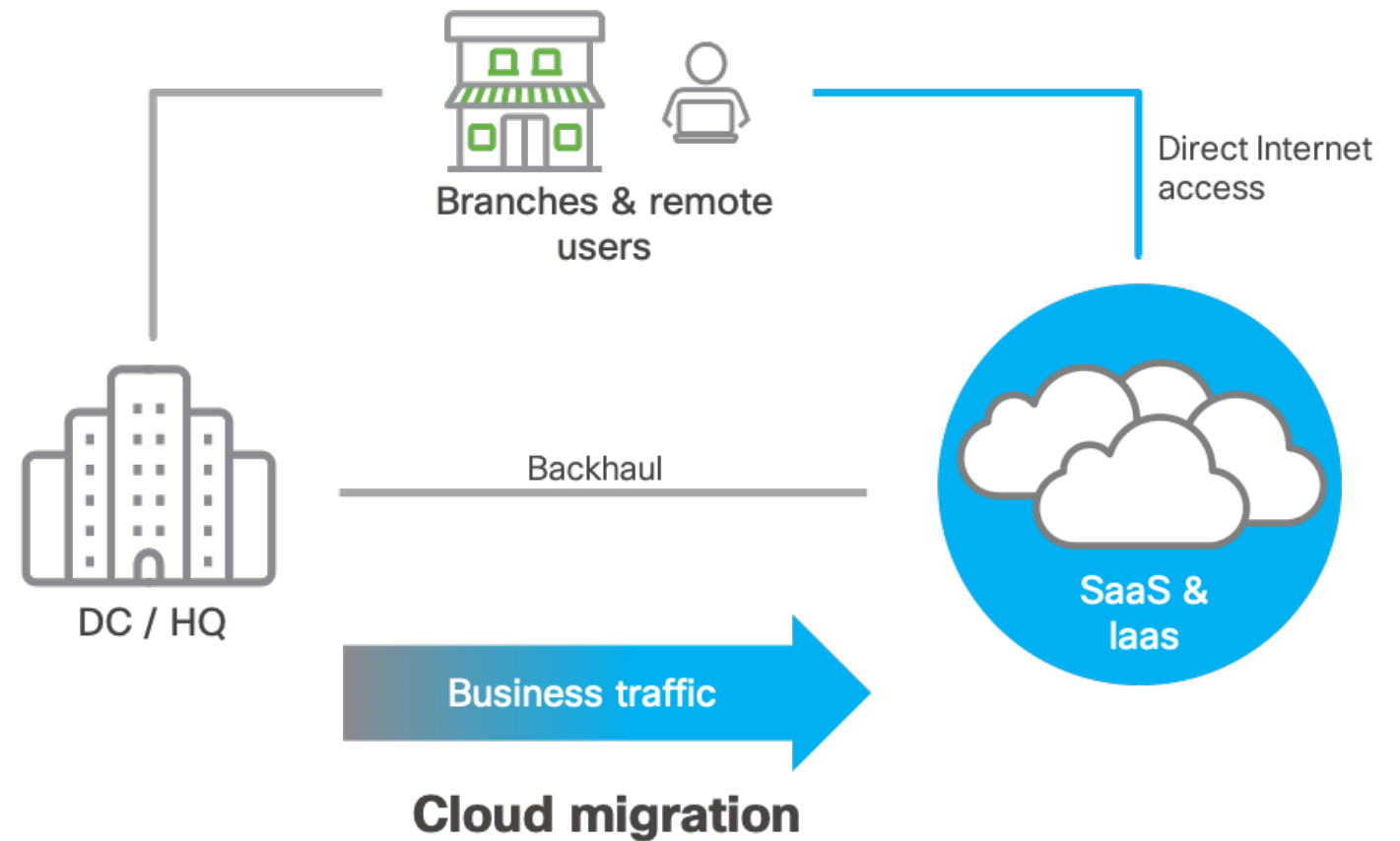


- Dual high speed broadband connections
- Load balance business critical traffic based on policy or link performance

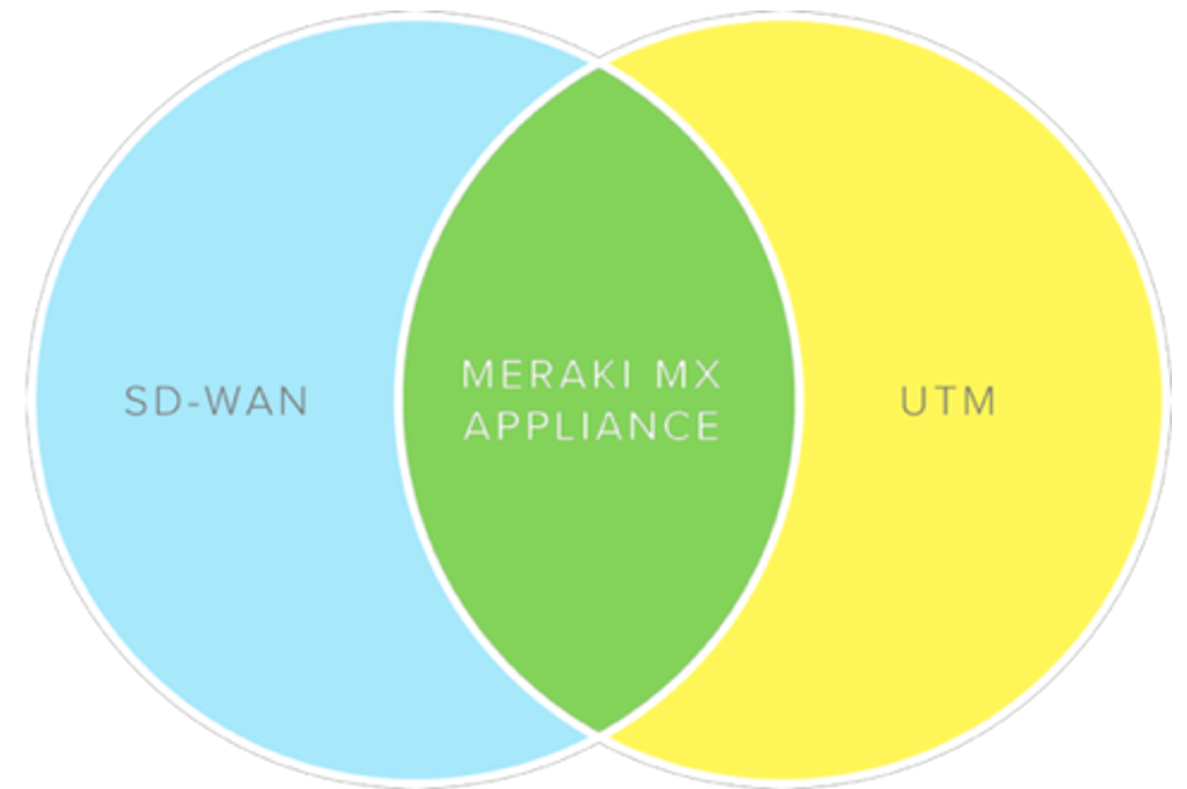
WHY SD-WAN: Beyond Conversion of MPLS

Quality of Experience

- Business traffic continues transition to be more **cloud-centric**
- Acceleration of resources and workloads moving to **SaaS & IaaS hosted in multiple cloud environments**
- Branches and remote users are increasingly accessing SaaS & IaaS **directly over the Internet**
- Visibility through **advanced analytics** is becoming essential to deliver high quality user experience
 - End-to-end: from the user to the application server
 - WAN including the Internet



