

The Cisco Live! logo features the word "CISCO" in a bold, black, sans-serif font, followed by "Live!" in a black, cursive script font. The background of the entire image is a vibrant, multi-colored abstract pattern of overlapping, wavy bands in shades of red, orange, yellow, green, and blue, radiating from a bright white center on the right side.

CISCO *Live!*

Let's go

#CiscoLive



The bridge to possible

# Getting SASE with Umbrella and Meraki

Understand best practices for simple and  
flexible integrations between Meraki and Umbrella

Chris Riviere, Technical Solutions Architect

@rivimont

BRKSEC-2238

CISCO *Live!*

#CiscoLive



# Cisco Webex App

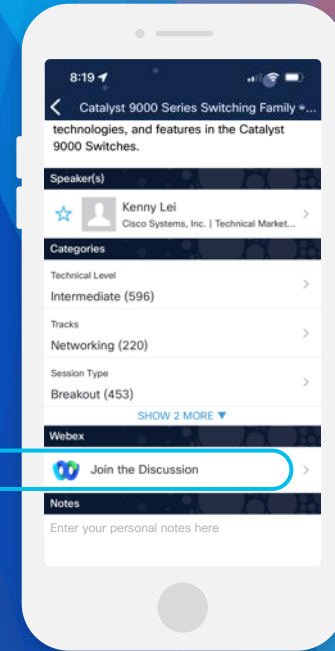
## Questions?

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 9, 2023.




<https://cislive.ciscoevents.com/cislivebot/#BRKSEC-2238>

# Agenda

- Introduction
- DNS Integrations
- Umbrella SIG
  - Option 1/Phase 1 – IPSEC Tunnels
  - Option 2/Phase 2 – AutoVPN
  - Secure Connect Foundation
- Value add/benefits
- Demo



# About Me

- Chris Riviere, Technical Solutions Architect
- OPNET, Riverbed, Piston Cloud Computing
- Cycling, Running, Scuba Diving, Traveling
-  @rivimont





# Industry leading SD-WAN meets industry leading security



## Meraki MX

On-prem security and SD-WAN

- Monitor and block malware and malicious traffic
- Restrict unauthorized users
- Prevent unwanted content or applications
- Firewall incoming traffic and VLAN to VLAN traffic
- Use secure site-to-site/in-tunnel VPN
- Detect and prevent intrusions (IDS/IPS)

