



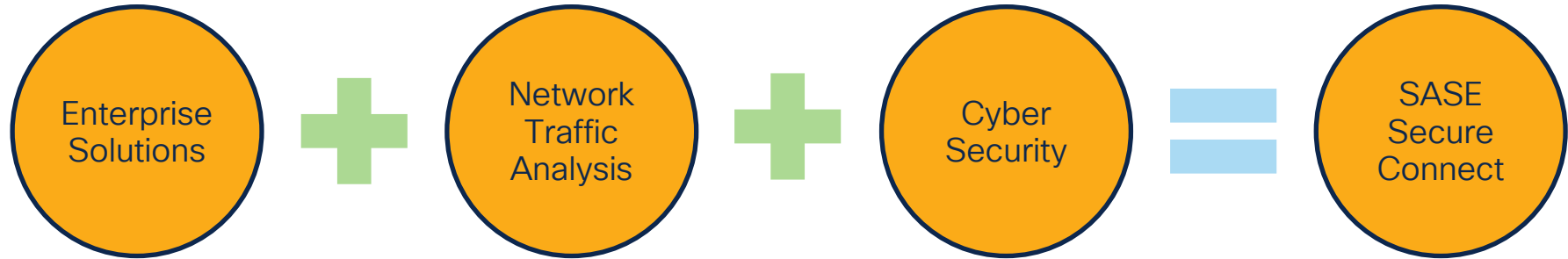
Building Resilient SASE Solutions with Secure Connect

Ana Andrijic - Technical Marketing Engineer
BRKMER-2577

CISCO *Live!*



Why Am I Here ?





On a scale of 1 to 5, how
familiar are you with
SASE architecture?

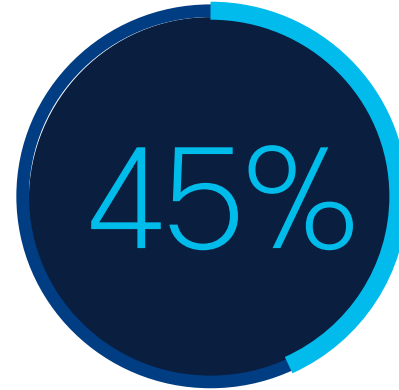
ⓘ Start presenting to display the poll results on this slide.

Strategic Planning Assumption by Gartner

By end of 2027 ...



70 % enterprises will
establish new roles
focused on IT resilience



Boost end-to-end
reliability, tolerability and
recoverability by 45%

*“The ability of a system to recover quickly and **maintain functionality** during and after a disruption, such as a **failure, attack, or unexpected event.**”*

ChatGPT

Secure Connect Resiliency Principles



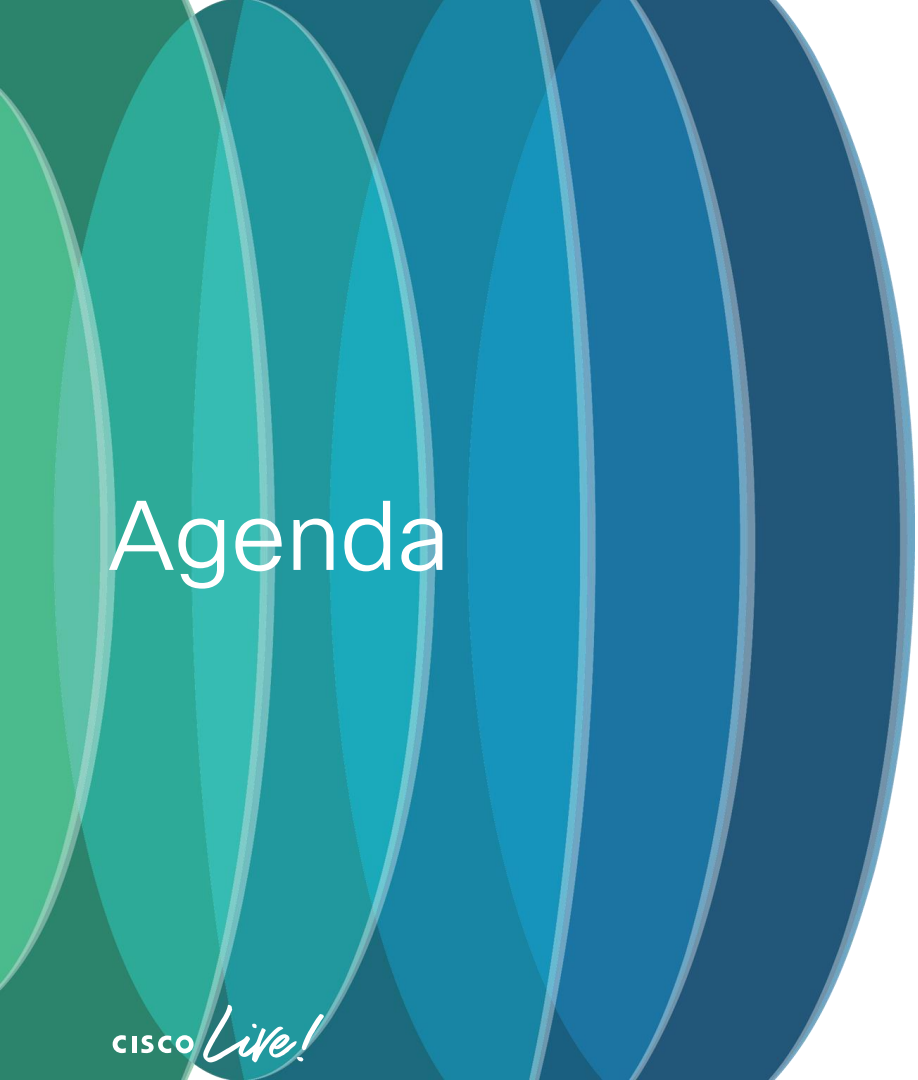
Network High Availability



Security Everywhere



Complete Visibility



Agenda

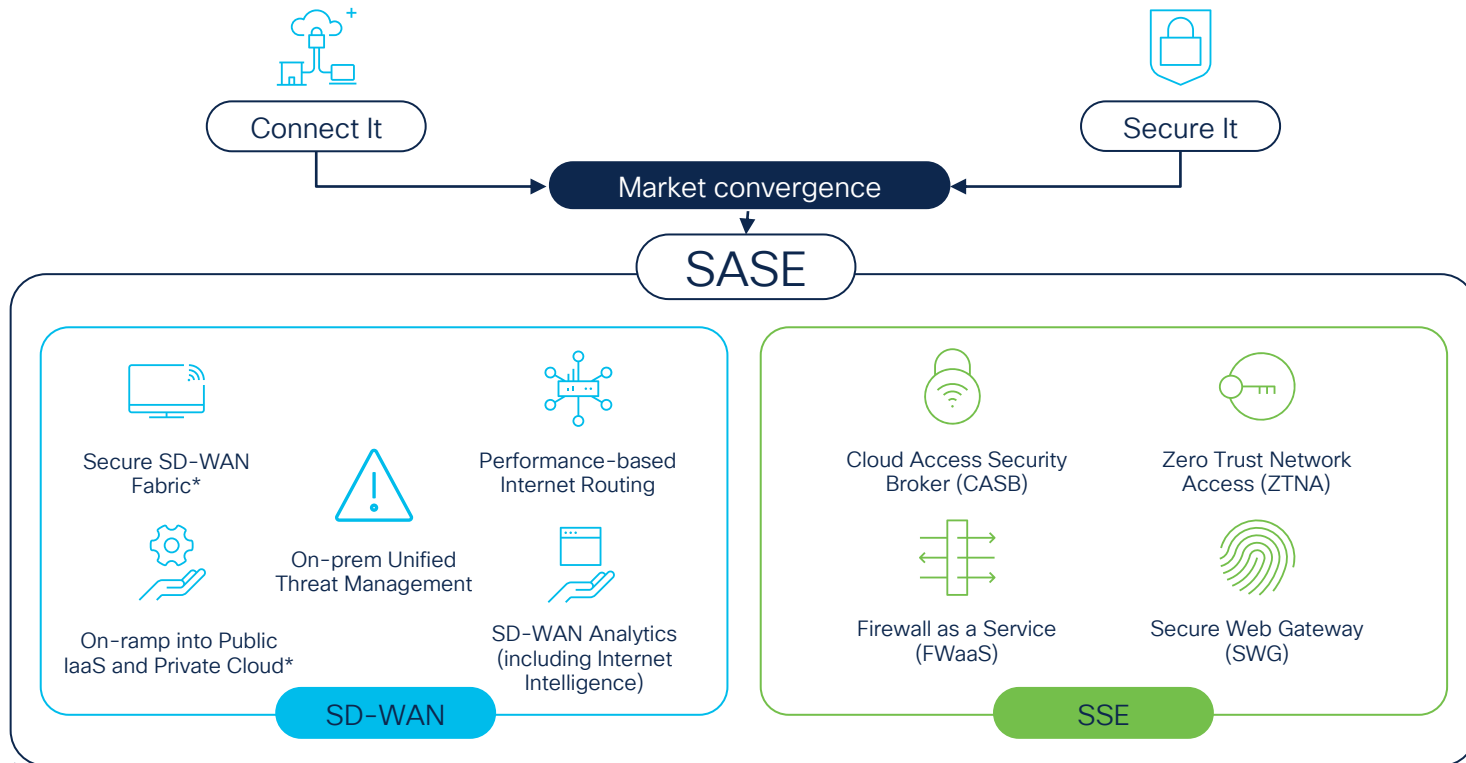
- Secure Connect
- Network High Availability
- Security Everywhere
- Digital Experience Monitoring
- Conclusion

Secure Connect

Secure Access Service Edge (SASE) Architecture

Network as a service

Network security as a service



Secure Connect Use Cases

Secure Private Access

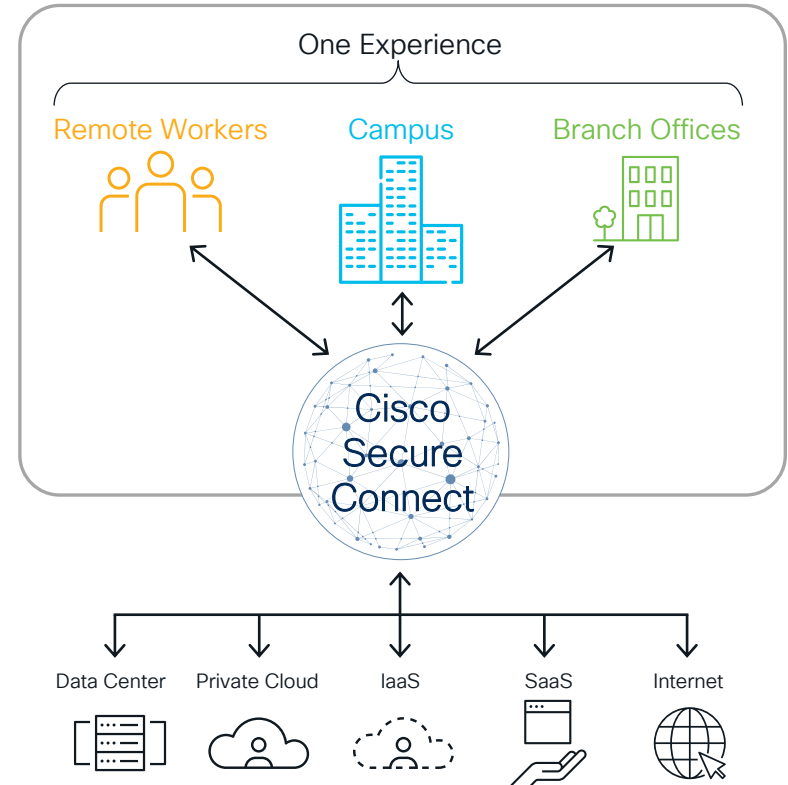
- Deliver secure access to company resources in private data centers or in the private cloud

Secure Internet Access

- Provide users with safe access to the internet and cloud applications from anywhere
- Block malicious activity and threats

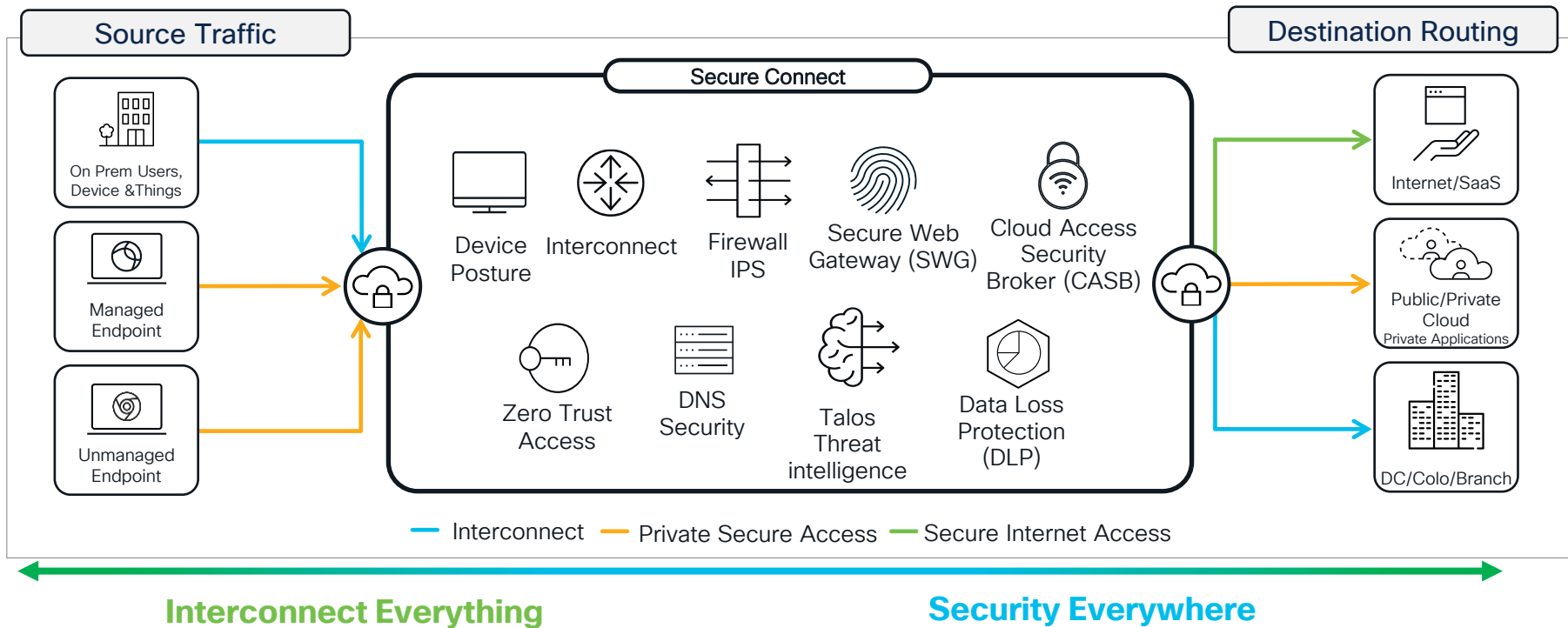
Interconnect Sites

- Dramatically simplify architecture and configuration by interconnecting everything to the SASE fabric