Industry Leading SD-WAN Meets Industry Leading Platform



NEW

MX

Appliances

Cost-effective **gigabit**

SD-WAN branch connectivity

MX75



RECOMMENDED USE

Small branch

WAN PORTS

×1 Gigabit Ethernet SFP
×2 Gigabit Ethernet RJ45

FIREWALL THROUGHPUT

1Gbps

SITE-TO-SITE VPN THROUGHPUT

500Mbps

MX85



RECOMMENDED USE

Small-medium branch

WAN PORTS

×2 Gigabit Ethernet SFP
×2 Gigabit Ethernet RJ45

FIREWALL THROUGHPUT

1Gbps

SITE-TO-SITE VPN THROUGHPUT

500Mbps

MX95



RECOMMENDED USE

Medium-large branch

WAN PORTS

×2 10 Gigabit Ethernet SFP+
×2 2.5 Gigabit Ethernet RJ45

FIREWALL THROUGHPUT

2Gbps

SITE-TO-SITE VPN THROUGHPUT

800Mbps

MX105



RECOMMENDED USE

Large branch

WAN PORTS

×2 10 Gigabit Ethernet SFP+
×2 2.5 Gigabit Ethernet RJ45

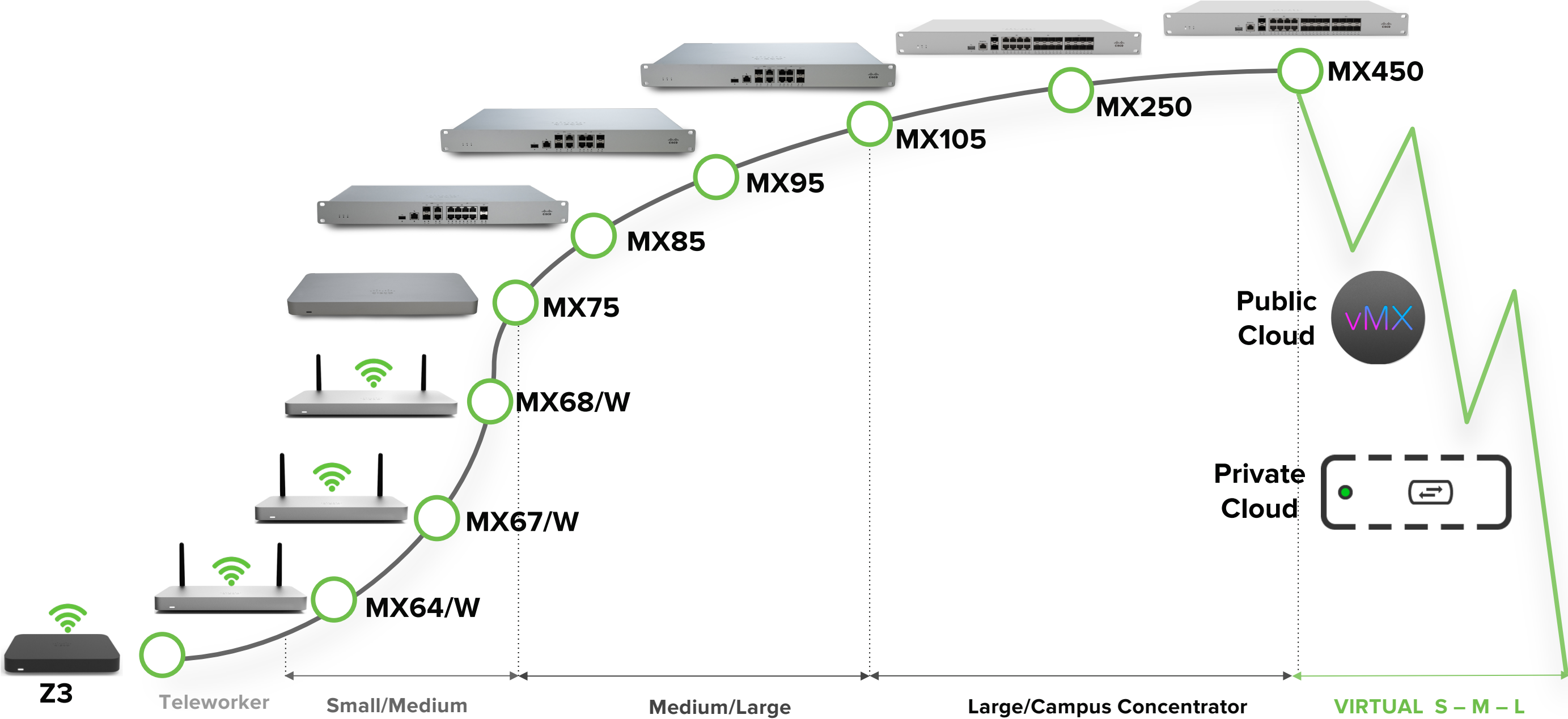
FIREWALL THROUGHPUT

3Gbps

SITE-TO-SITE VPN THROUGHPUT

1Gbps

SD-WAN & Security Appliance Product Line



Meraki SD-WAN - Build on Top of a Solid Architecture



Gerenciamento Centralizado



Zero Touch Deployment



Visibilidade & Relatório



Auto VPN Capability



Segurança



Meraki Insight APP & WAN Health



Serviços de Cloud Pública e Privada

Site-to-Site Auto VPN in Three Clicks



Meraki Auto VPN

The ability to configure site-to-site, Layer 3 IPsec VPN tunnels in just three clicks in the Cisco Meraki dashboard over any WAN link

Automatically configured VPN parameters

The Cisco Meraki dashboard uniquely acts as a broker between MXs in an organization, negotiating VPN routes, authentication and encryption protocols, and key exchange automatically to create hub-and-spoke or mesh VPN topologies

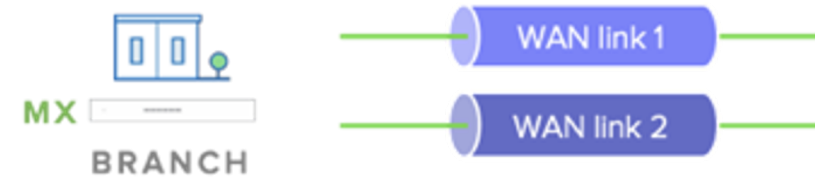
Redundancy built-in

MXs with two uplinks will automatically self-heal to re-negotiate VPN tunnels if a primary uplink goes down

Smart Path Selection

Dual Active VPN

Layer 3 IPsec tunnel em poucos cliques



Policy Based Routing

Roteamento do Tráfego baseado em Protocolo, Port, IP de Origem ou Destino, ou Aplicação Layer 7.



Dynamic Path Selection (PfR)

Seleciona o Melhor Túnel VPN para tráfego baseado em Performance do link.



Auto VPN tunnels

A License For Every Use Case

1:1 ratio of devices to licenses. Pair your chosen MX appliance(s) with the relevant license for your use case.



Enterprise

Essential SD-WAN features

Secure connectivity & basic security



All I need is Auto VPN and a firewall



Advanced Security

All enterprise features plus:

Fully featured unified threat management



I connect to the internet, so I need UTM security too



Secure SD-WAN Plus


All advanced security features plus:

Advanced analytics with ML
Smart SaaS quality of experience



My business relies on SaaS/IaaS/DC served apps

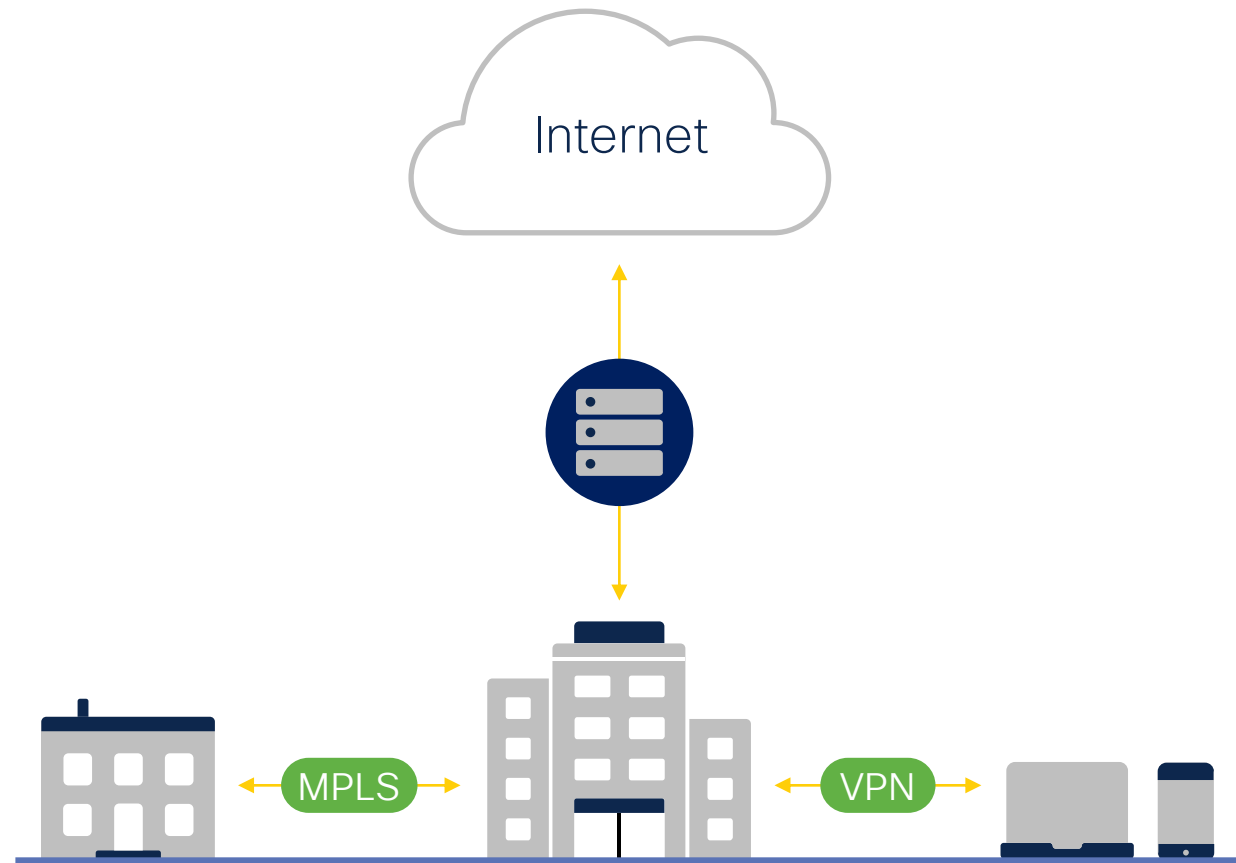
Secure **A**ccess **S**ervices **E**dge

 / 'sæsi /

A **consolidated** architectural solution that provides effective & homogenous levels of **security** and **experience** for users from anywhere on any device.