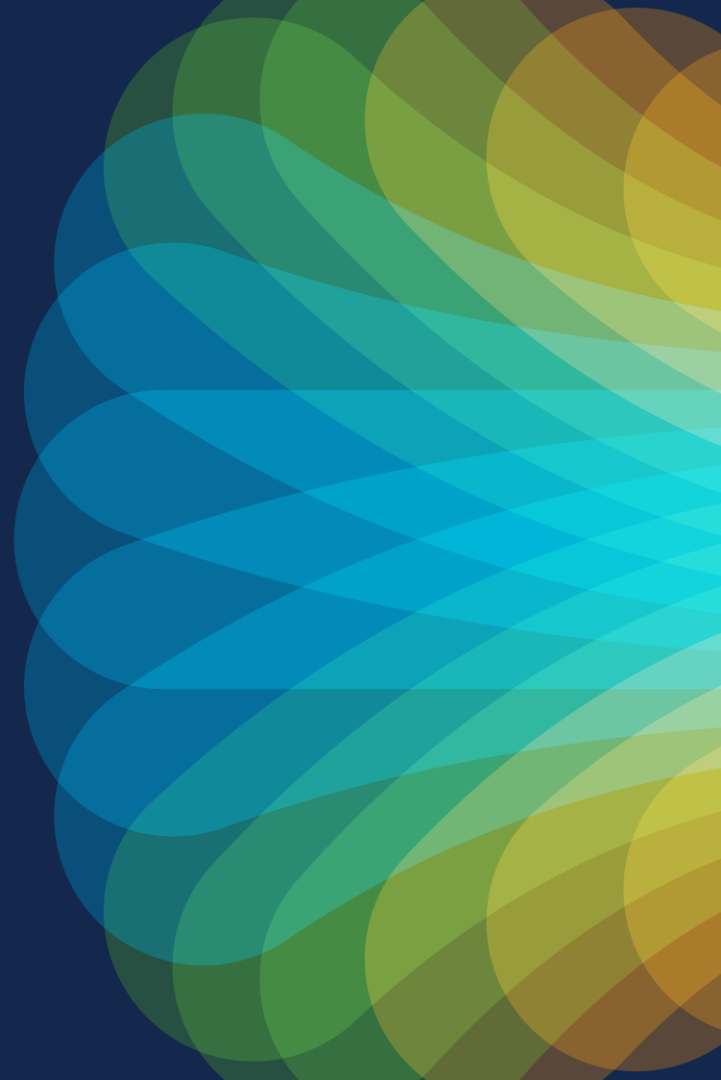


## Cisco Umbrella

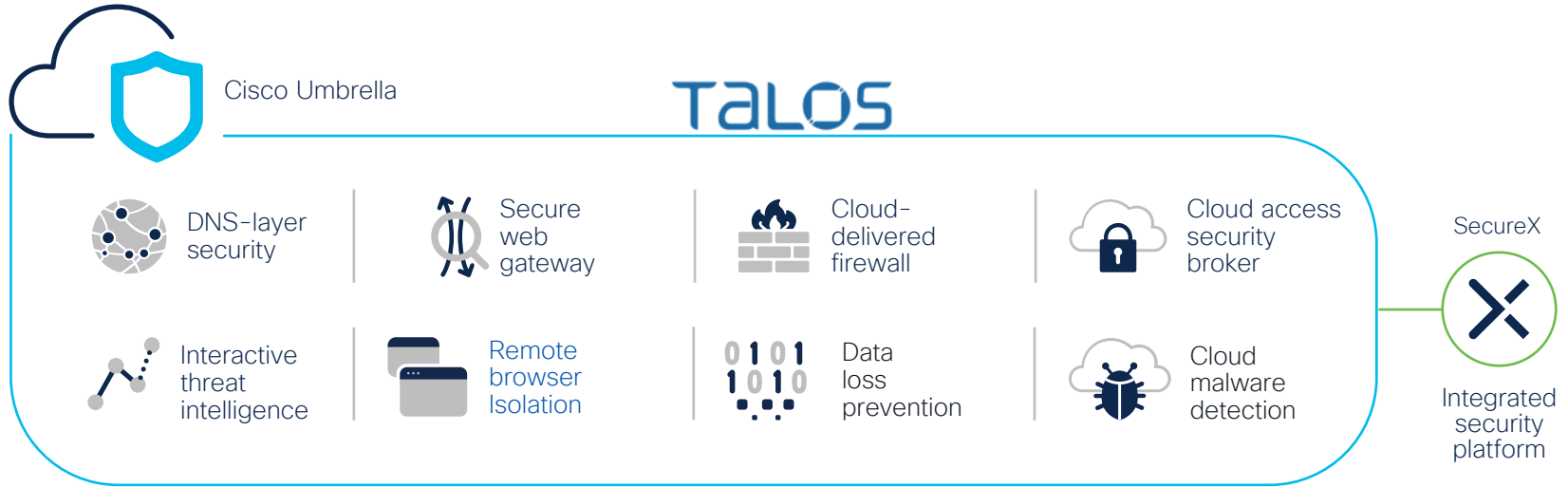
Cloud-native security

- Secure users at the edge with the best detection
- Increased reliability and performance with the speed and scale of the cloud
- Easily extend protection off-network
- Reduce the time, money, and resources required to identify and remediate threats