Secure Connect Architecture

Meraki Dashboard

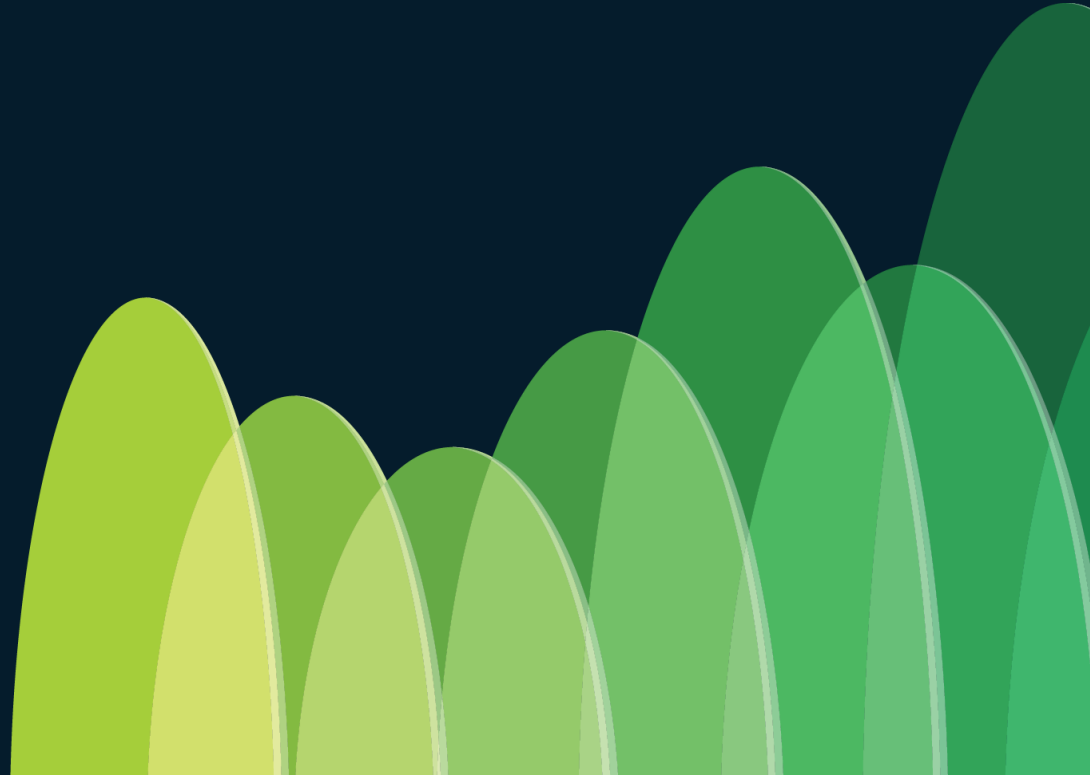


Digital Experience Monitoring

ThousandEyes

CISCO Live!

Network High Availability

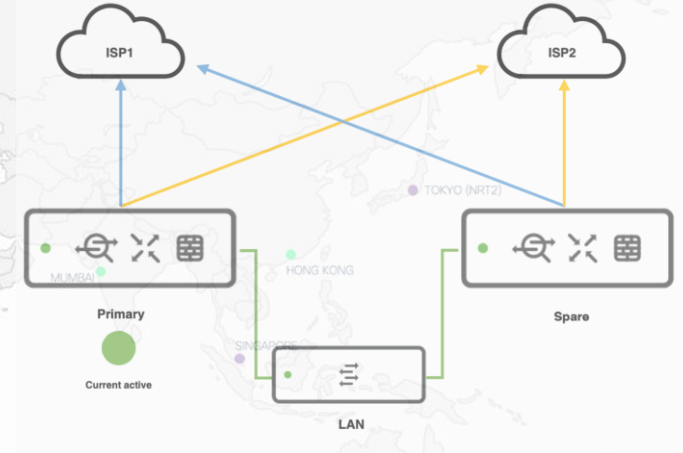


What is Network High Availability

- Redundancy
- Failover mechanisms
- Load Balancing
- Geographic distribution

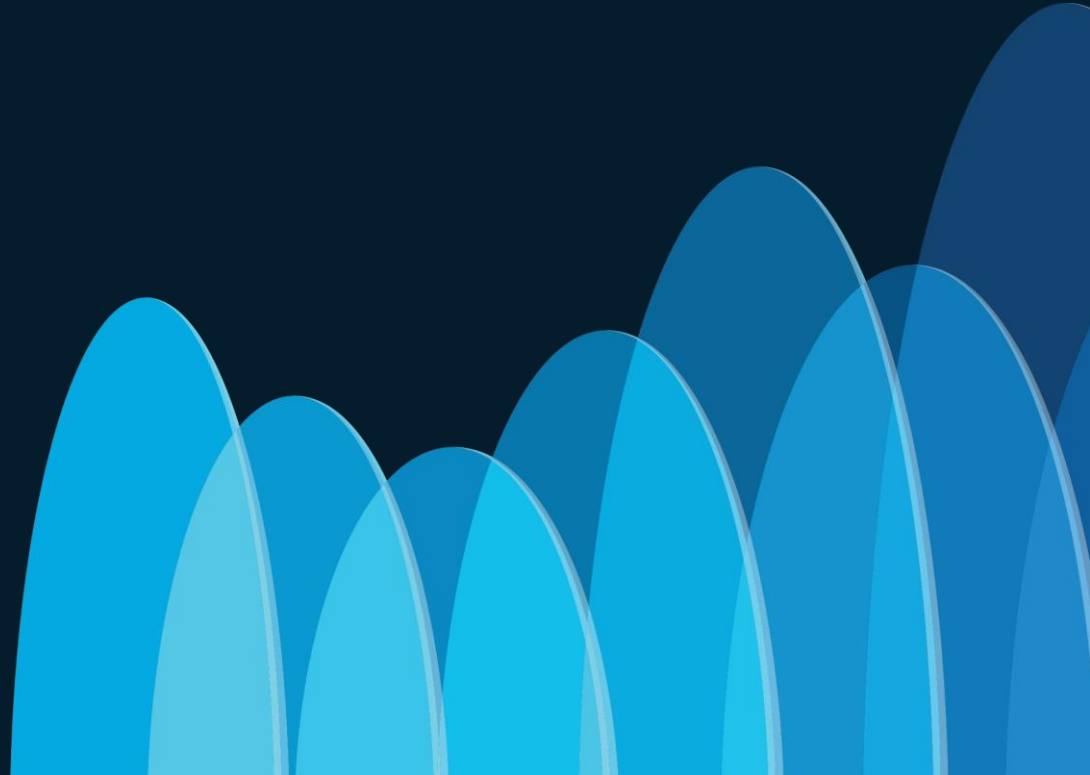
Available Services

- Secure Connect Complete and Foundation
- Secure Connect Foundation
- Disaster Recovery

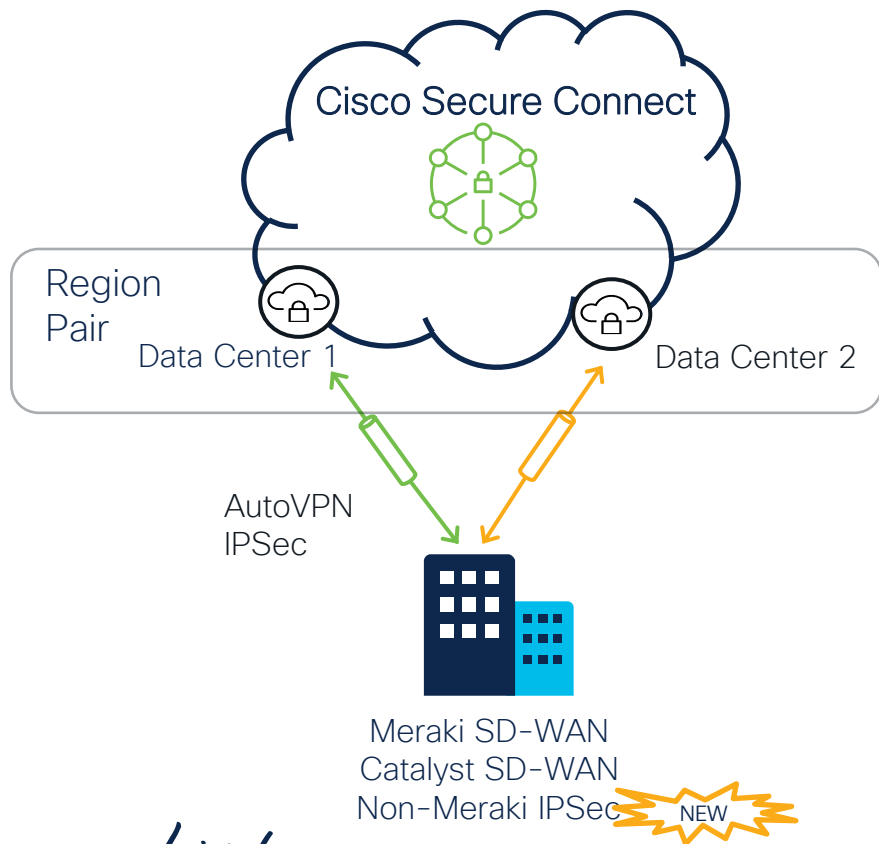


Sites Integration

Interconnect: Behind the
Curtains



Secure Connect Sites



- Built-in High Availability
- Adjustable Primary and Secondary tunnel
- Static (IPSec) or dynamic BGP routing
- Regional sync across Data Centers pairs

-  Primary Secure Tunnel
-  Secondary Secure Tunnel

Dual Data Center Failover Mechanism

- Failover is immediate with tunnel failure
- BGP failover based on hold timer and size of routing table
- BGP convergence lower downtime from 2:30 min to 30 sec
- BGP optimization with summary routes (in progress)

Non-Meraki IPSec Sites



	Prior Nov 2024	Post Nov 2024
Configuration	SD-WAN -> VPN + Umbrella	Secure Connect -> Sites
Bandwidth	250 Mbps	500 Mbps
Termination point	SLVPN	Cloud Native Head End
Redundancy	Single Tunnel	Dual Tunnel to DC region pair
Routing	Static	Static or dynamic

Attaching IPSec Site

Secure Connect > Sites

+ Add Site ▾

Manage

Meraki networks

Cisco SD-WAN app h

Non-Meraki IPSec tunnels

1

Configure site

Configure initial settings for t

Site name

cat8k DC

10 character limit

Device Type

Catalyst IOS-XE (Autonomous mo... ▾

Region

Europe-1 ▾

2

Device Type

Catalyst IOS-XE (Autonomous mo... ^

Cisco ASA

Cisco ISR

Cisco FTD

Catalyst IOS-XE (Autonomous mode) ✓

Others (Third-Party Device, Private Cloud)

Region

Select Region ^

US West

US Northeast

US Central

US Southeast

US Midwest

Europe-1

Europe-2

Europe-3

Europe-4

Asia-1

Australia-1

Brazil-1

Canada-1

4

cisco *Live!*

BRKMER-2577

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

19

Configure tunnels and Routing

Tunnel ID Format

☒ Email ☐ IP Address

5

Tunnel pair name

cat8k-DC

Passphrase

[Blurred passphrase]

Cancel

Static or dynamic routing

☒ Dynamic routing (BGP) ☐ Static routing

AS number

65217

6

Data for peer tunnel setup

Tunnel 1

Tunnel ID

cat8k-DC@: [REDACTED] -
umbrella.com

Secure Connect DC IP

155.190.214.2

Passphrase

[REDACTED]

Tunnel 2

Tunnel ID

cat8k-DC@: [REDACTED] -
umbrella.com

Secure Connect DC IP

155.190.212.2

Passphrase

[REDACTED]

Configure these details in vManage for BGP peering to Secure Connect

AS

64512

Neighbor Peer IP 1

169.254.0.9

Neighbor Peer IP 2

169.254.0.5

!!! Peer Tunnel IPs should must be 169.254.0.10 and 169.254.0.6 !!!