Network Transformation

Before



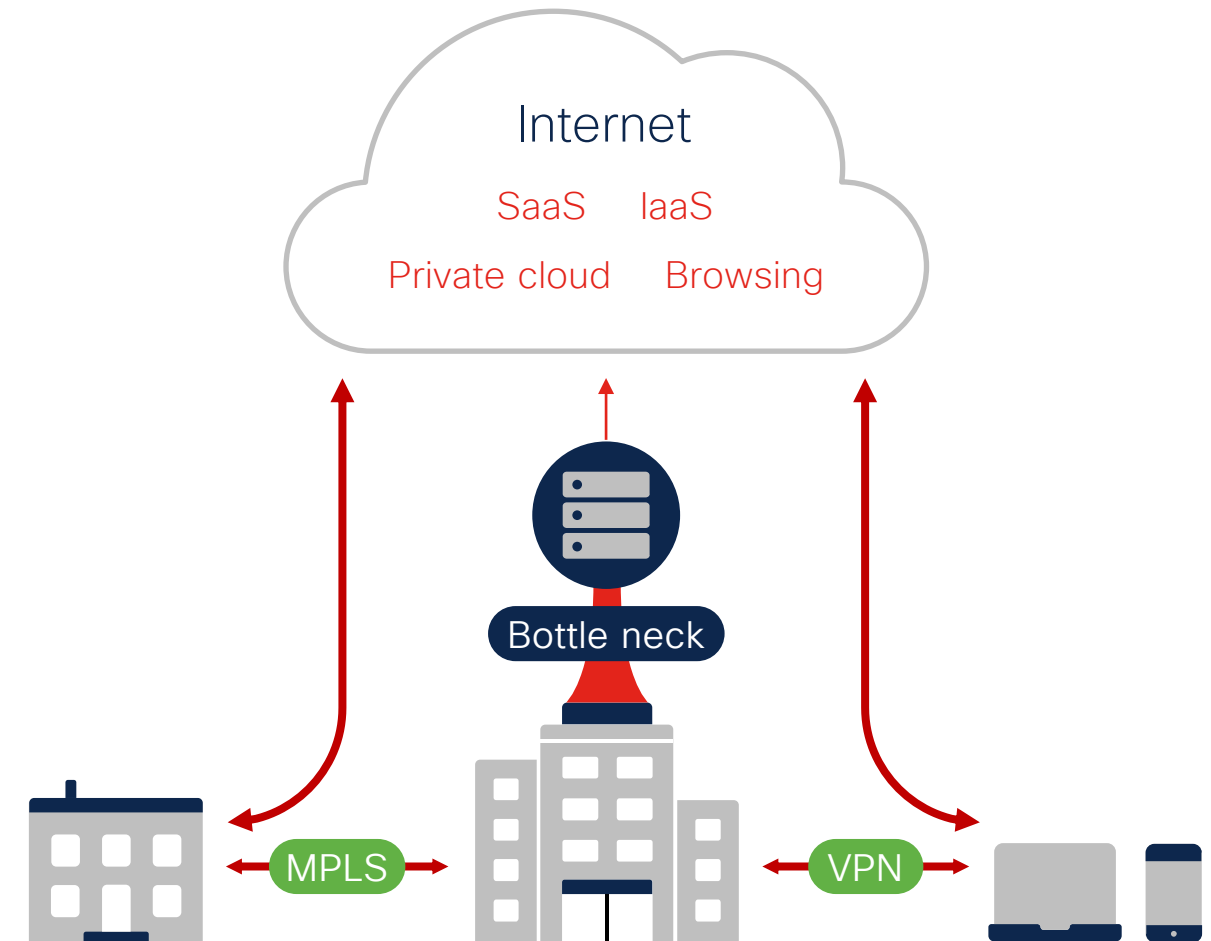
Apps: Hosted in datacenter

Users: Connected to corporate network to work

Network: Centralized

Security: On-premises security stack

What's changed



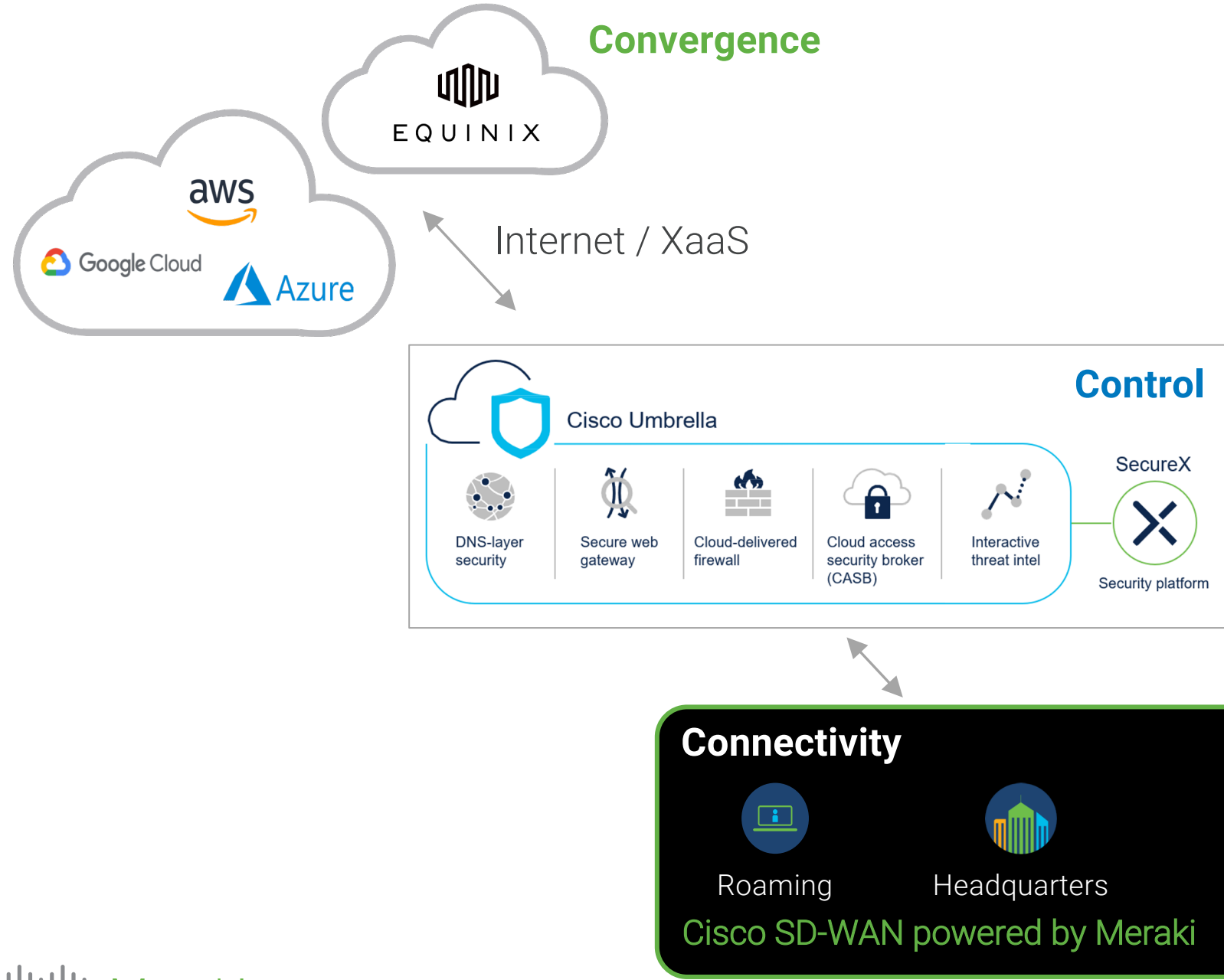
Apps: More hosted in the cloud

Users: More work done off-network

Network: De-centralized

Security: Gaps in protection

Your bridge to SASE

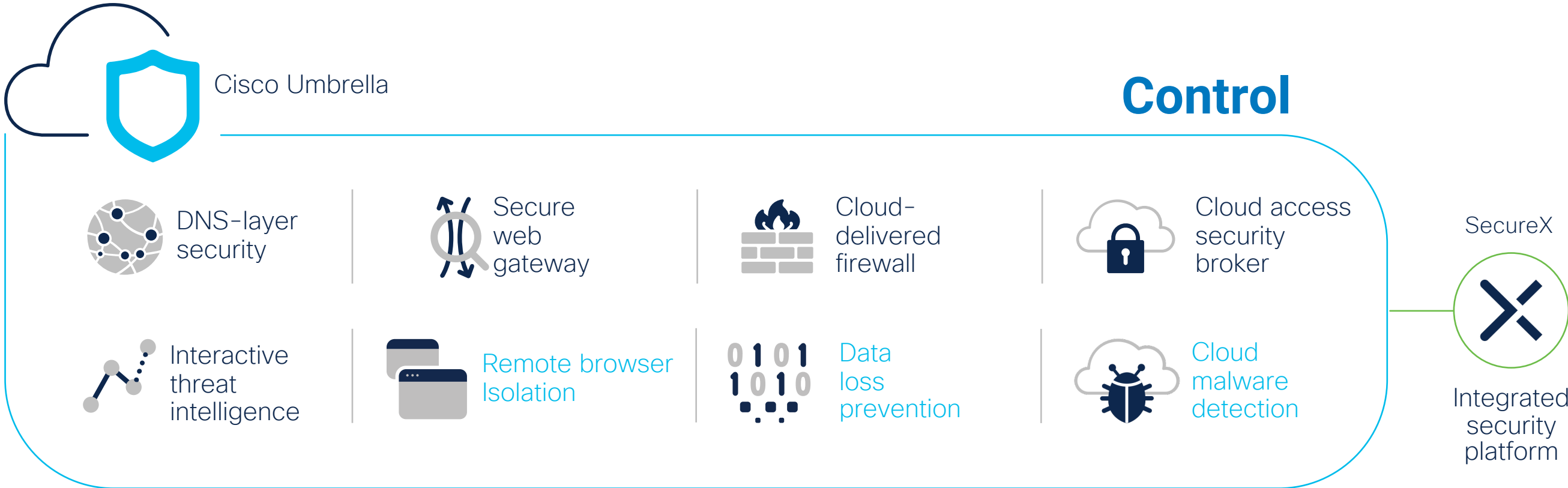