# Umbrella Overview



# Umbrella



Customer locations



Remote users



CISCO *Live!*



# Proven leader in cloud-native security



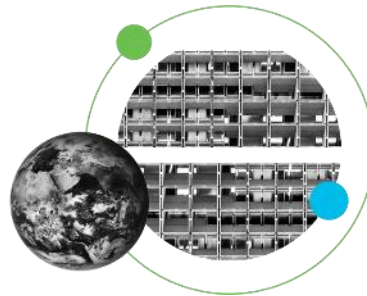
620B  
requests per day



5B  
web reputation requests  
processed daily



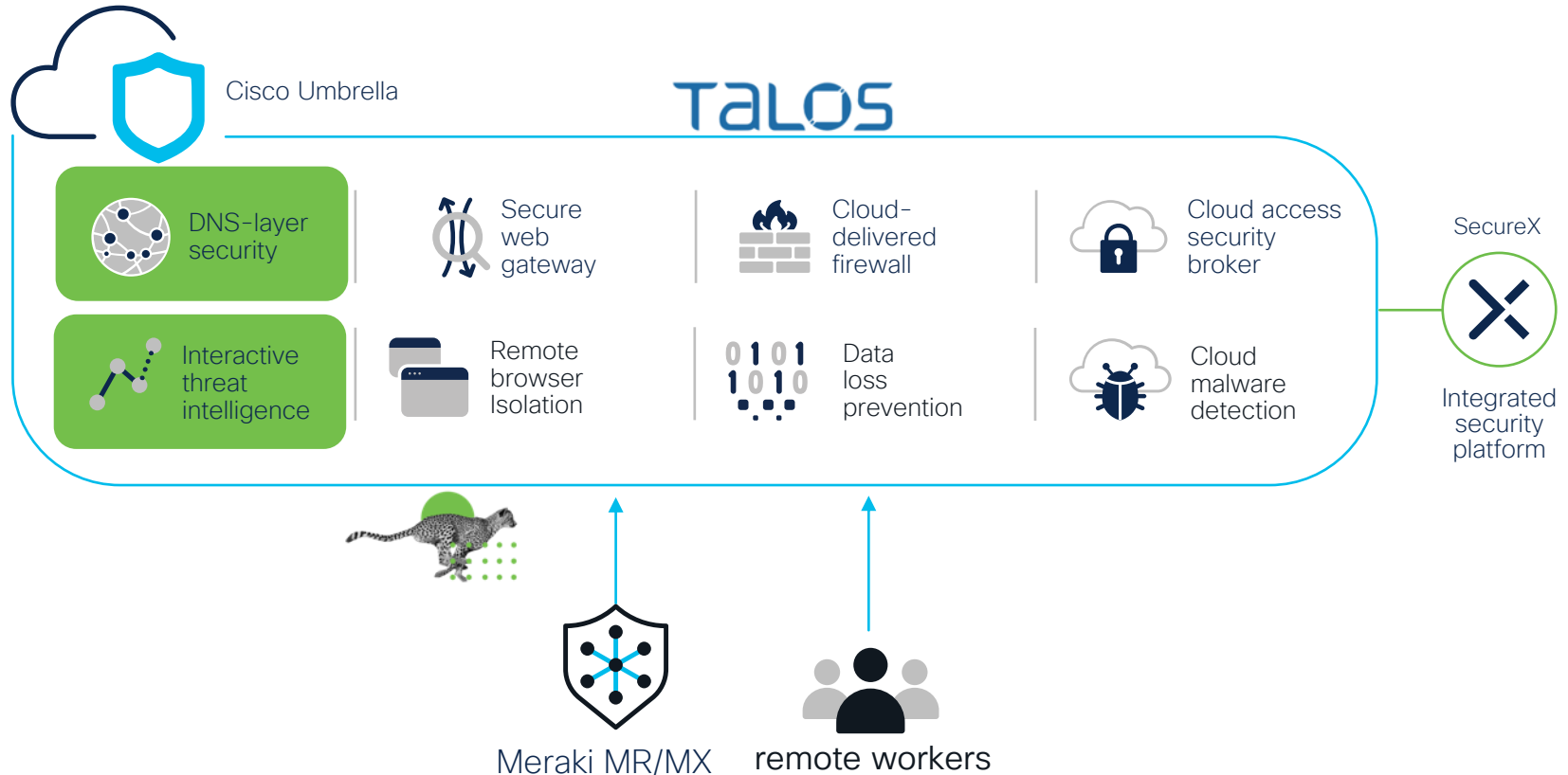
25K+  
enterprise customers



#1  
in AV-TEST security  
efficacy report

# DNS Integrations

# Simplified connectivity from Meraki to Umbrella



# DNS Integration Options


- MR-ADV
  - Canned Umbrella policies
  - No access to Umbrella dashboard
  - Co-Term AND Per Device Licensing (PDL)
  - Not compatible with other integration options
- MR/MX DNS Integration
  - Customizable Umbrella policies with access to Umbrella dashboard
- Both offer
  - Encrypted traffic between device <> Umbrella
  - Tamperproof
  - Additional visibility

# Meraki MR\_ADV DNS Security - Setup

## Step 1: Claim and Assign License

Assign licenses

You are currently assigning burning licenses which can only be assigned to unlicensed matching devices

 1x LIC-MR-ADV-1YR Licenses

Wireless devices

4 devices selected Select # of licenses

<input type="checkbox"/>	Device name	Network	Model	Serial number	Expiration date	Select # of licenses
<input type="checkbox"/>	ac:17:c8:#e5:8c	Umbrella Wireless	MR55	Q2ZD-F5UL-7WR5	None → Sep 17, 2020	<span>Select # of licenses</span>

## Step 2: Assign Policy

Select an Umbrella policy to apply.

Security & Full Appropriate Use Filtering ▲

-- Security and Appropriate Use Filtering --

Security & Full Appropriate Use Filtering

Security & Basic Appropriate Use Filtering

Security Filtering Only

Security & Moderate Appropriate Use Filtering (Default)

-- Appropriate Use Filtering --



Block applications and content categories

Layer 7 firewall rules

There are no rules defined for this SSID.  