Complete Site Integration

Physical or Virtual
(vMX)
Private or Public Cloud

Meraki SD-WAN
Catalyst SD-WAN
Non-Meraki IPsec

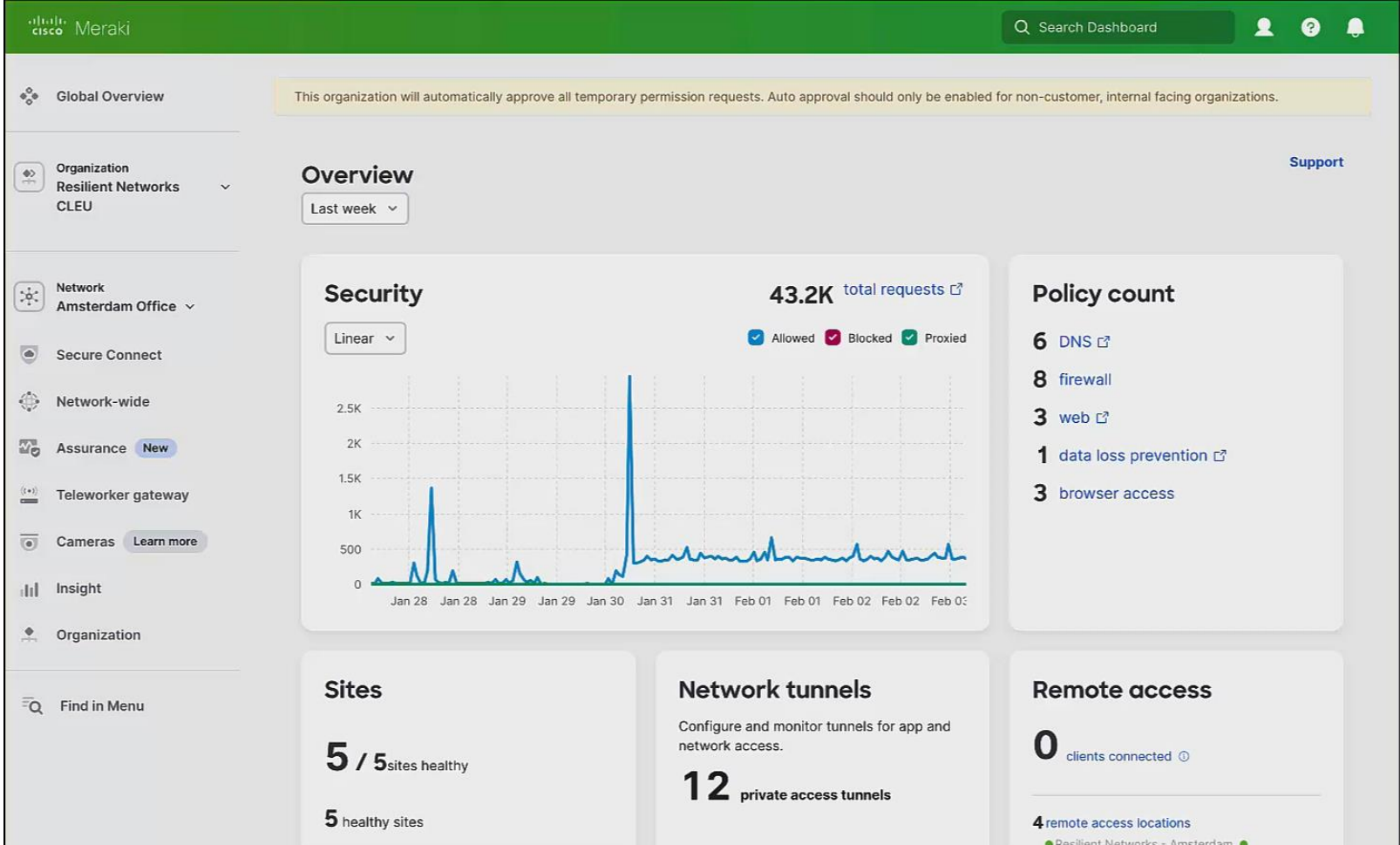
Hub or Spoke

Status for all sites

Site name	Region / Cloud Hub	Site Features	Connectivity ⓘ
✓ London Office 208	Europe-1 Region	Meraki network Spoke	
✓ cat8k DC	Europe-1 Region	IPsec Site Private Access	
✓ Amsterdam Office	Europe-2 Region	Meraki network Spoke	
✓ AWS vMX Connector	Europe-1 Region	Meraki network Hub	
✓ Azure vMX Connector	Europe-2 Region	Meraki network Hub	

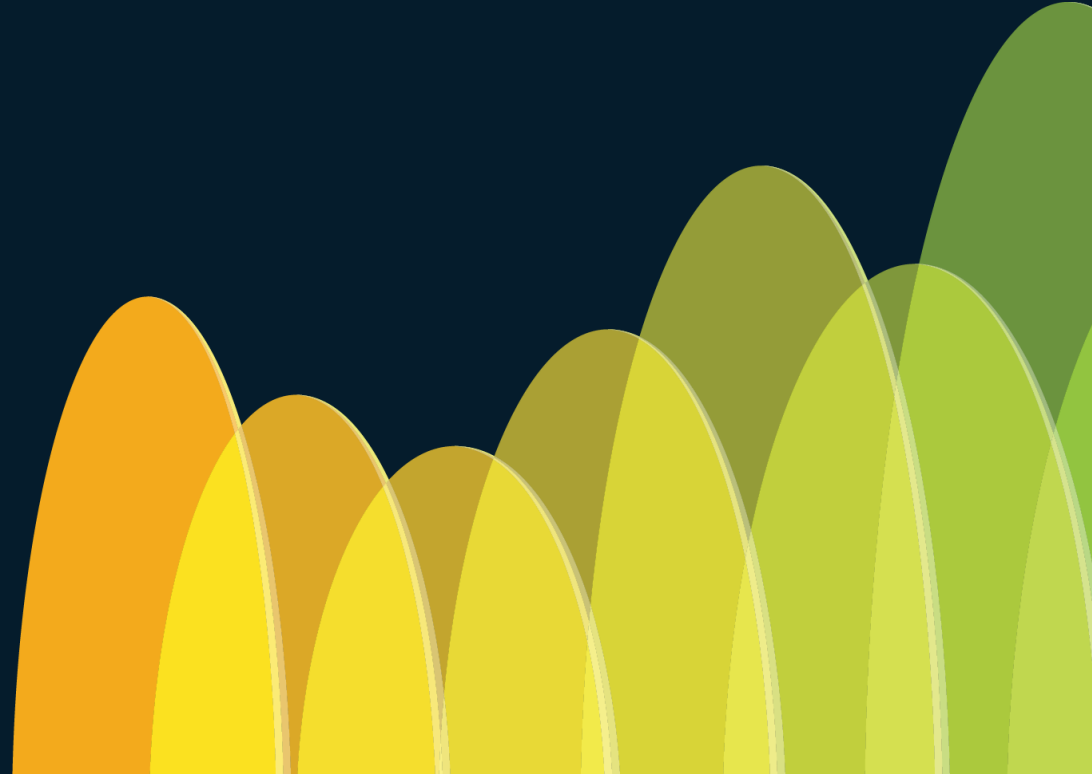
Adding Sites Demo



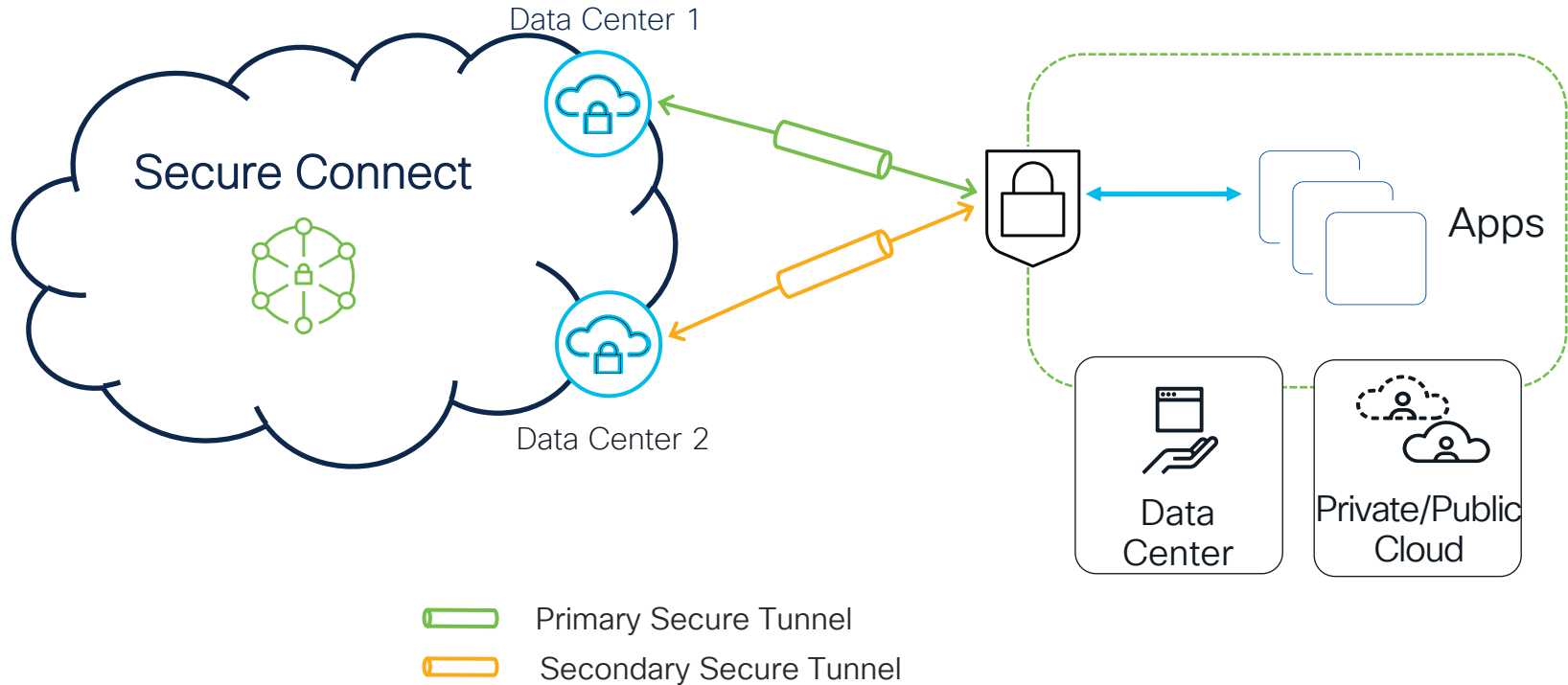


Multi Cloud

Auto VPN vMX

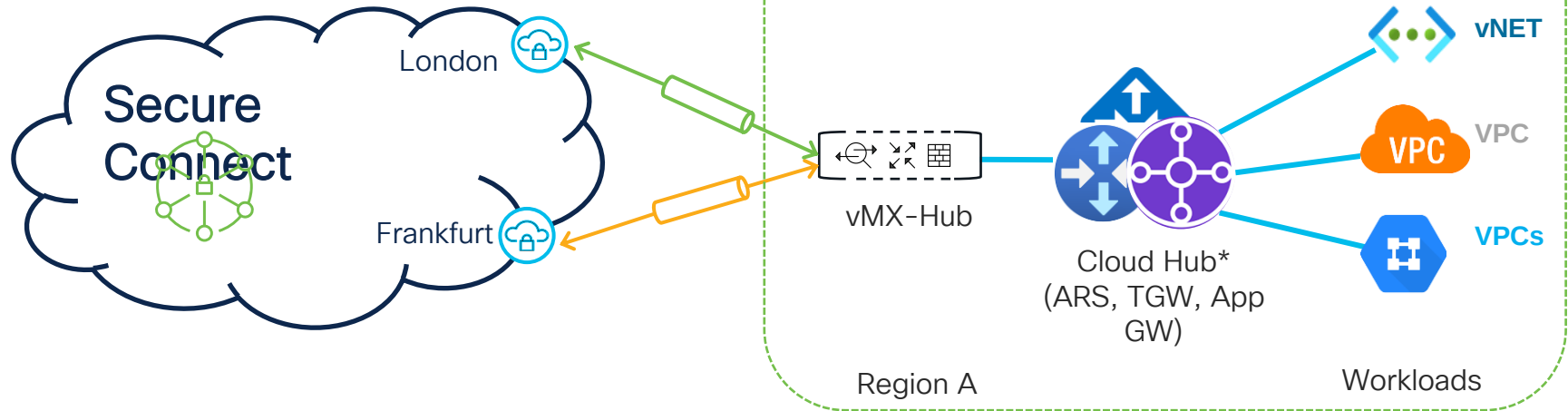


Private Resources & Applications



Public Cloud Deployment with vMX

- Redundant Auto VPN connection
- Passthrough or routed mode (default)
- Static or BGP routing support