Cisco: Proven leader in networking and security

- Protect 100% of the Fortune 100
- #1 in cybersecurity market share
- \$1B in cloud-native security investments

Cisco Umbrella

Control



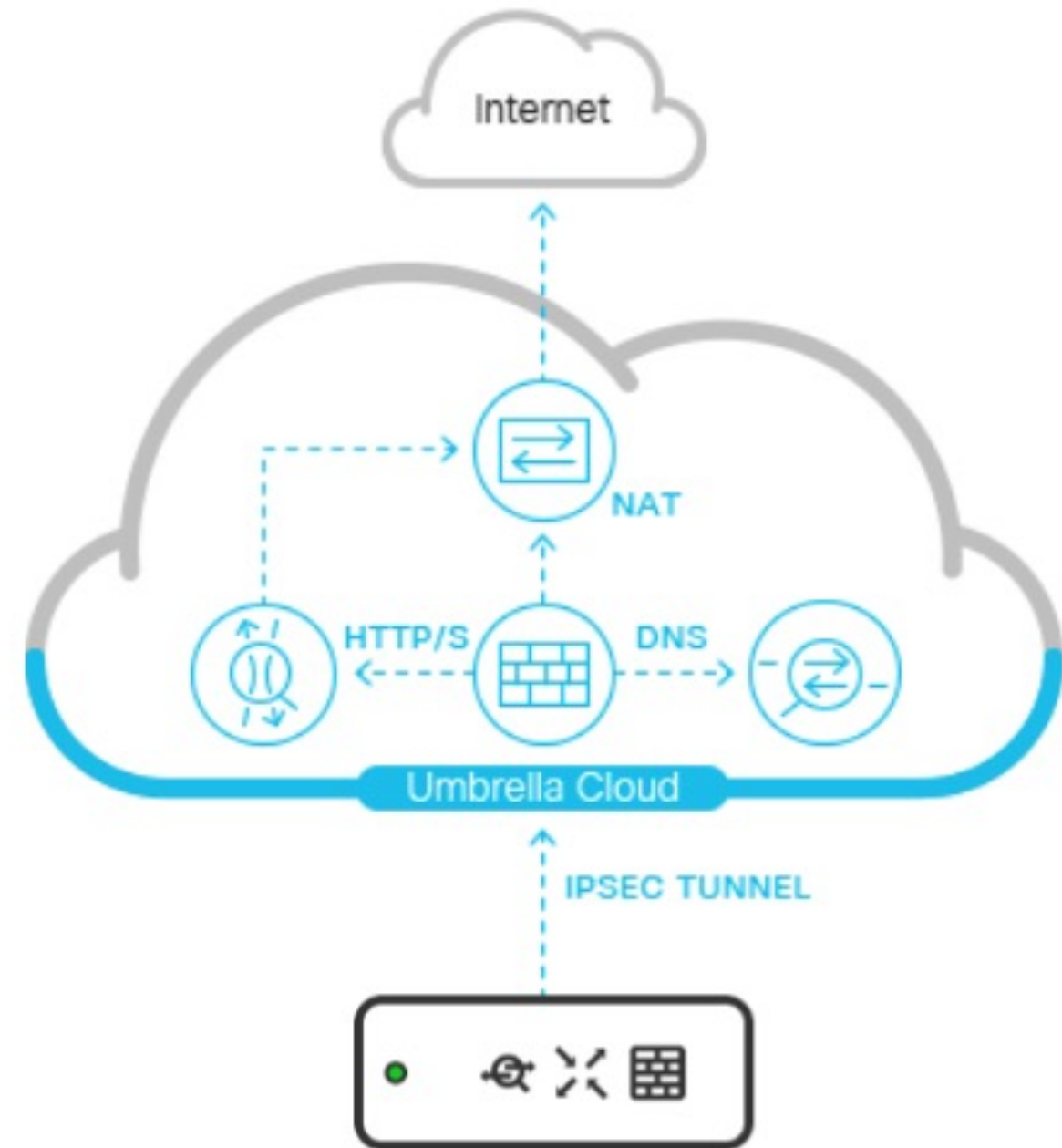
Cisco Umbrella

- **TUNNEL:**

Umbrella SIG between the Umbrella dashboard and a Meraki MX Security and SD-WAN device.

- **TRAFFIC:**

All internet-bound traffic will be forwarded to Umbrella SIG through an IPsec tunnel for inspection and filtering.