[Add a layer 7 firewall rule](#)

DNS layer protection (Cisco Umbrella)

Route DNS requests through Cisco Umbrella DNS and deny DNS requests by linking Umbrella policies.

Select an Umbrella policy to apply.

Security & Full Appropriate Use Filtering ▼

Specify one or more domain names below (one per row) to be excluded from being routed to Cisco Umbrella.

# Meraki DNS Security - Enforce

## Prebuilt Block Page



 This site is blocked.

binarycousins.com

Sorry, binarycousins.com has been blocked by your network administrator.

[> Diagnostic Info](#)

[Terms](#) | [Privacy Policy](#) | [Contact](#)

## Built-in Reporting

Security Center the last 2 weeks Print Download Filter

url: binarycousins.com url: twitter.com url: mail.ru url: live.com url: facebook.com Search events

Summary Events DNS Events

Time	Type	Internal IP	External IP	Network	Destination	Action	Details
Aug 8 14:00:00	content	54.183.40.98	54.183.40.98	jsa1t-0462	live.com	blocked	Whitelist
Aug 8 13:59:59	security	54.183.40.98	54.183.40.98	jsa1t-0462	binarycousins.com	blocked	Malware
Aug 8 13:59:58	content	54.183.40.98	54.183.40.98	jsa1t-0462	twitter.com	blocked	Social Networking
Aug 8 13:59:50	security	54.183.40.98	54.183.40.98	jsa1t-0462	binarycousins.com	blocked	Malware
Aug 8 13:59:50	content	54.183.40.98	54.183.40.98	jsa1t-0462	twitter.com	blocked	Social Networking
Aug 8 13:00:04	security	54.183.40.98	54.183.40.98	jsa1t-0462	binarycousins.com	blocked	Malware
Aug 8 13:00:02	content	54.183.40.98	54.183.40.98	jsa1t-0462	facebook.com	blocked	Social Networking
Aug 8 12:59:56	content	54.183.40.98	54.183.40.98	jsa1t-0462	mail.ru	blocked	Chat Whitelist
Aug 8 12:59:52	content	54.183.40.98	54.183.40.98	jsa1t-0462	twitter.com	blocked	Social Networking
Aug 8 12:59:43	content	54.183.40.98	54.183.40.98	jsa1t-0462	mail.ru	blocked	Chat Whitelist