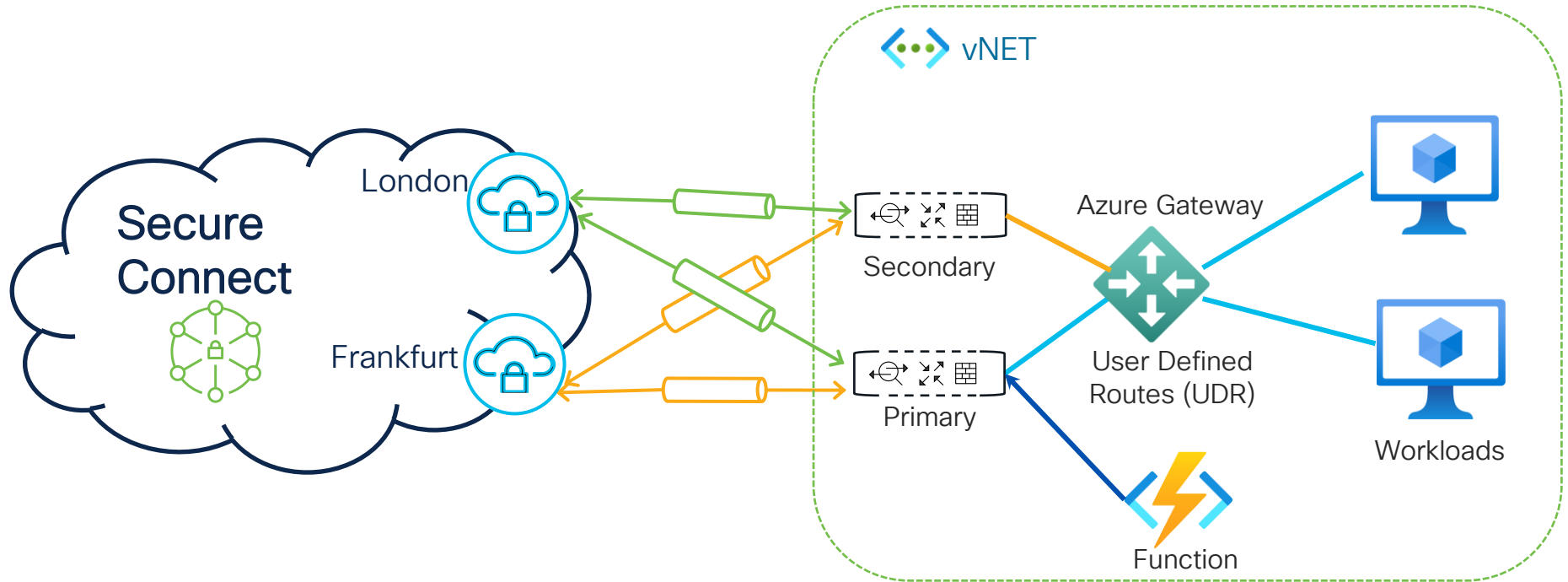


* Intra VPC routing via Cloud Hubs (AWS Transit Gateway or Azure Route Server or Azure Functions)

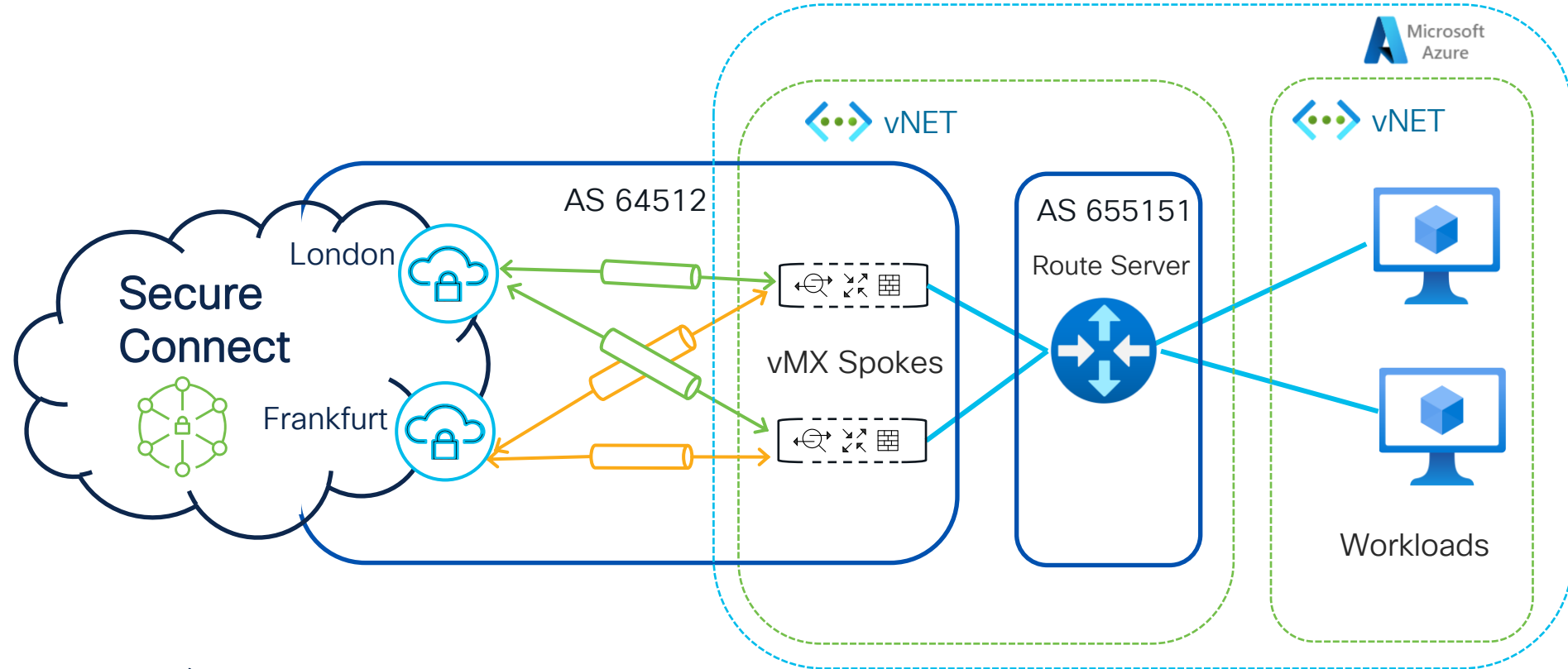
vMX Resiliency in the Cloud

- Organizational security compliance (Organization Policy)
- Auto failover for redundancy
- Automated firmware upgrade

Active-Passive Deployment in Azure



Dual vMX Deployment in Azure



Cloud Deployment Steps

- Must have valid vMX license
- Create Meraki Network
- Deploy vMX to an existing vNET/VPC with network token
- Create Route Table, Transit Gateway or Route Server

Cloud Integrations: Simplified Deployment

- Zero touch deployment
- Must have valid vMX license
- Integrate with AWS account
- Deploy vMX to an existing VPC
- Routed mode by default

Cloud Integrations – Meraki Dashboard

Organization > Cloud Integrations

Account title	Provider	Added	Updated	Deployments	
AWS TME	 AWS	Nov 20, 2024	Nov 20, 2024	2	 

Cloud Integrations

Deployments

Cloud accounts

Q Search

2 deployments

+ Add Deployment

Instance name	Provider	VMX type	Instance type	Instance ID	Region
ResilientNetwork	 AWS	VMX-S	c5.large	i-02aa8c1d935ff68e1	Europe (London)
ResilientNetwork2	 AWS	VMX-S	c5.large	i-0442808a917446597	Europe (London)

Cloud Integration Demo

CISCO *Live!*



Global Overview

Organization
Resilient Networks
CLEU

Network
Amsterdam Office

Secure Connect

Network-wide

Assurance New

Teleworker gateway

Cameras Learn more

Insight

Organization

Find in Menu

This organization will automatically approve all temporary permission requests. Auto approval should only be enabled for non-customer, internal facing organizations.

Cloud Integrations

Deployments Cloud accounts

3 deployments
+ Add Deployment

Instance name	Provider	VMX type	Instance type	Instance ID	Region
DEMO CLEU	AWS	VMX-S	c5.large	i-0b16954345e4f87b7	Europe (London)
ResilientNetwork	AWS	VMX-S	c5.large	i-02aa8c1d935ff68e1	Europe (London)
ResilientNetwork2	AWS	VMX-S	c5.large	i-0442808a917446597	Europe (London)

<
1
>



What does your company use for hybrid workforce connectivity ?

① Start presenting to display the poll results on this slide.

Zero Trust Access

Security and Connectivity as
One



Remote User Connectivity Methods



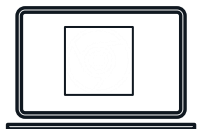
VPNaaS

- Authentication & Posture at Connect time
- DTLS Tunnel
- Carry Internet & Private Traffic (All ports & protocols)
- SAML 2.0 Authentication



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, geo-location)
- Web applications only

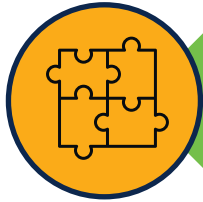
Unmanaged Device



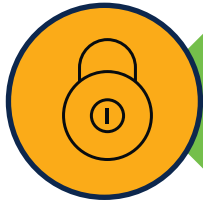
Client-based ZTA

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

Zero Trust Access IS Resilient



Next Gen Protocols : MASQUE and QUIC
Delivers low latency & high throughput connectivity

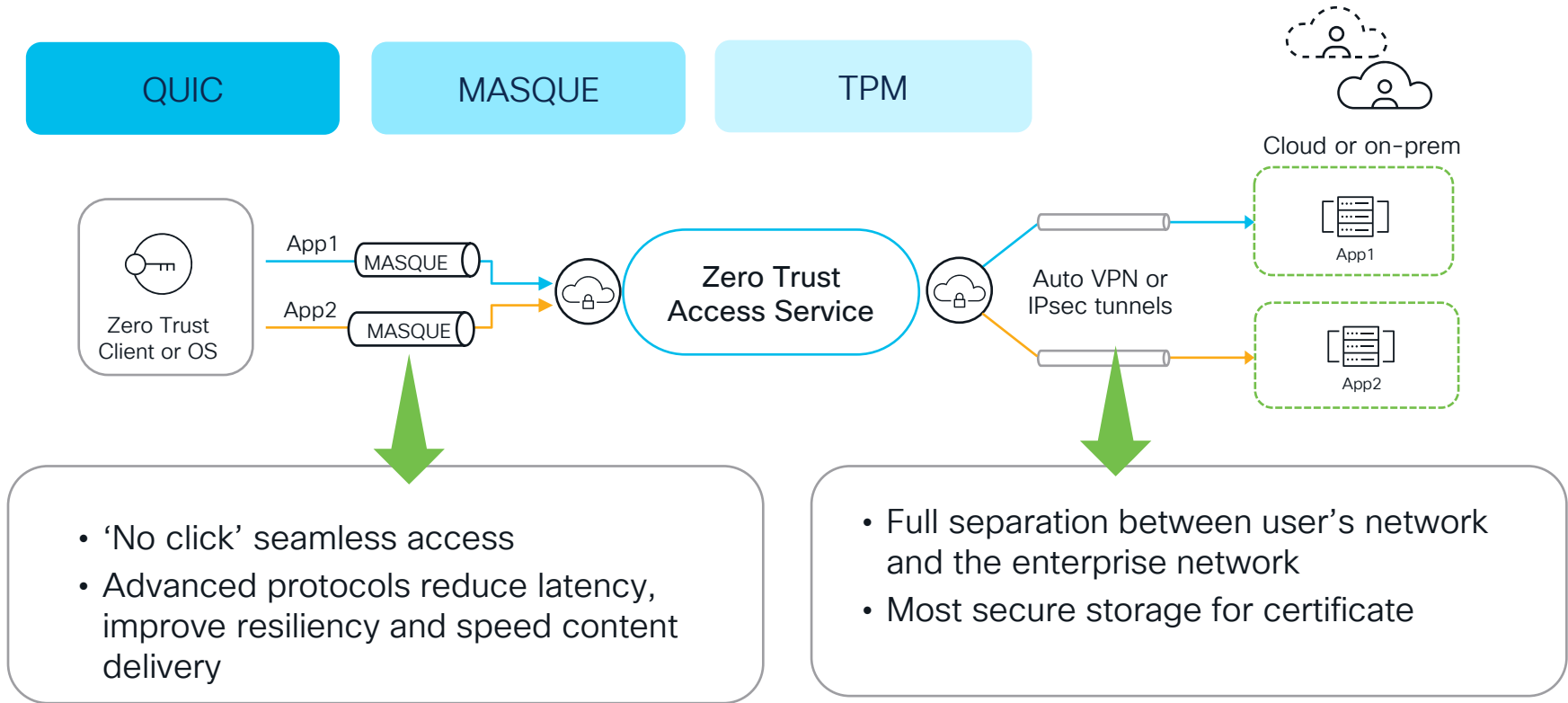


Verify, Then Trust: No automatic trust. Every access request requires authentication and authorization.

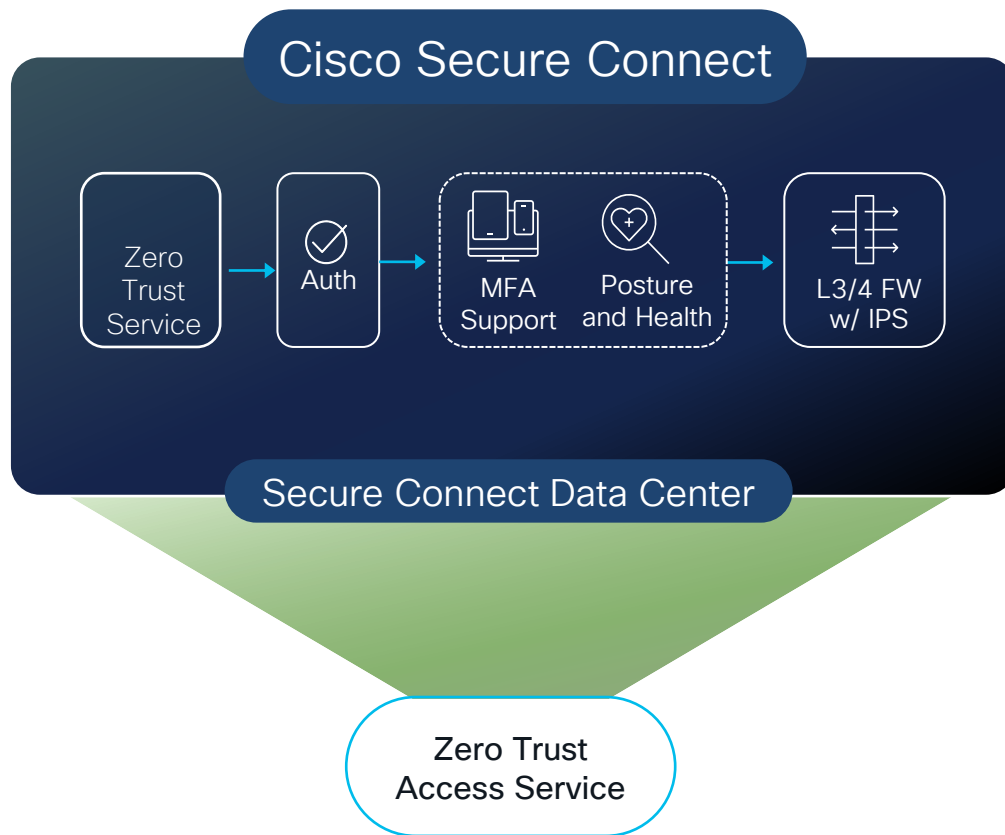


Micro-segmentation: Network is divided into isolated zones, limiting the impact of a breach.