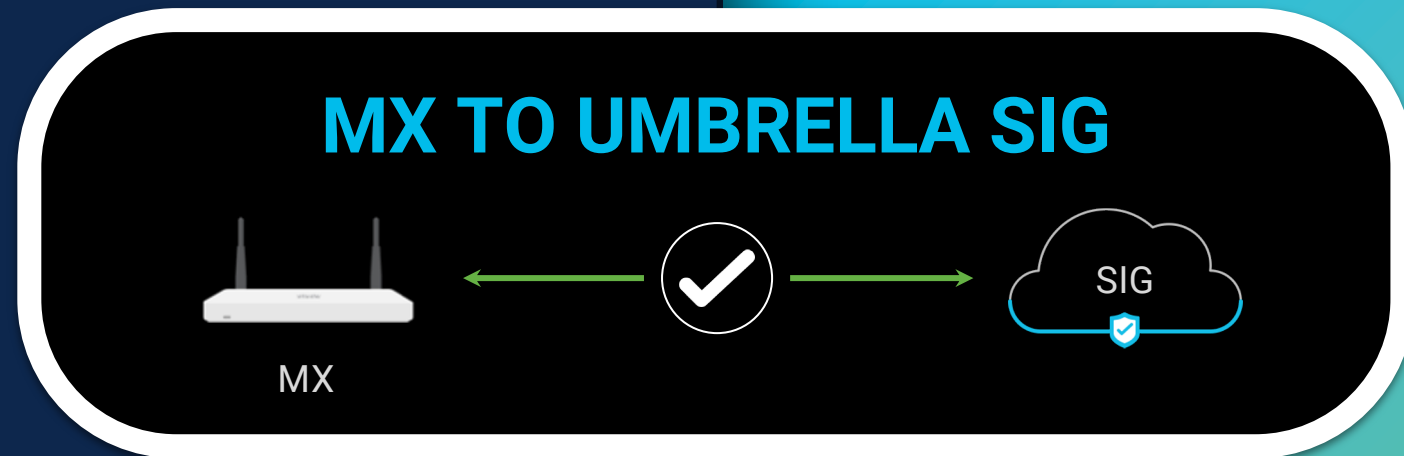


PHASE I

PHASE II

PHASE III

Future



- Send business critical traffic to Umbrella SIG using MX

Available
TODAY

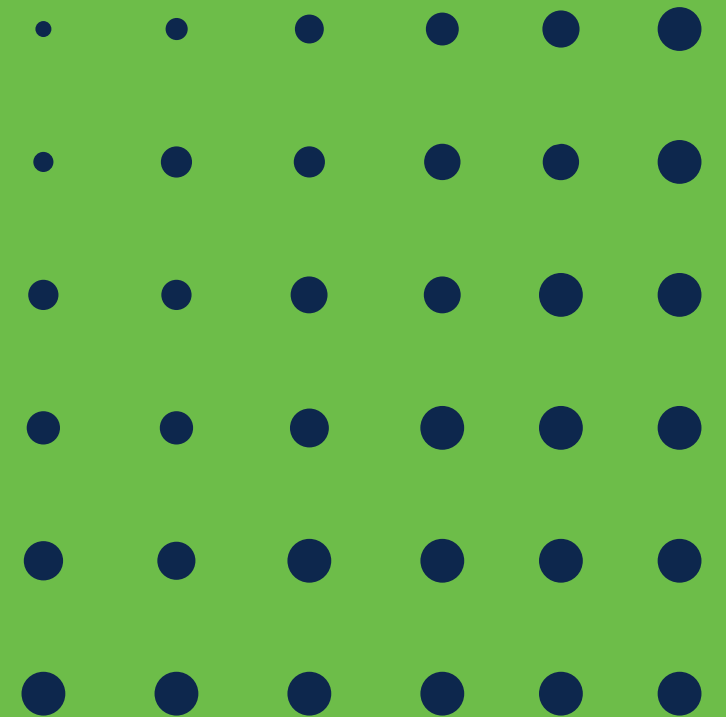
- Integrate Umbrella SIG into the SD-WAN fabric
- Limited Availability

Available
TODAY



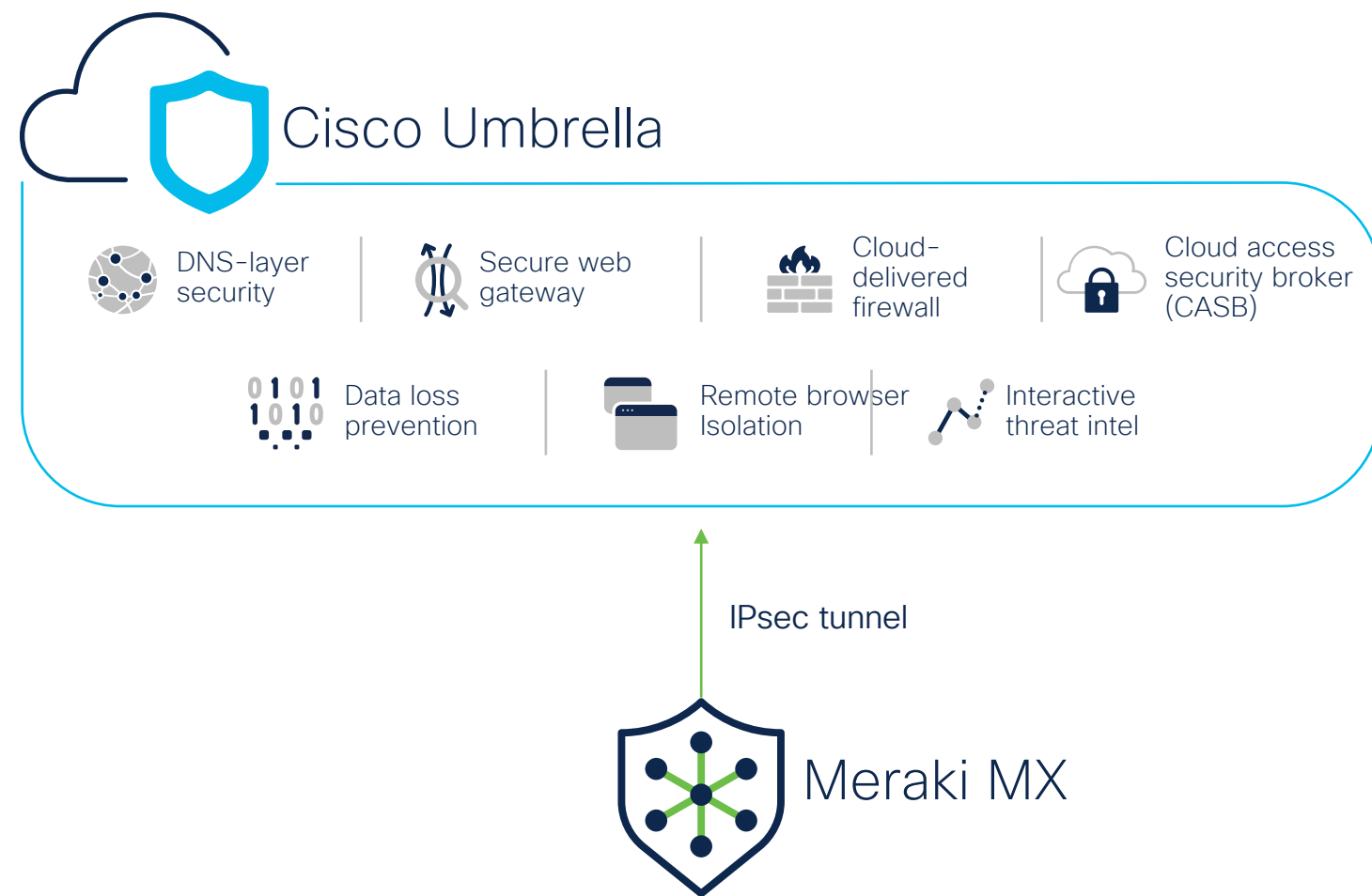
- As-a-service
 - Delivery
 - Consumption

Phase I Tunnel IPSec IKEv2



Phase I: Simplified IPsec tunnel connectivity with Meraki MX

- Flexible security options (DNS or more advanced SIG capabilities)
- Quickly create IPsec tunnels from Meraki MX devices to Umbrella through the Meraki dashboard and user interface
- Easily forward all outbound traffic to Umbrella for advanced inspection and control of web and app traffic without on-premises hardware limitations
- **Future proof!** Easily migrate to SD-WAN in the future



Regions: All the regions
Brasil: Rio de Janeiro and Sao Paulo

Phase I: IPsec tunnel technical details

IPsec capacity

- 250 Mbps per tunnel, ongoing development to increase capacity

Availability

- Umbrella-defined primary, secondary DCs
- Failover to secondary DC and DR is handled by **anycast**
- Failure detection uses IKE DPD
- Available in all SIG datacenters globally