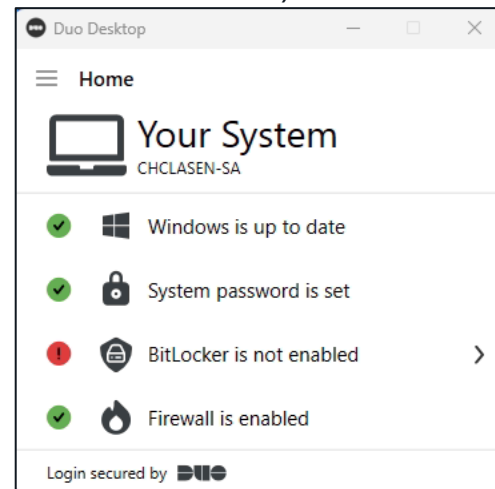
Introducing MASQUE – unlocking QUIC proxying



ZTA in Secure Connect

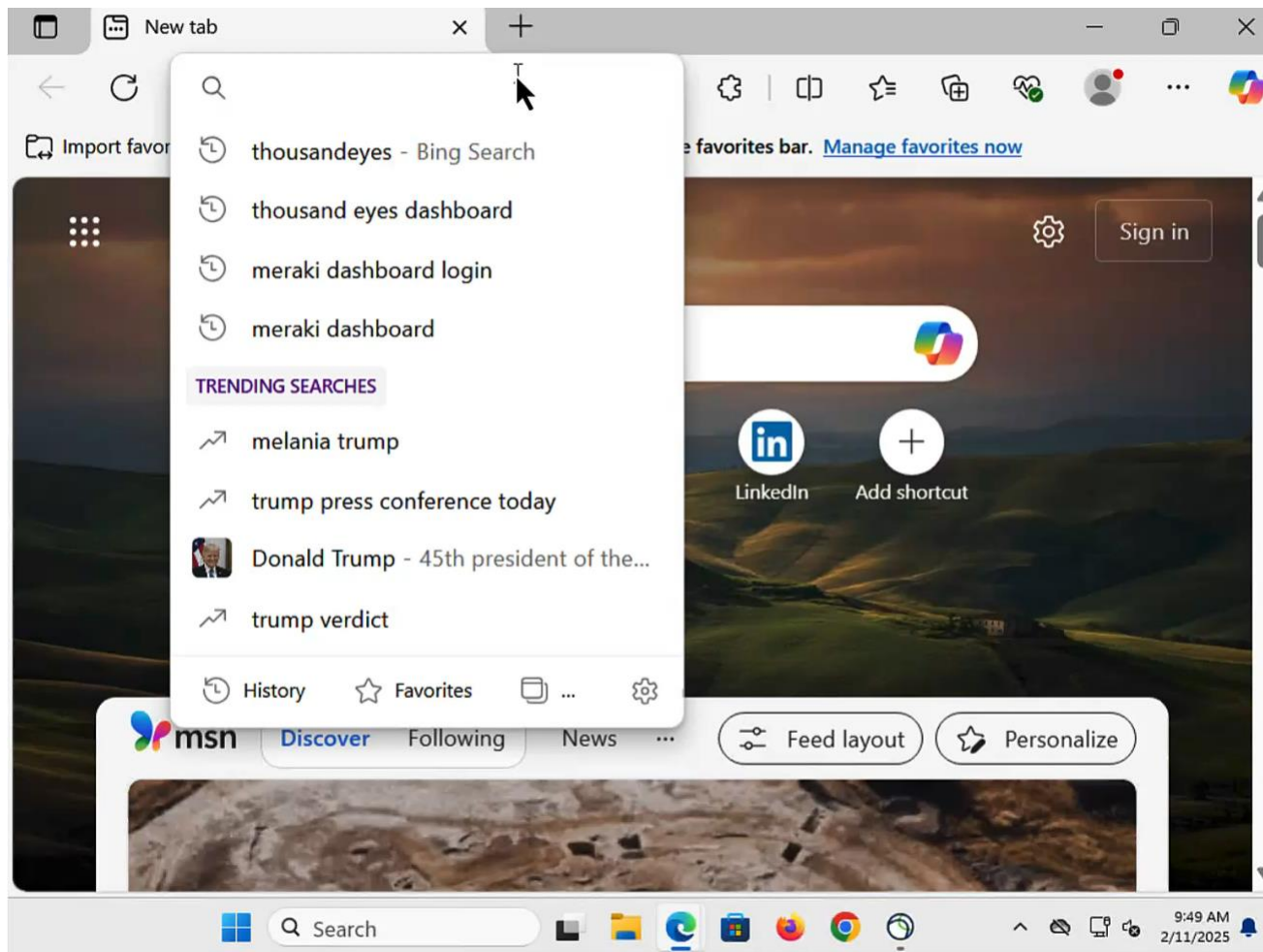


- QUIC tunnel (MASQUE proxy)
- Carry Private Traffic
 - Clientless: Browser-based (80, 443)
 - Client-based: All ports & protocols
- SAML2.0 Authentication and Posture per session + Auto re-new
- Posture based on Duo Health agent (embedded into client)



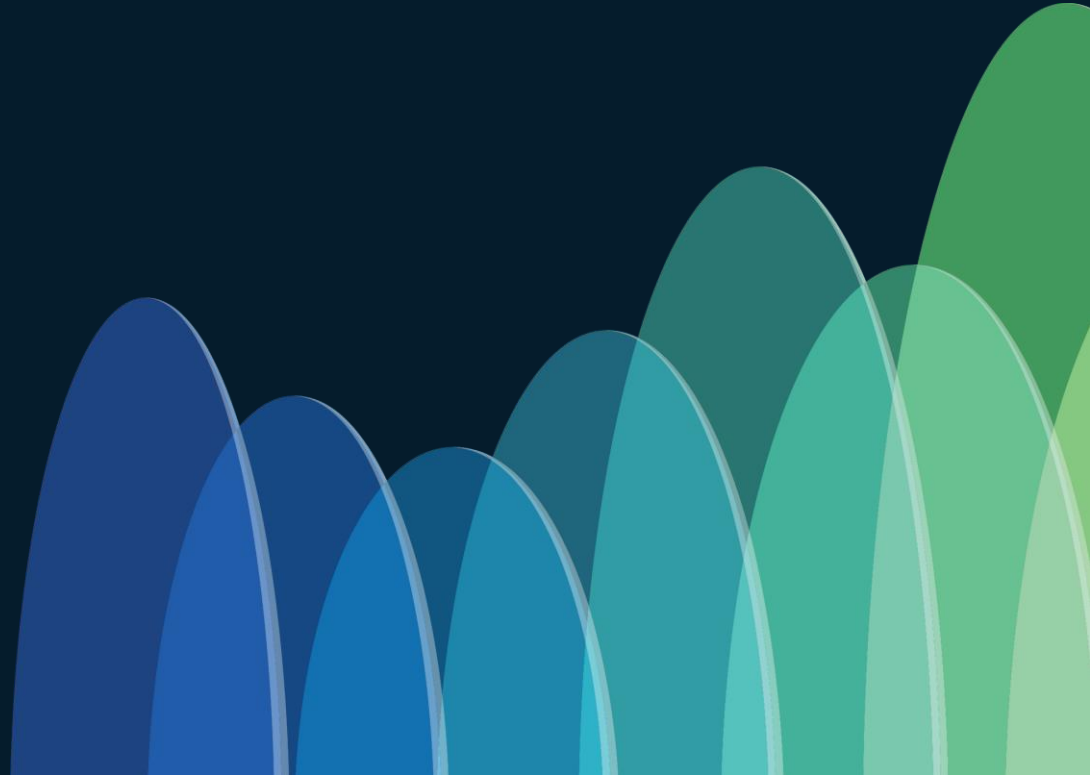
ZTA Enrolment Demo



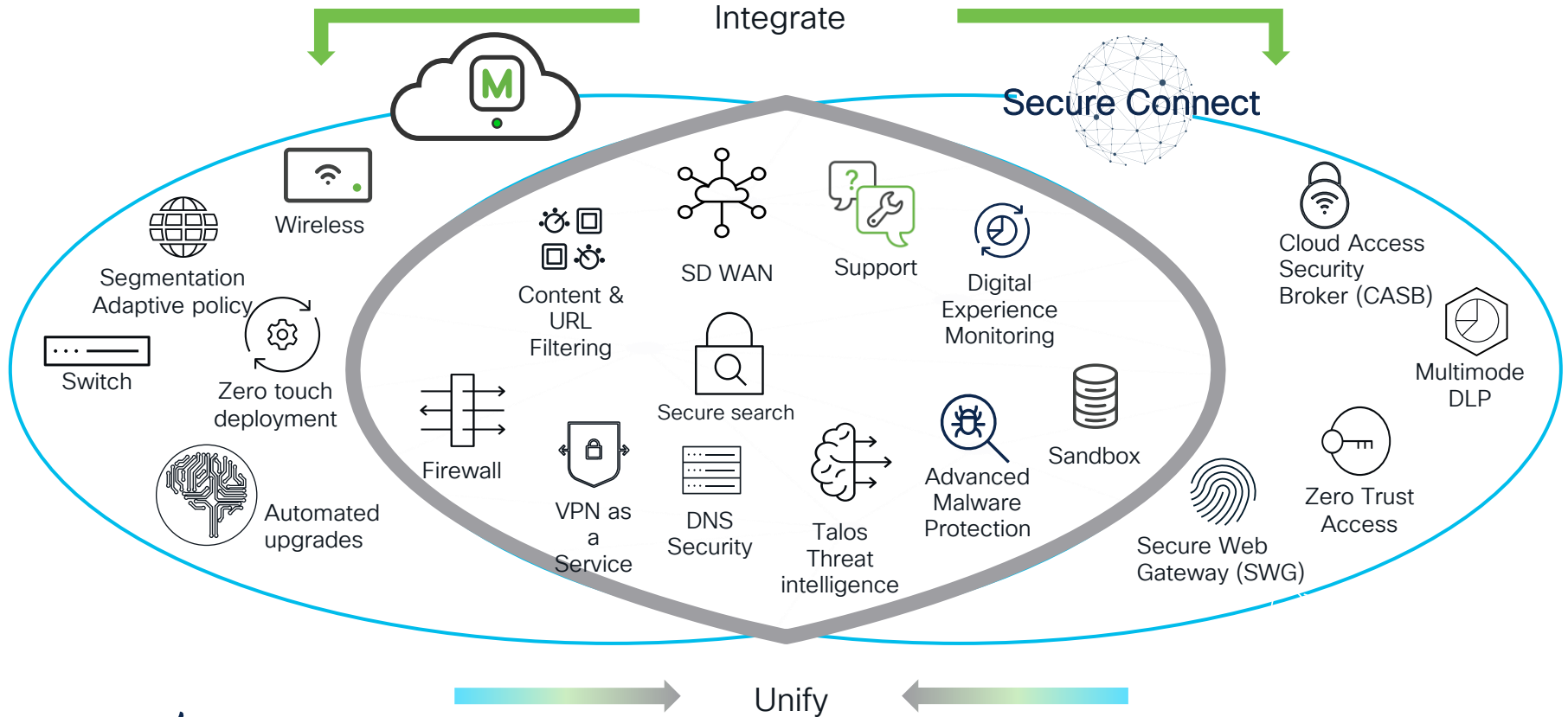


Security Everywhere

CISCO *Live!*

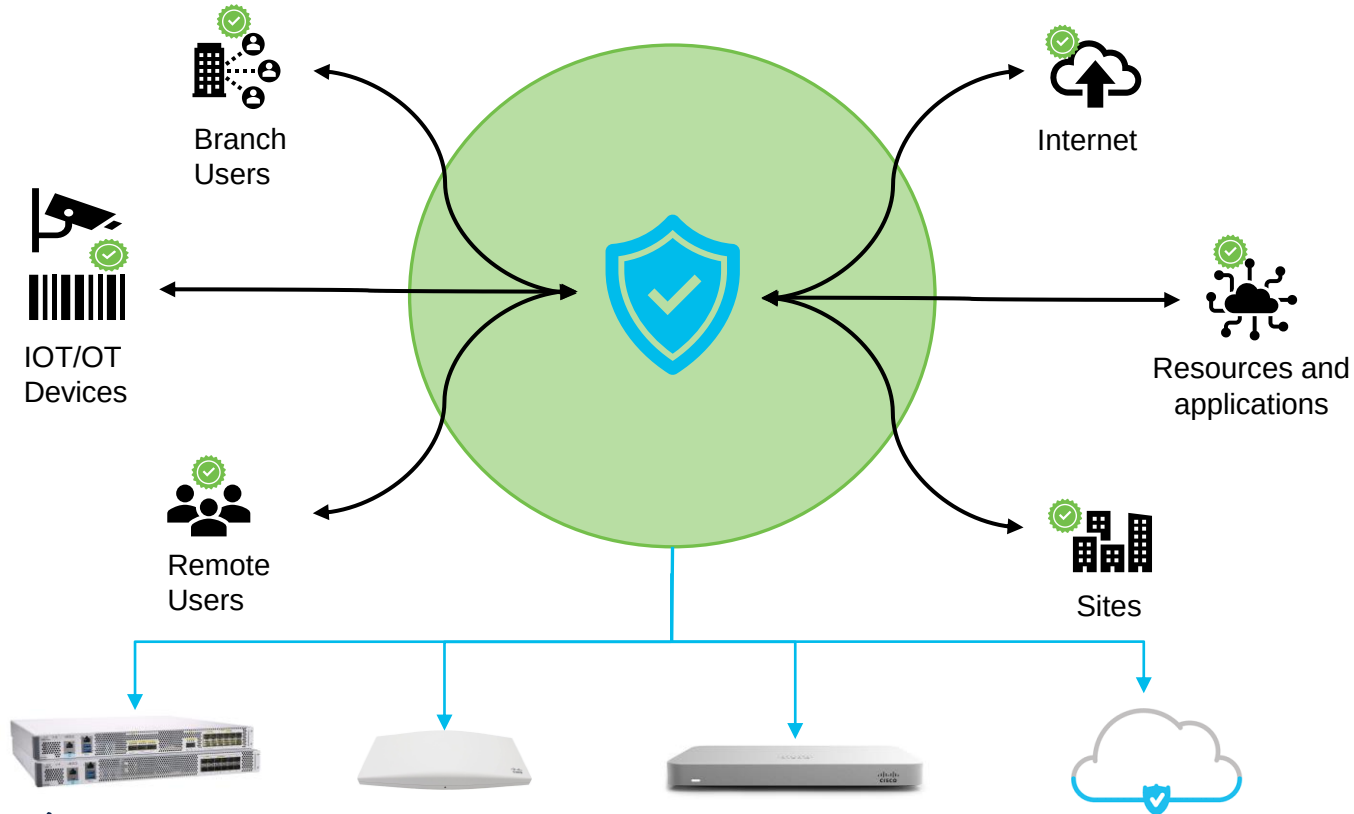


Cisco Meraki Platform



Meraki Platform Policy Vision

Centralized Management Distributed Enforcement



Meraki Platform Firewall Policy Pain Points

- Policy enforcement is segmented and requires repeated tasks
 - 1 Policy rule is repeated across many branches
 - Prone to inconsistency and human error
- One policy list page with thousands of rules
 - Top-down execution
 - Hard to manage
 - A giant conditional statement
- One large network-level list can lead to
 - Shadowed and duplicate rules

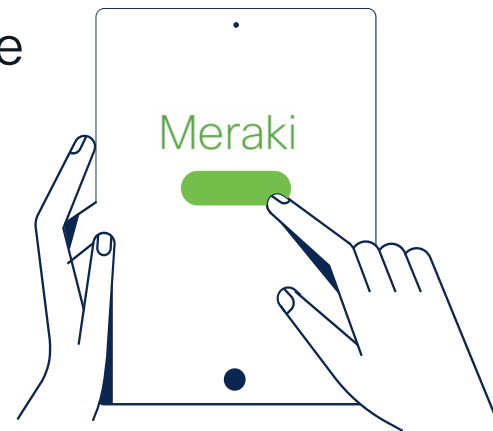




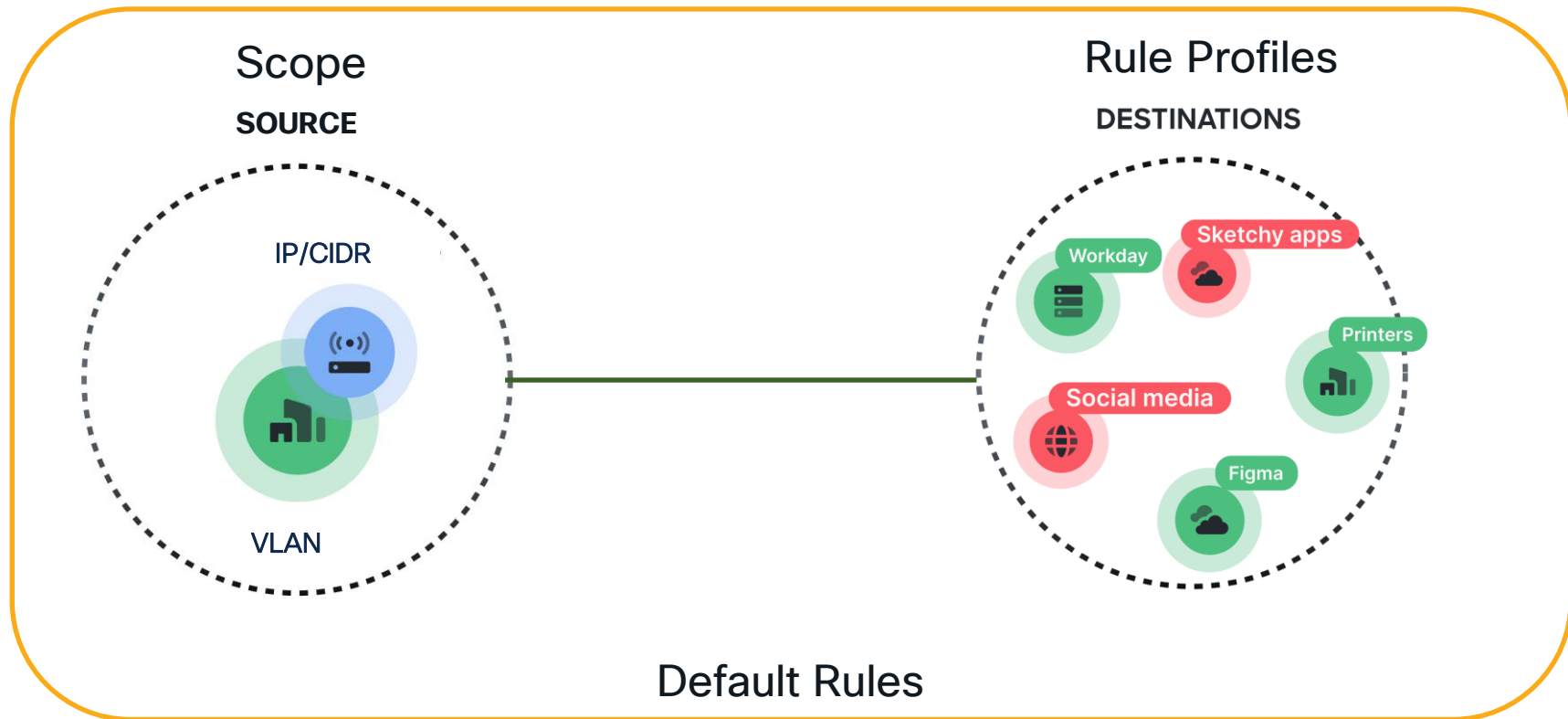
Organization Policies

Organization Policies

- Firewall policy centralized management distributed enforcement across MXs
- Simplified policy usability with reusable objects (rule profiles)
- Smart enforcement logic based on the scope
- Enforcement closer to the user



Policy Components



Organization Policy

Organization Group Policies

Enforce policies across your entire organization with group policies and re-usable rule profiles. [Documentation](#)

Group policies

Scope

Rule profiles

Change log

Search	Scope ▾	Enforced at ▾	Rule profile ▾	Filters	48 results	+ Add group policy
Policy name	Description	Scope	Enforced at	Rule profiles	Last modified	
Engineers - remote	–	Engineers (33)	Secure Connect Cloud	Engineer tools	Just now Samandersen	...
Branch offices	–	Branch offices	SF-012, Den-202, CHI-312, Den-921 +4 Show 4 more	Collaboration tools	Just now Samandersen	...

Who or what
the rule
applies to

Enforce policy
across
branches or
cloud

Reusable sets of
rules can be
applied across
multiple policies

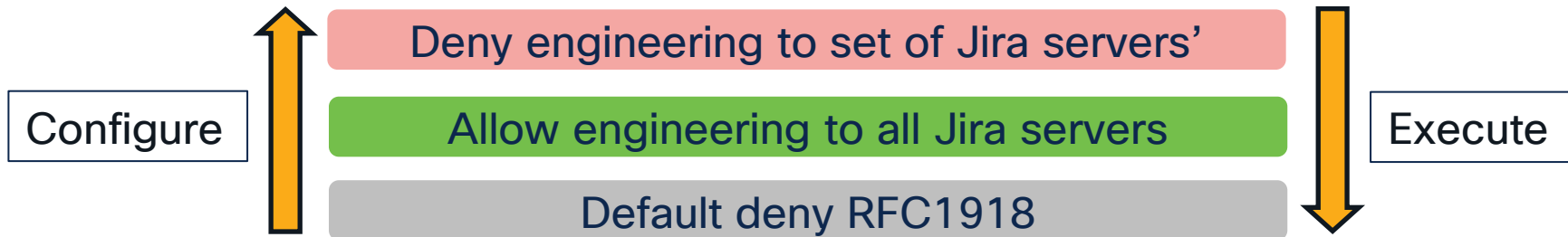
Innovative Approach



No policy ordering: “Deny Wins” simplifies policy management

1. Deny rules
2. Allow rules
3. Default rule (Deny RFC1918 OR Deny All OR Allow All)

Example: All engineers can access Jira except servers at locations that are not compliant with organization security policy



Reusable Rule Profiles – Sets of Rules

MX Operation:

1. All Layer 3
2. All Layer 7

Order of Operation:

1. All Deny rules
2. All Allow rules
3. Deny Default

Rule name	Type	Source	Src port	Action	Destination	Protocol and port pairs	Profile
Risky app	L3	Engineers (33)	Any	Deny	1.1.1/24	TCP: 40	Engineering tools
Compromised app	L3	Engineers (33)	Any	Deny	168.12.2.1/24	Any	Engineering tools
Jira access	L3	Engineers (33)	Any	Allow	Jira	TCP: 40, UDP: 20	Collaboration tools
Workday access	L3	Engineers (33)	Any	Allow	Workday	Any	Employee toolkit
O365 access	L3	Engineers (33)	Any	Allow	O365	TCP: 40	Collaboration tools
Slack access	L3	Engineers (33)	Any	Allow	Slack	UDP: 20	Collaboration tools
L3 default rule	Default L3	Any	Any	Deny	RFC 1918 traffic	–	Default rule profile
Social media	L7	Engineers (33)	Any	Allow	Social media (32)	–	Profile name

Organization Policy Demo



Organization-wide Group Polic... x

n123.meraki.com/0/A1B2C3/manage/organization/cpsc/Group_policies

☆

Meraki

Business Corp, Inc

Search Dashboard

?

🔔

👤

⋮

Network
Chi-10

Network-wide

Security & SD-WAN

Switching

Wireless

Systems Manager

Camera

Sensors

Organization-wide

Org-wide security

Insight

Secure Connect

Admin

Organization Group Policies

Enforce policies across your entire organization with group policies and re-usable rule profiles. [Documentation](#)

Group policies

Scope

Rule profiles

Change log

Search

Scope

Enforced at

Rule profile

Filters

0 results

+ Add group policy

Policy name	Description	Scope	Enforced at	Rule profiles	Last modified
No policies, yet					

© 2024 Cisco Systems, Inc.

[Privacy policy](#) [Terms of service](#)

Last login
about 2 hours ago from your current IP address

Current session started
about 2 hours ago

Data for this organization is hosted in [North America](#)

Give your feedback

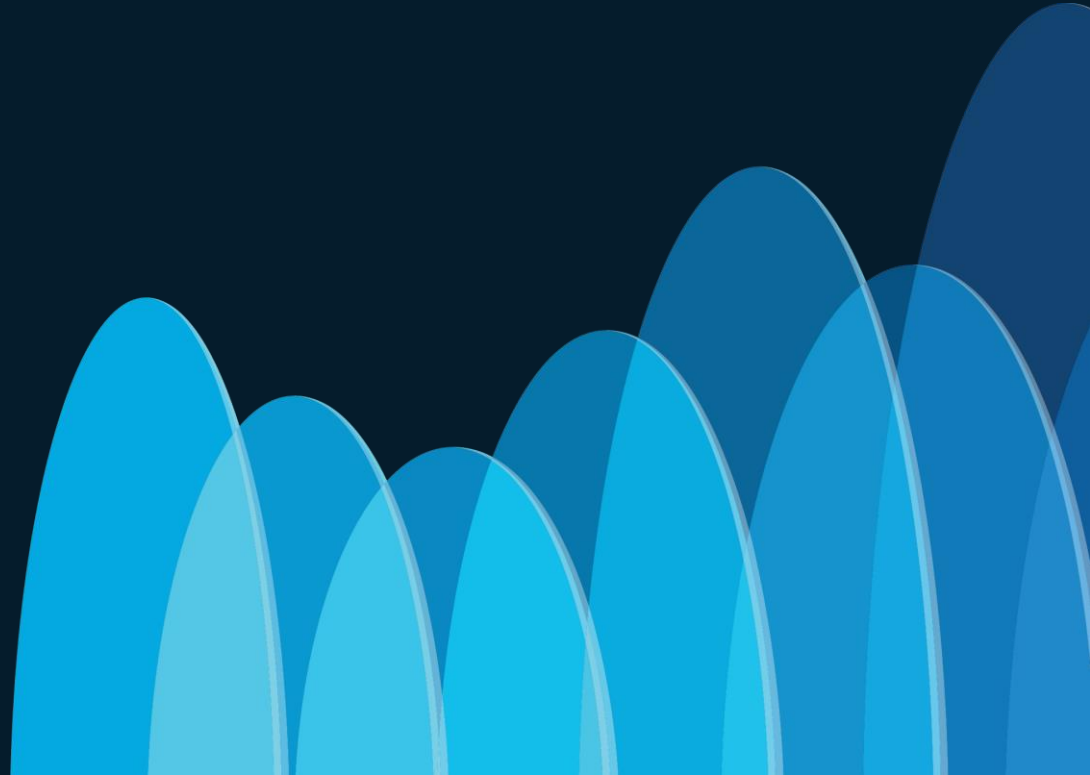
CISCO Live!