Firmware

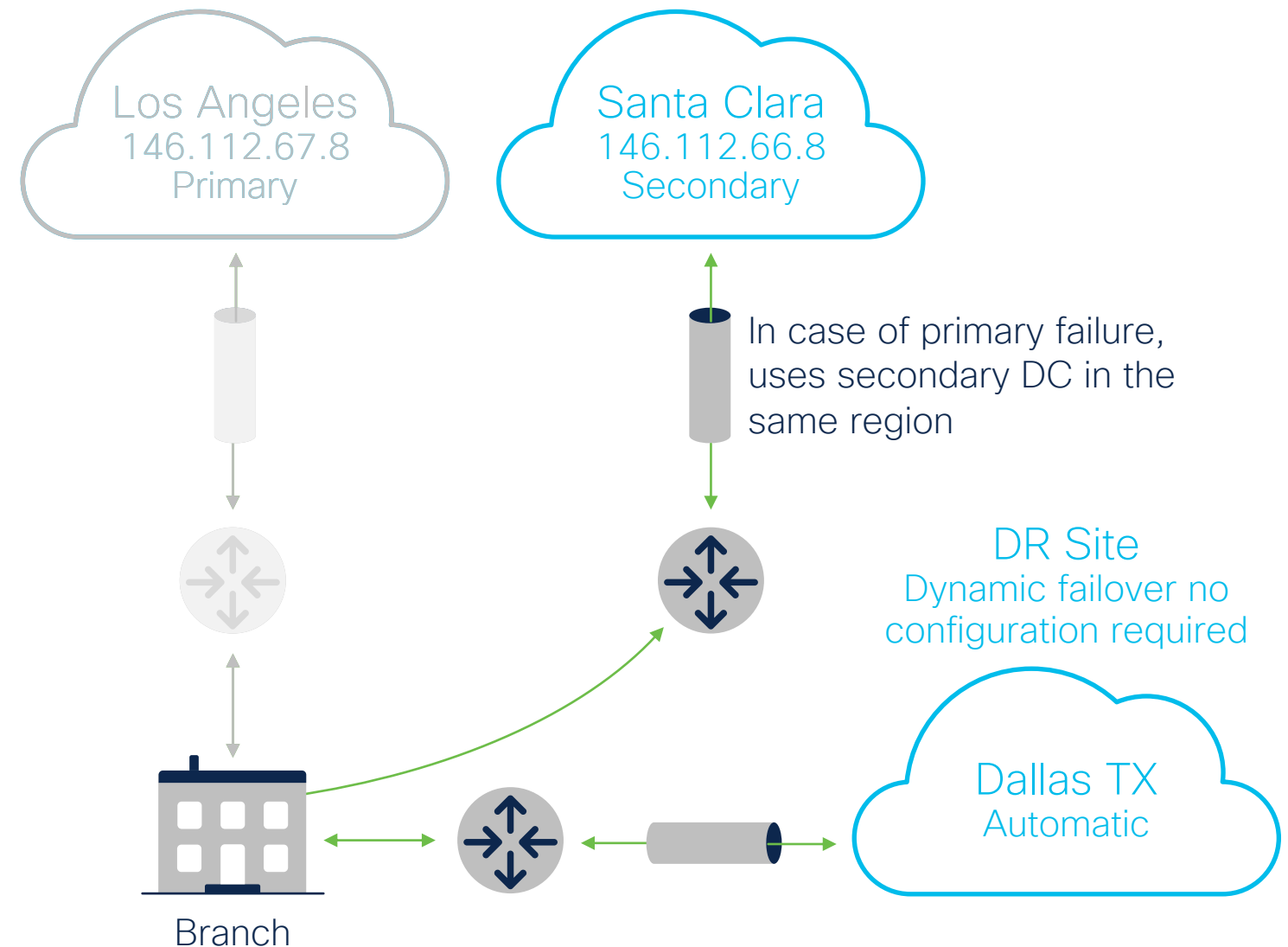
- Requires MX15+ Firmware

Licensing

- Requires Umbrella SIG license + any MX license tier

Example

Data center region code US-1



Phase I: How to

- Create Umbrella tunnels
 - Specify different credentials for each instance to tunnel
- Create Meraki IPsec tunnels

Umbrella Dashboard

Set Tunnel ID and Passphrase

To add a tunnel so that you can configure your firewall, you need a Tunnel ID and Passphrase. For more information, see [Network Tunnel Configuration »](#)

Tunnel ID

Test-SIG-MX2 @*****.com

Passphrase

.....

✓ 16 - 64 characters, at least 1 uppercase and 1 lowercase letter, 1 numeral, no special characters

Confirm Passphrase

.....

✓ Passphrases match

Meraki Dashboard

Organization-wide settings

Options in this section apply to all VPN peers in this organization.

Non-Meraki VPN peers ⓘ

Name	IKE Version <small>BETA</small>	IPsec policies	Public IP	Local ID	Remote ID ⓘ	Private subnets	Preshared secret	Availability ⓘ	Actions
SIG1	IKEv2 ▼	Umbrella	146.112.82.8	TEST-SIG-MX1@2365:		0.0.0.0/0	SIG x	⊕ X

[Add a peer](#)

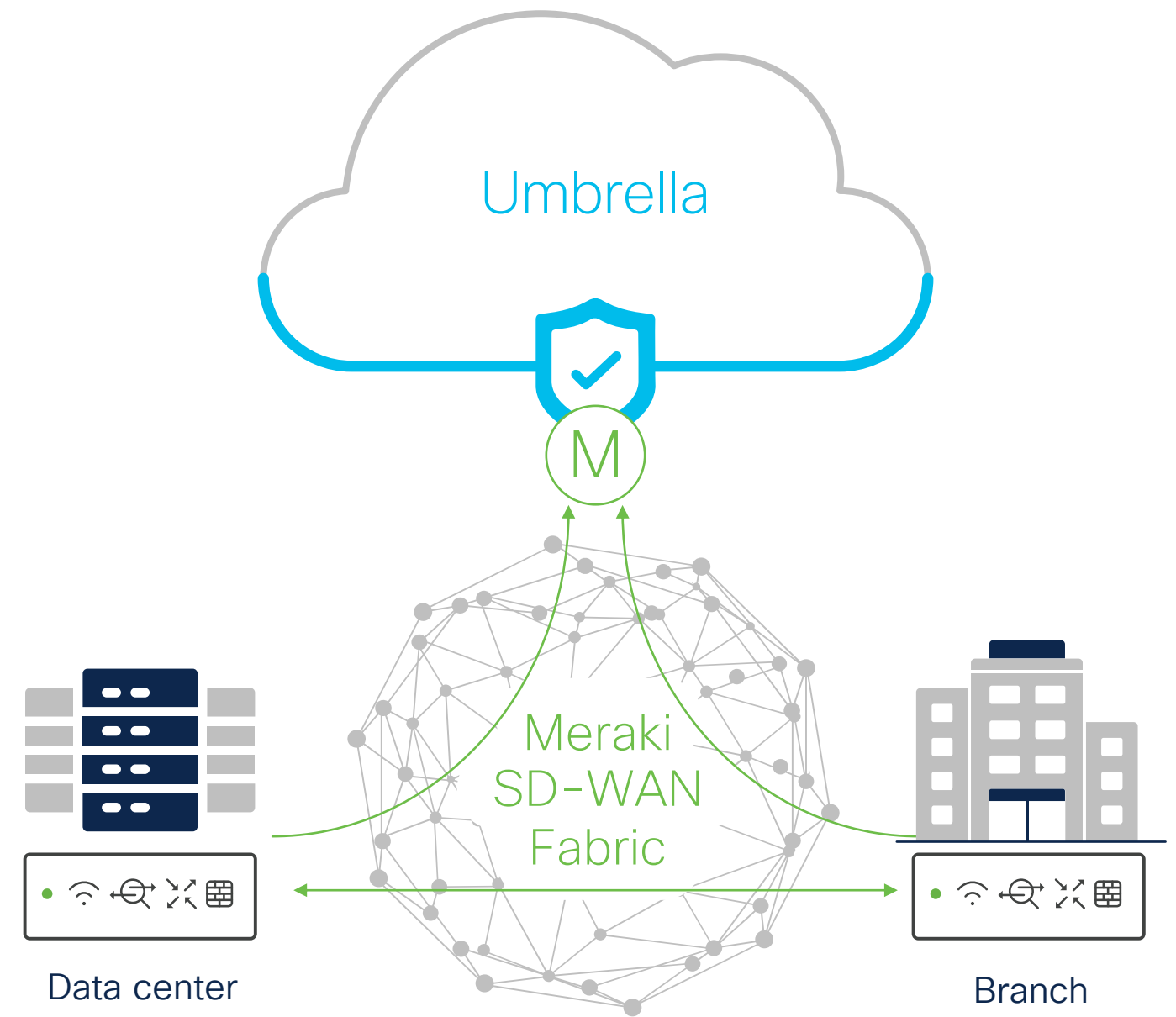
Phase II

Meraki SD-WAN Fabric



Phase II: Extend Meraki's SD-WAN into the Umbrella cloud

- Meraki SD-WAN directly to Umbrella with Auto VPN
- Flexible security options (DNS or more advanced SIG capabilities)
- Native SD-WAN traffic engineering
- New Meraki Umbrella SD-WAN Connector will enable SD-WAN fabric for more intelligent path selection with zero cost!



Regions: Los Angeles, New York City, Tokyo, Sydney, London, Paris, Frankfurt.