BRKMER-2577

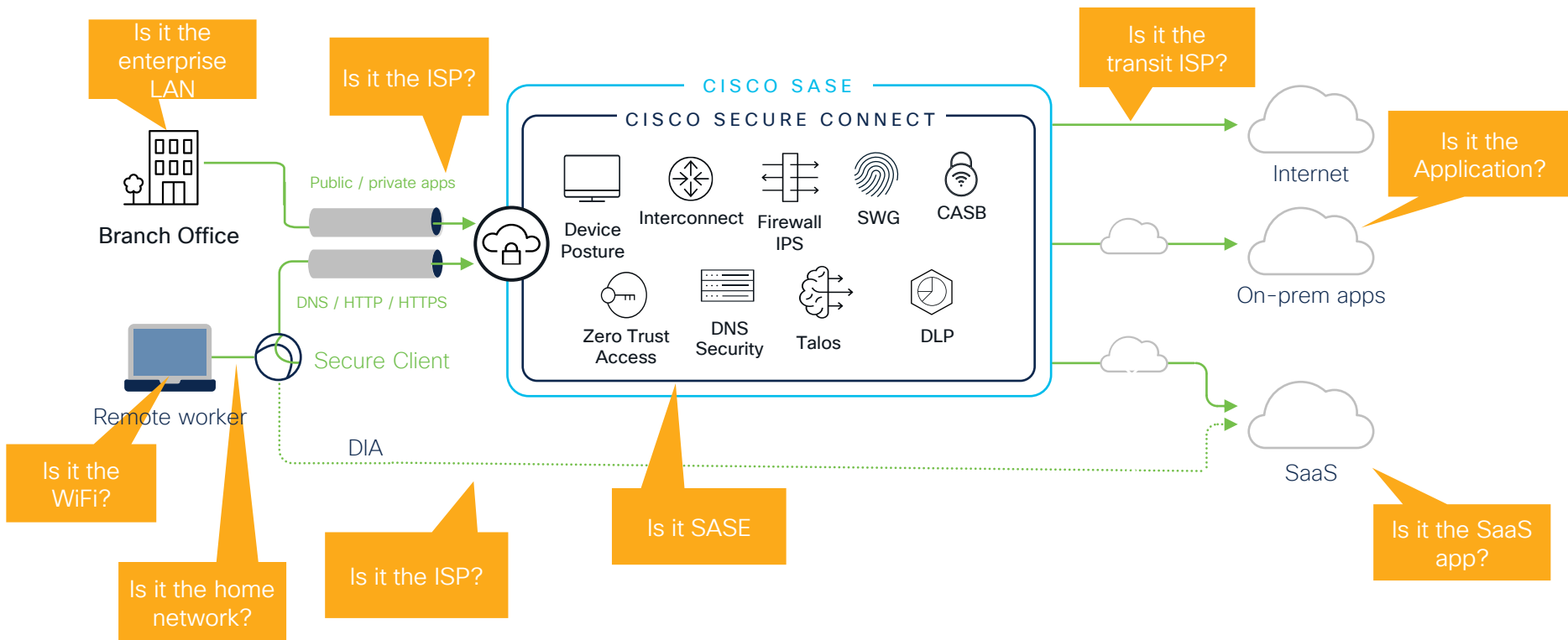
© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

59

Digital Experience Monitoring

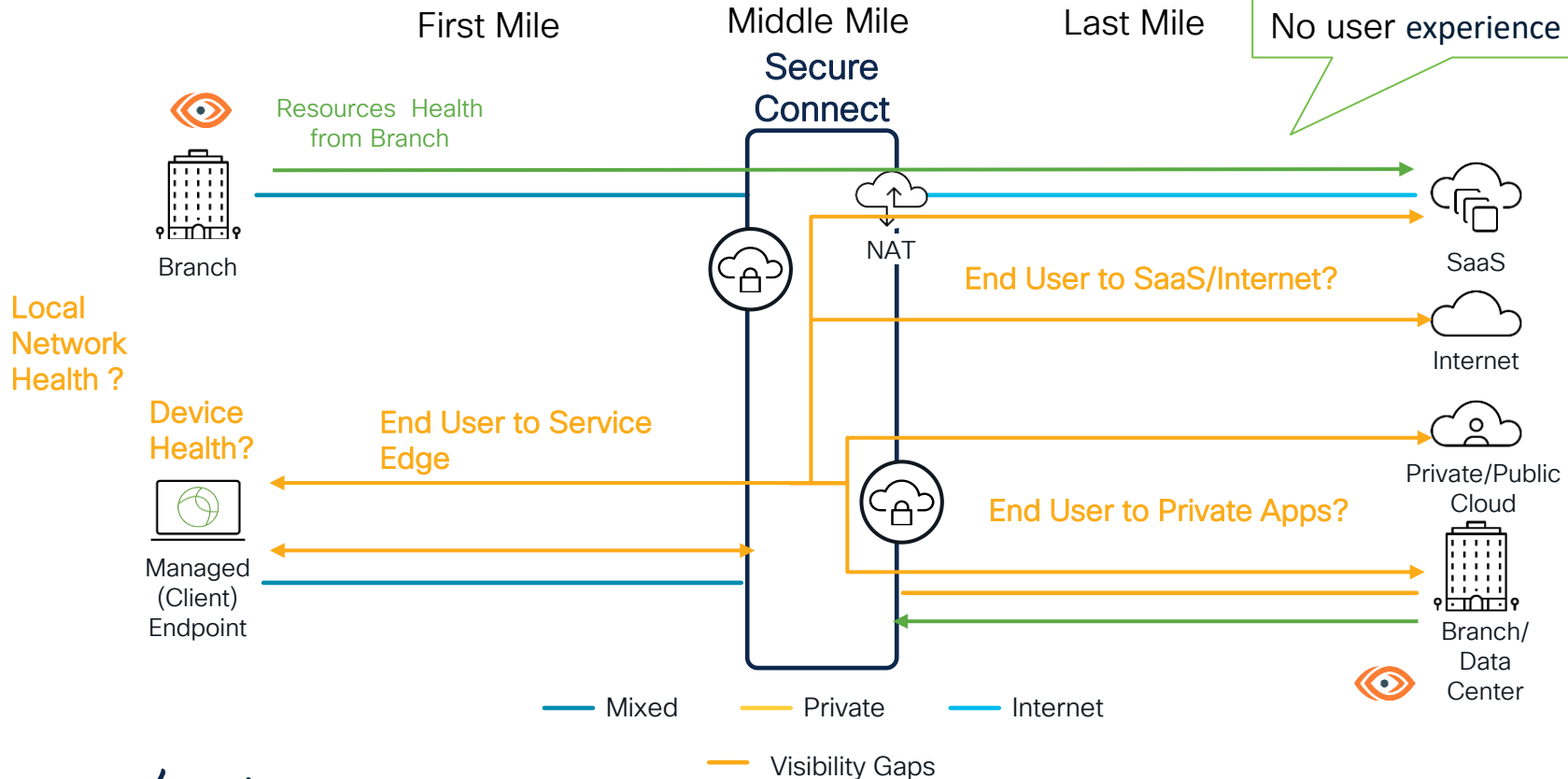


Troubleshooting Hybrid Workforce

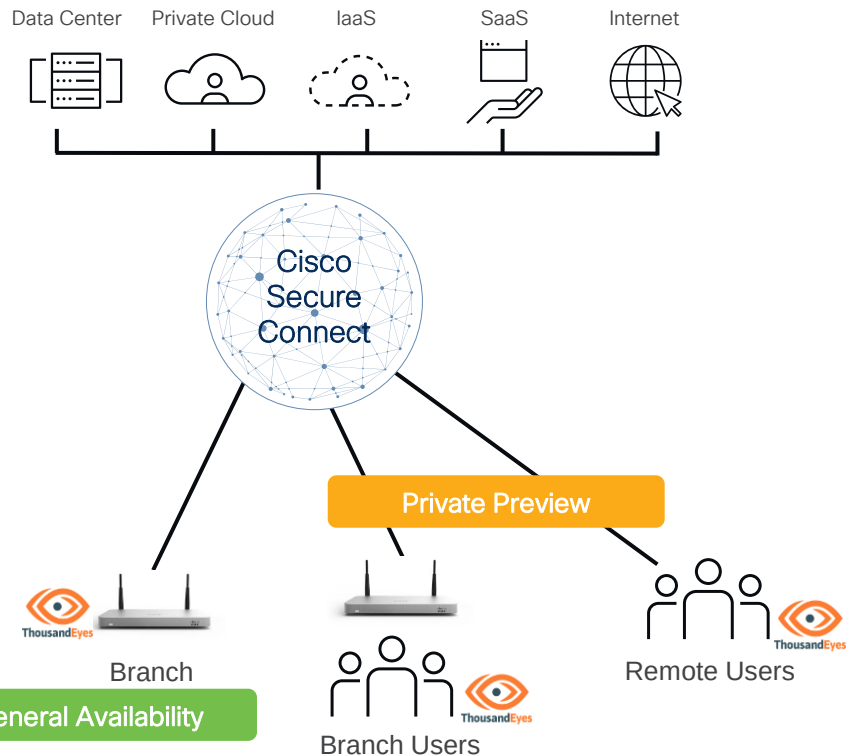


Problem Statement

IT Admin's pain:
Visibility is fragmented.
No end-to-end testing.
No user experience visibility



Remote Access Digital Experience Monitoring (DEM)



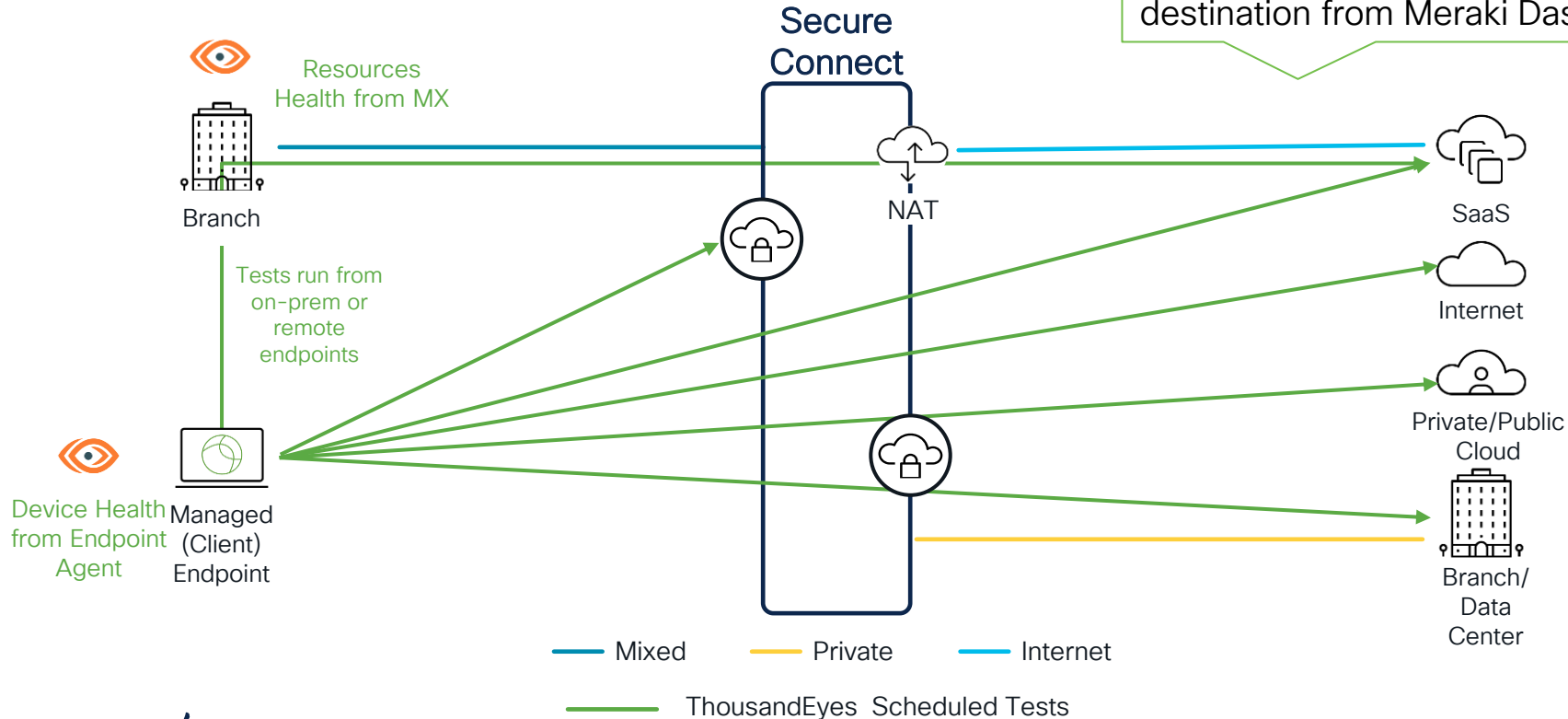
Enrich the Meraki platform with visibility into:

- Quality of user connectivity
- Health of end-user machines
- Simplified usability and visibility
- Monitor the end-to-end experience for users (remote or on-prem)

Unified End-to-end Visibility

Customer Experience

IT Admins can create tests from end-user's devices to any destination from Meraki Dashboard.



Technical Support Persona

Scenario: The user Ima Healer opened a ticket with IT support that performance to Medical Portal Application is slow today.

IT Admin Persona

Scenario: IT Admin has received an alerting email that Financial Portal Application performance is degraded.

Endpoint ThousandEyes Agent

- Bring your own License (BYOL)
- Standalone or Cisco Secure Client module
- Performs active application and networking performance tests
- Automatic default test to Secure Connect
- Passively collects performance data (WiFi, CPU, ...)
- No path visualization through Secure Connect Fabric

Remote Access DEM – End Device Health

Configure New Active Tests

End Device Health

Wifi and Local Network Test

Digital Experience Monitoring

Monitored endpoints

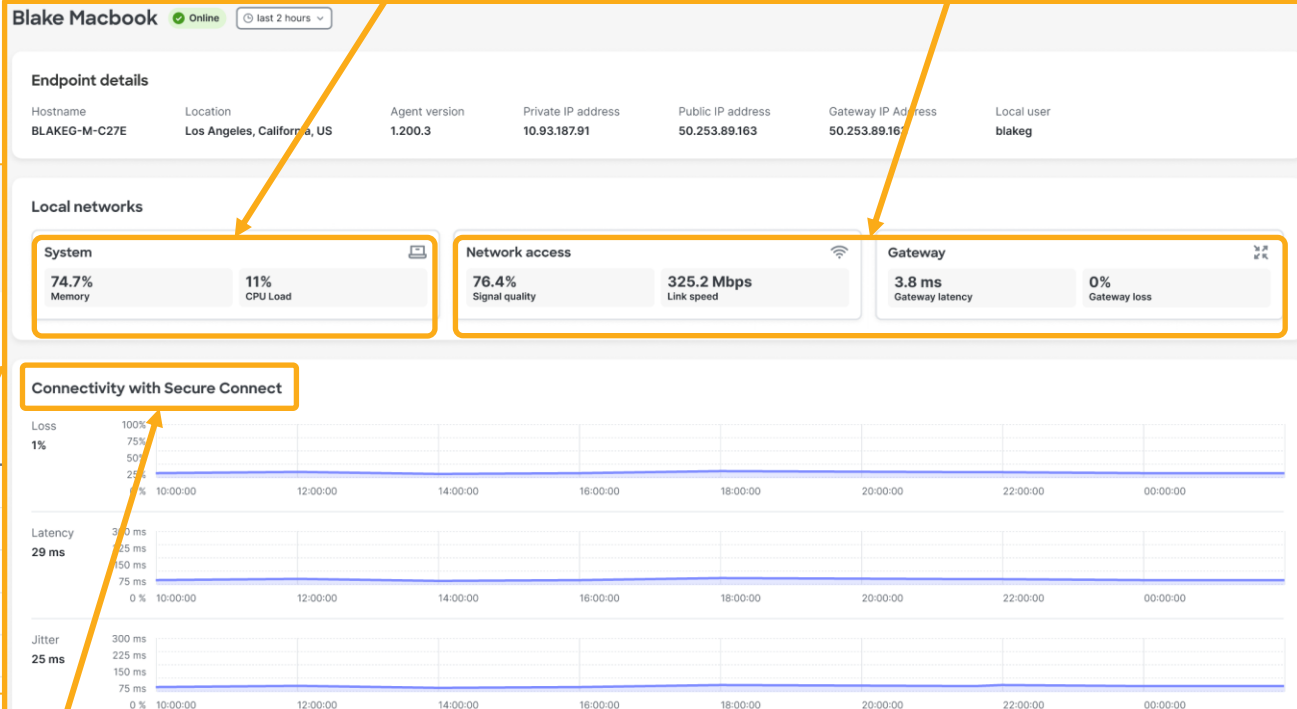
Endpoint tests

Monitored endpoints 5

Q Search

5 results

Status	Endpoint agent	Local username
Online	Betsy Webex Device	betsyw
Online	Blake Macbook	blakeg
Online	Byron Macbook	byronl
Offline	Kevin Lenovo	kevinc
Offline	Grace Lenovo	graces



Default Test

DEM Demo



Meraki Dashboard

n123.meraki.com/o/A1B2C3/manage/organization/cpsc/sites_display

☆ ⋮

Meraki

Search Dashboard

🔔 ? 👤

Network
Acme-HQ-AUS

Secure Connect

Network-wide

Cellular Gateway

Security & SD-WAN

Switch

Wireless

Systems Manager

Cameras

Environmental

Insight

Organization

Digital Experience Monitoring

Powered by ThousandEyes

Monitored Endpoints

Endpoint Tests

Settings

Monitored endpoints 5

Q Search

5 results

Status	Endpoint agent	Local username	Computer name	Platform	Device model	Location	Last seen (UTC-5)	
Online	Betsy Webex Device	betsyw	Webex-72D37	Webex	Cisco Desk Pro	Los Angeles	Nov 1 2024 09:41	...
Online	Blake Macbook	blakeg	Desktop-45A38	Mac	Macbook Air 7	Detroit	Nov 1 2024 09:41	...
Online	Byron Macbook	byronl	Desktop-85P27	Mac	Macbook Pro 16	Sacramento	Nov 1 2024 09:41	...
Offline	Kevin Lenovo	kevinc	Desktop-67B61	Windows	Thinkpad X1	San Francisco	Jun 3 2024 17:05	...
Offline	Grace Lenovo	graces	Desktop-81J23	Windows	Thinkpad X1	San Jose	Oct 9 2024 07:28	...

Rows per page

30

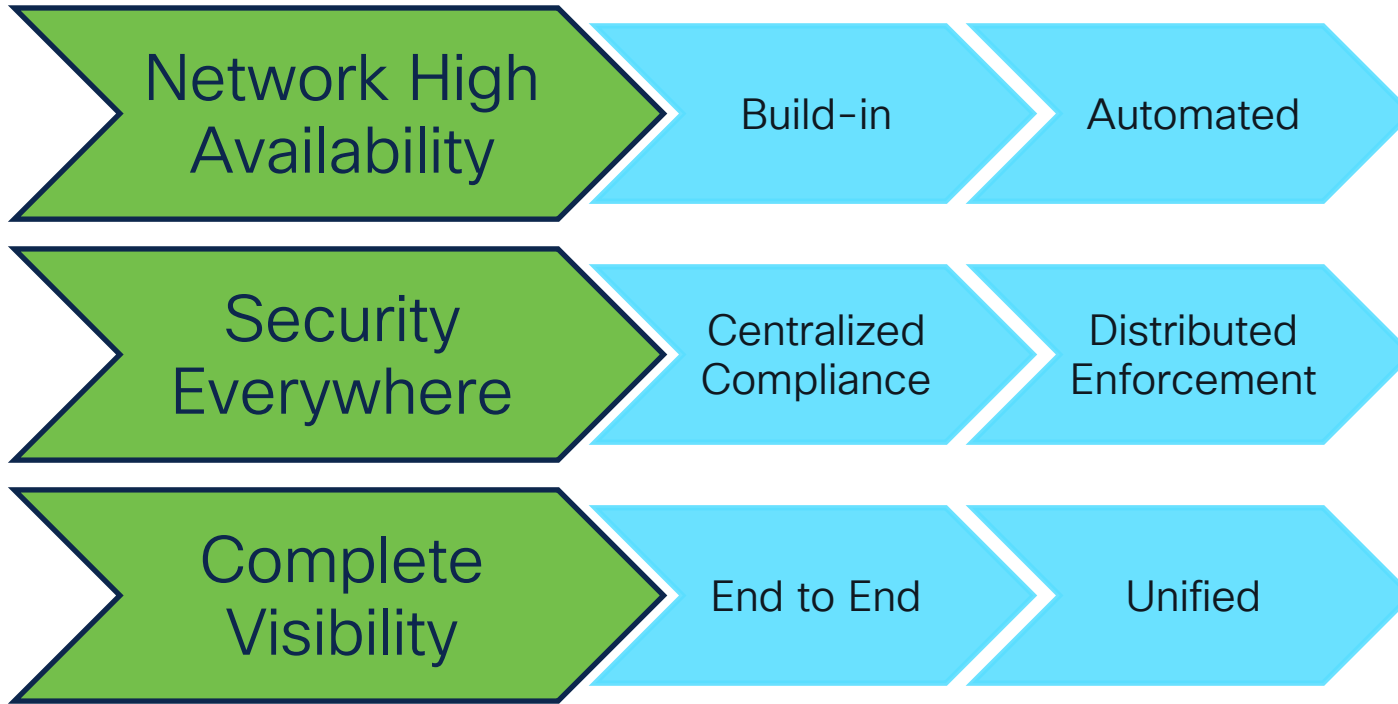
1-30 of 300

< 1 2 3 >

Recap



Secure Connect Resiliency



Webex App

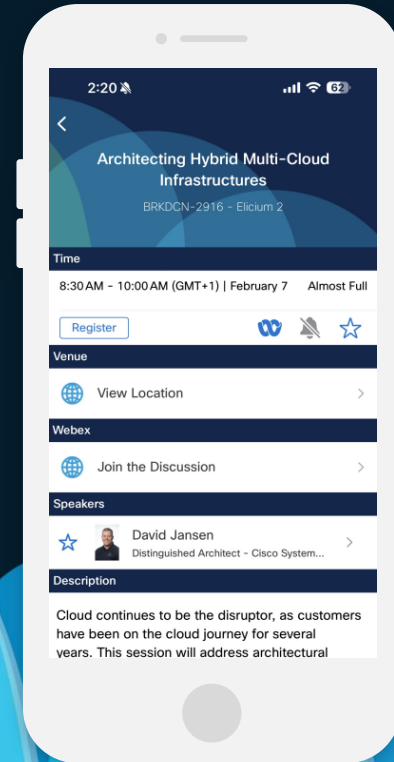
Questions?

Use the Webex app to chat with the speaker after the session

How

- 1 Find this session in the Cisco Events 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 February 28, 2025.



Fill Out Your Session Surveys



Participants who fill out a minimum of 4 session surveys and the overall event survey will get a unique Cisco Live t-shirt.

(from 11:30 on Thursday, while supplies last)



All surveys can be taken in the Cisco Events mobile app or by logging in to the Session Catalog and clicking the 'Participant Dashboard'



Content Catalog

Continue your education

- Visit the Cisco Showcase "Unified SASE" booth NET09
- Visit the On-Demand Library for more sessions at ciscolive.com/on-demand. Sessions from this event will be available from March 3.

Contact me at: [Linkedin](#)

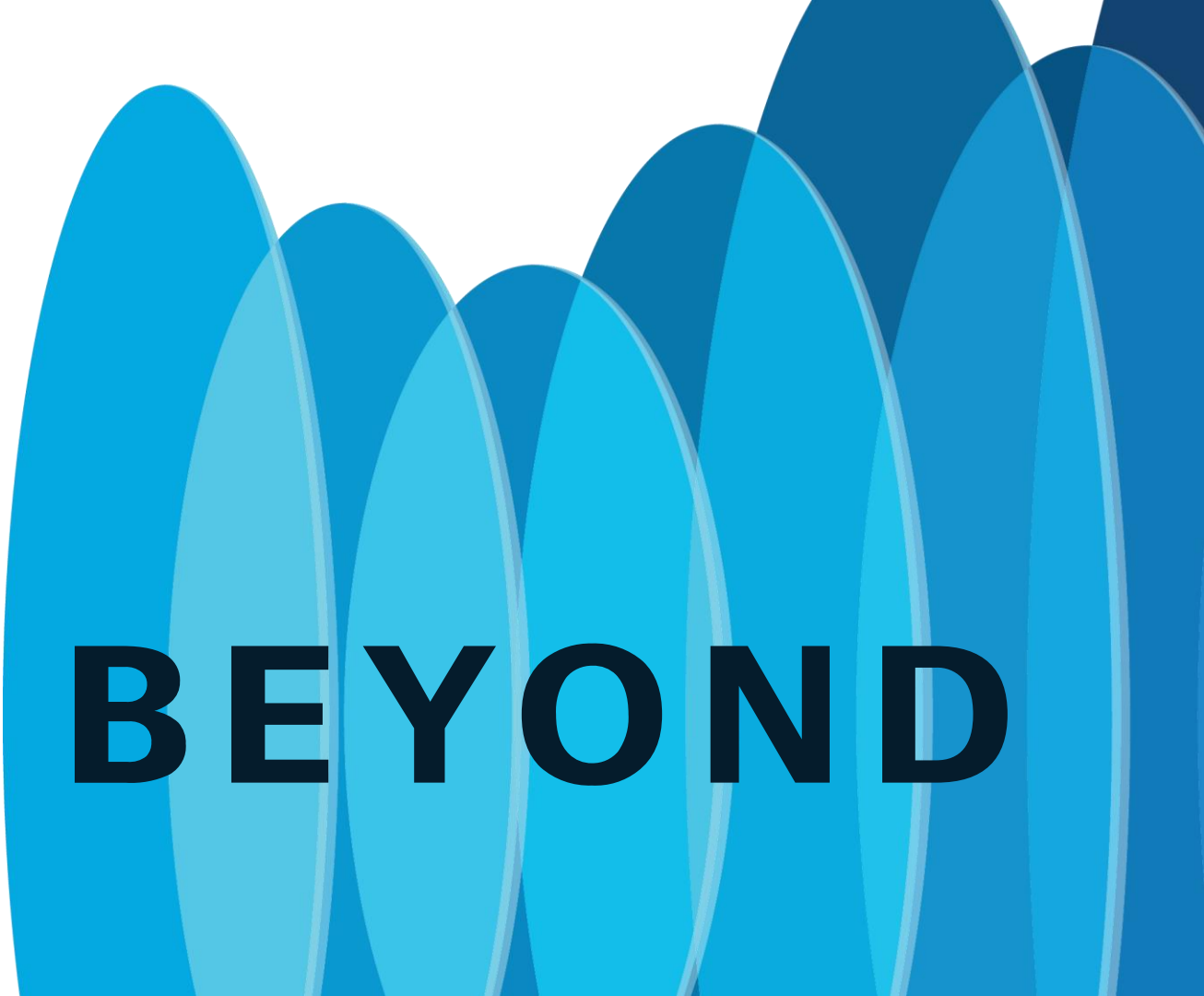


Thank you



CISCO *Live!*

GO BEYOND

The background of the slide features a series of overlapping, teardrop-shaped elements in various shades of blue, ranging from light sky blue to deep navy blue. These shapes are arranged in a way that creates a sense of depth and movement, resembling a stylized mountain range or a series of waves. The overall aesthetic is clean and modern.