Phase II: SD-WAN Connector Capabilities

UMB-SIG SD-WAN Connector

- 250 Mbps per UMB-SIG connector, ongoing development to increase capacity
- Multiple UMB-SIG connectors can be deployed to support higher capacity
- Supports VPN exclusions for DIA

Availability/HA

- Customer-defined primary and secondary DC
- Failover to secondary DC is handled by the Meraki SD-WAN fabric
- Initially available in select SIG DC's globally

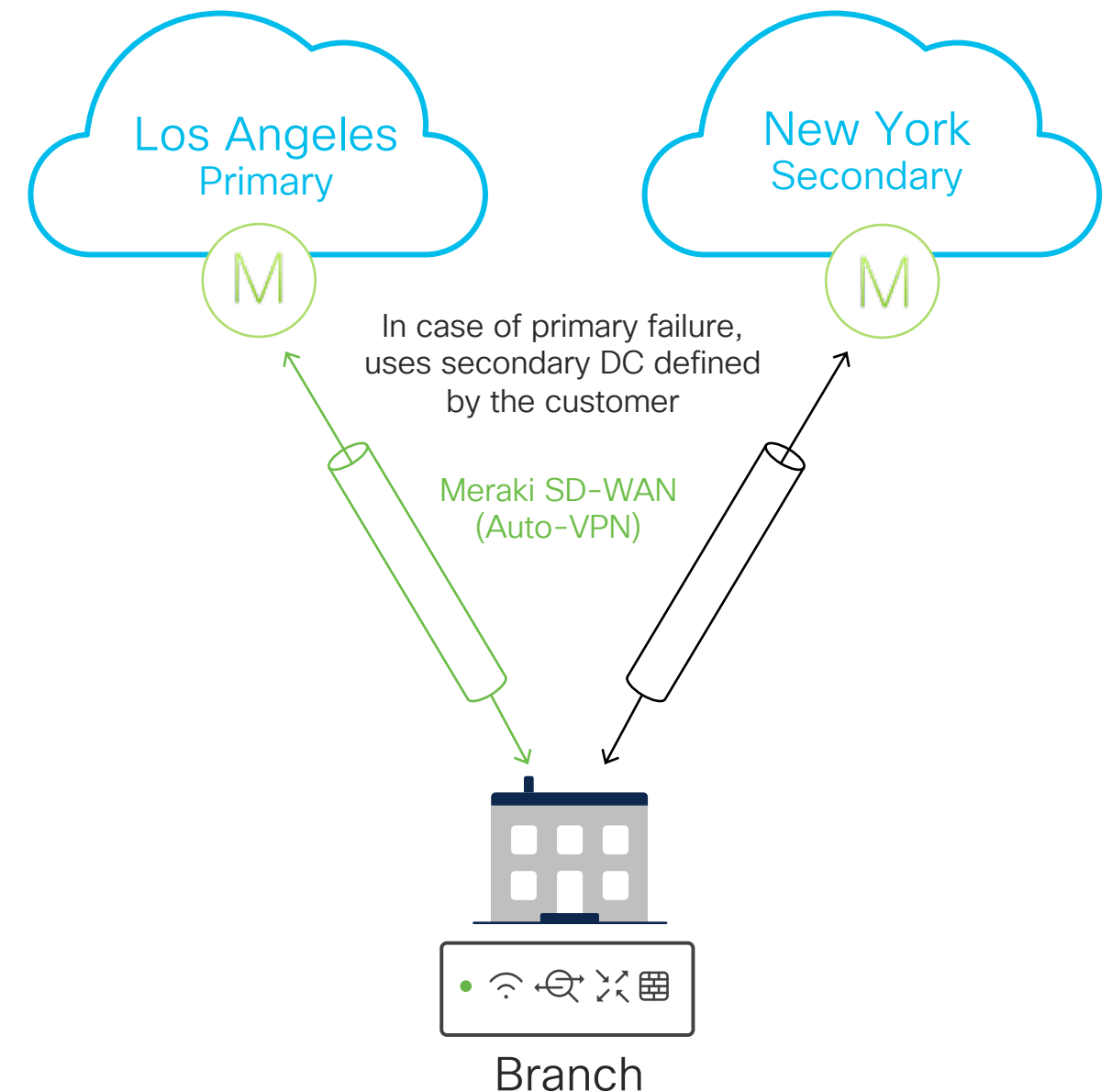
Firmware

- Requires MX14+ Firmware

Licensing

- Requires Umbrella SIG licensing + any MX license tier

Example



Phase II: How to

- API Integration
- Define relevant HUBs
- Establish Auto VPN tunnel to Umbrella

New Deployment: Umbrella SD-WAN Connector

Network name

Choose primary datacenter

Choose secondary datacenter

Casos de Uso DEMO



Cassio Gomes
Technical Solutions Architect

Use case: Secure edge

CORE ELEMENTS

- ▶ Cloud security
- ▶ MX SD-WAN appliance
- ▶ Z3 teleworker gateway
- ▶ MI Observability

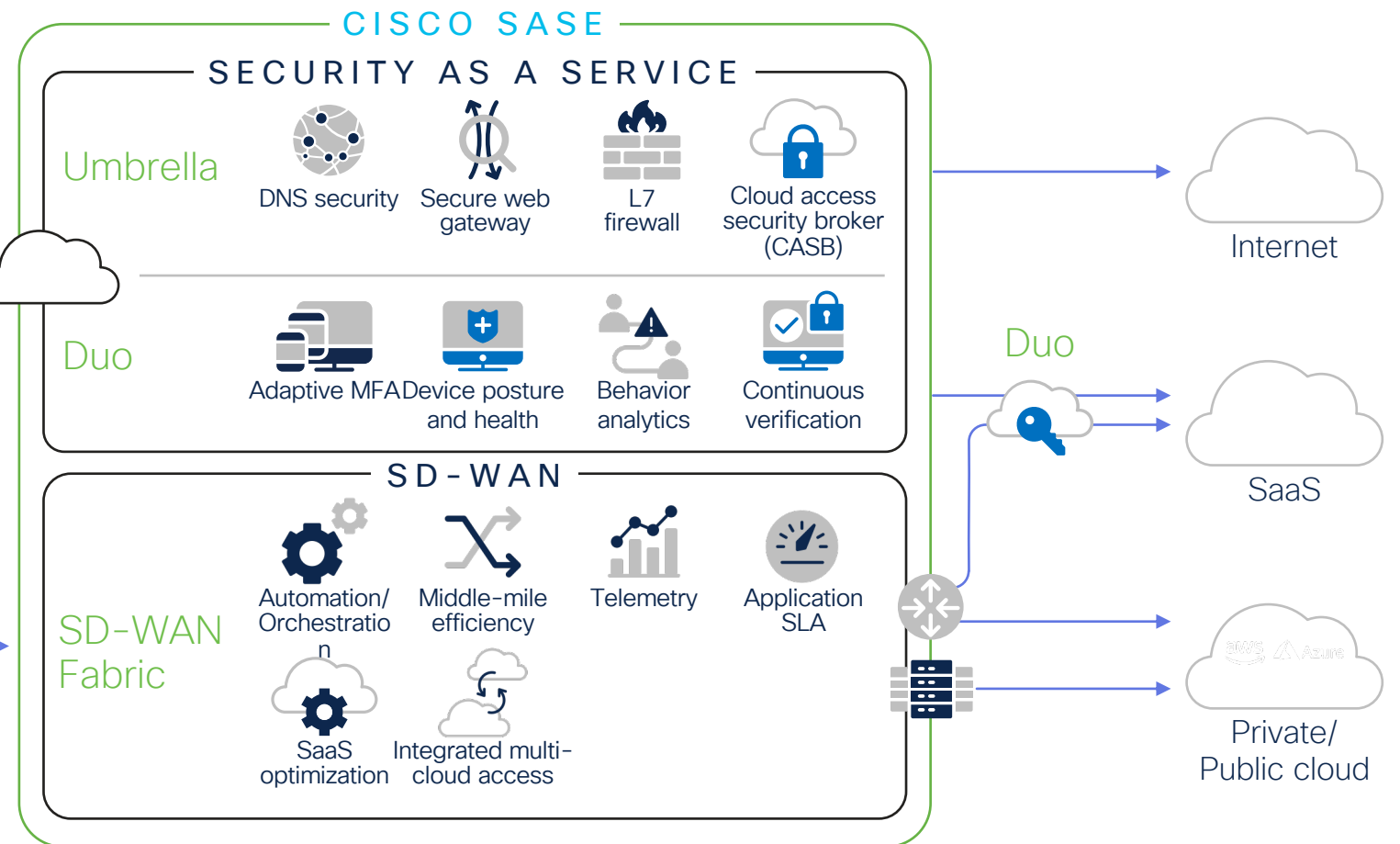
Meraki Insight



Umbrella tunnel

SD-WAN router

SD-WAN mesh



Connect

- Provide software defined transport from any network edge (Whole office, office of 1, HQ)
- Encrypted transport to SASE for direct internet access
- Dynamic path selection via SD-WAN fabric
- App aware Intelligent path selection through telemetry exchange between SDWAN and O365

Control

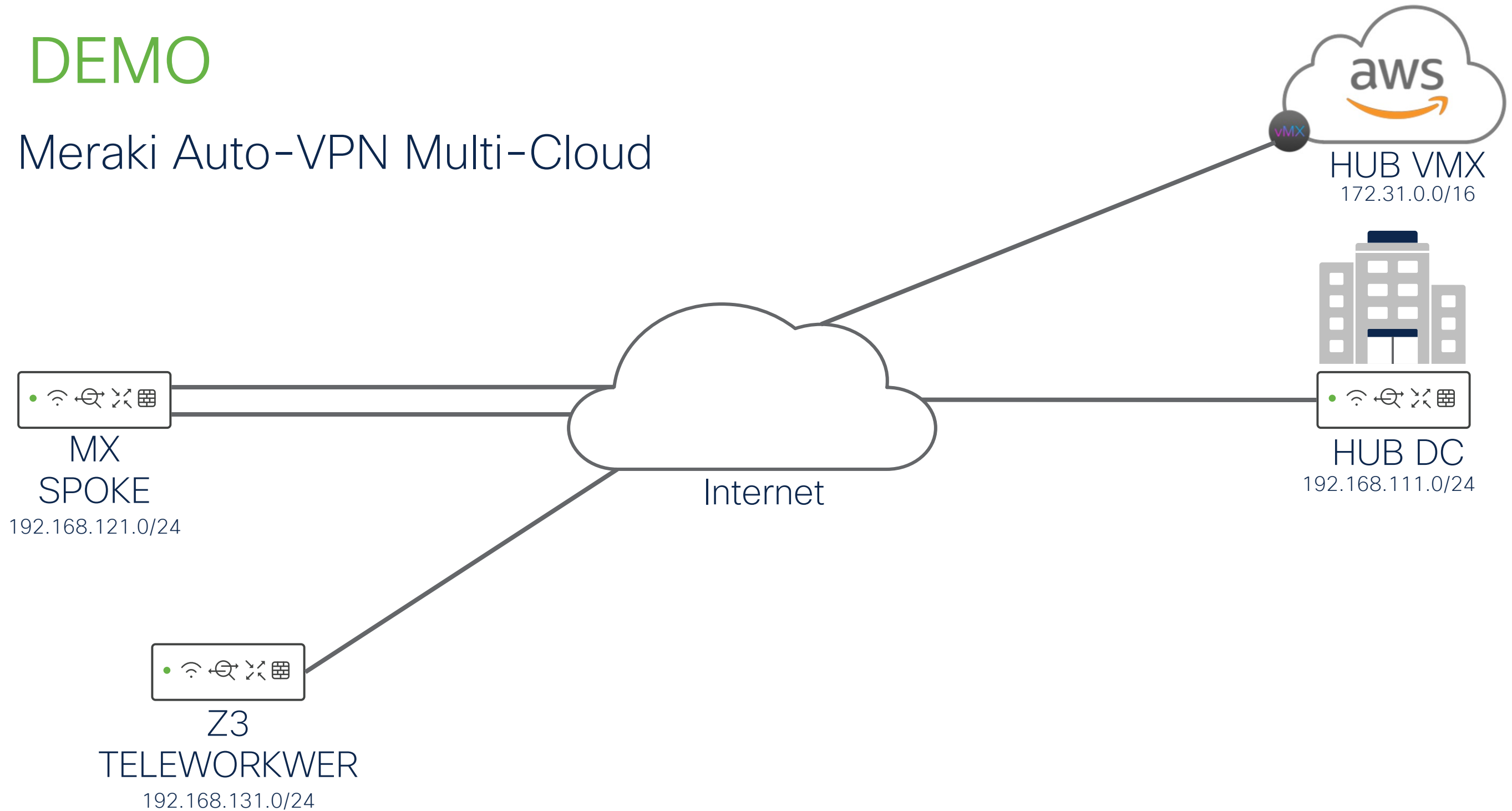
- Cloud security stack to secure all outbound traffic to internet/SaaS
- Establish zero trust application access for user/device

Converge

- Simple, fast deployment of network and security
- Zero touch provisioning
- Common cloud-delivered security policy
- Automate response across network diameter with SecureX
- Common observability into all networks and services with Meraki Health and Meraki Insight

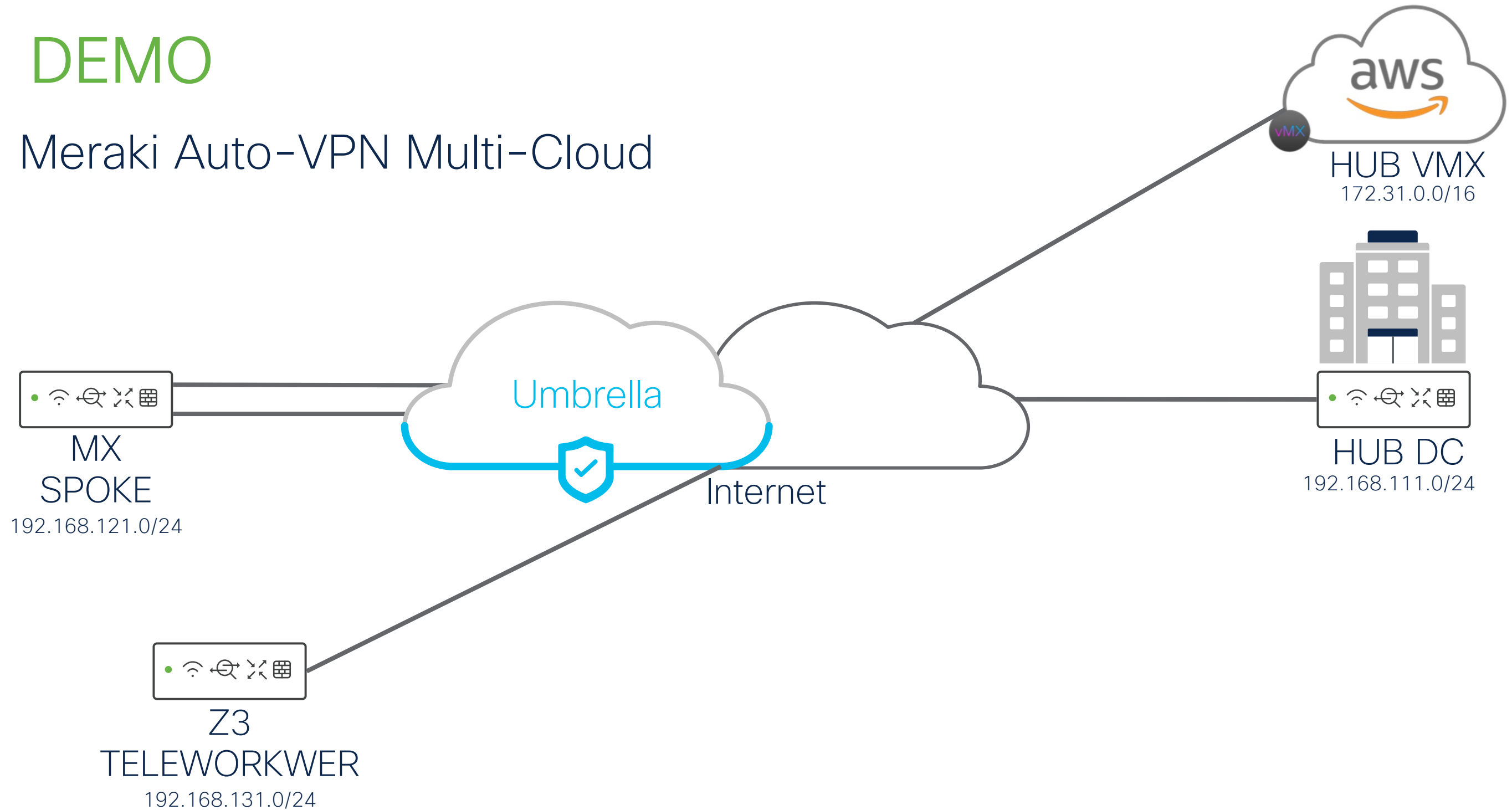
DEMO

Meraki Auto-VPN Multi-Cloud



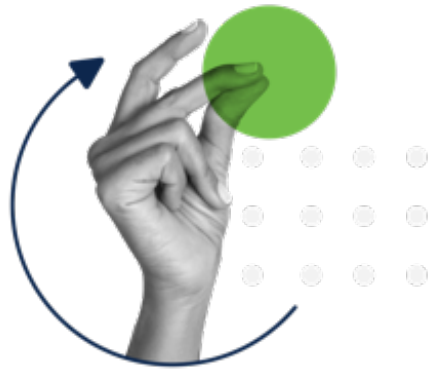
DEMO

Meraki Auto-VPN Multi-Cloud



Meraki MX and Cisco Umbrella integration

A simple and flexible way to deploy Umbrella across MX devices



Simple

- Fast protection of users across your distributed network with simple, flexible deployment options
- Higher security efficacy with less effort and less resources



Secure

- Multiple layers of security from a single, cloud-native service
- Flexible policy enforcement for any use case
- Off-network protection using Umbrella without a VPN
- Continuous protection with automatic failover



Scalable

- Consistent high-performance security for multi-cloud demands
- SSL decryption at a scale not possible with on-prem hardware

OBRIGADO
THANK YOU