Page 4 of 148 10 results per page

# Umbrella DNS-layer integration with Meraki



+



Meraki SM

- Deploy cert
- AnyConnect, roaming client, IOS Clarity



+



Meraki MR

- Encryption
- Additional Visibility (internal IP/SSID)
- Tamperproof



+



Meraki MX

- Encryption
- Additional Visibility ( private/internal IP)
- Tamperproof

# Meraki MX/MR DNS Security - Setup

**Firewall & traffic shaping**

SSID: DumplingNet

**Block applications and content categories**

Layer 7 firewall rules: There are no rules defined for this SSID. [Add a layer 7 firewall rule](#)

DNS layer protection (Cisco Umbrella):

Select an Umbrella policy to apply:

Specify one or more domain names below (one per row) to be excluded from being routed to Cisco Umbrella.

**Threat protection**

**Umbrella protection**

DNS layer protection (Cisco Umbrella):

Select an Umbrella policy to apply:

Specify one or more domain names below (one per row) to be excluded from being routed to Cisco Umbrella.

MR Policy - Log Security | Protection DNS Policy | Applied To 4 Identities | Contains 4 Policy Settings | Last Modified Mar 29, 2020

What would you like to protect?

**Select Identities**

Search Identities

**All Identities / Network Devices**

- DumplingNet\_Chris\_Home\_-\_wireless
- mx\_default\_North\_Carolina\_-\_appliance
- mx\_default\_Chris\_Home\_-\_appliance
- ssid0\_Home\_WiFi\_MR55
- ssid0\_SiGraki\_North\_Carolina\_-\_wireless
- ssid2\_slig-time\_Chris\_Home\_-\_wireless
- ssid3\_DumpingNet5\_Chris\_Home\_-\_wireless

**4 Selected**

- Δ DumplingNet\_Chris\_Home\_-\_wireless
- Δ ssid0\_Home\_WiFi\_MR55
- Δ ssid3\_DumpingNet5\_Chris\_Home\_-\_wireless
- Δ ssid2\_slig-time\_Chris\_Home\_-\_wireless

- Link orgs using network device APIs
- Policies automatically update in Meraki/Umbrella dashboard
- Set policy at MX, MR, SSID level
- Group policies can also be used



# Don't forget the Umbrella Virtual Appliance

- For Umbrella DNS environments, the VA can provide the following:
  - Integration with Microsoft AD for allowing the ability to set policies on AD Group/user as well as user visibility
- Encrypting traffic between VA <> Umbrella
- Must be deployed in groups of two (for HA) ideally as close to users as possible
- Required for user attribution
- If also using SIG, rely on SAML for identity

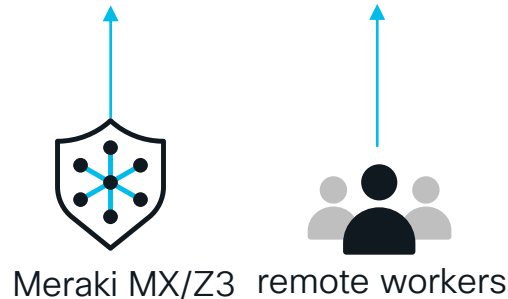
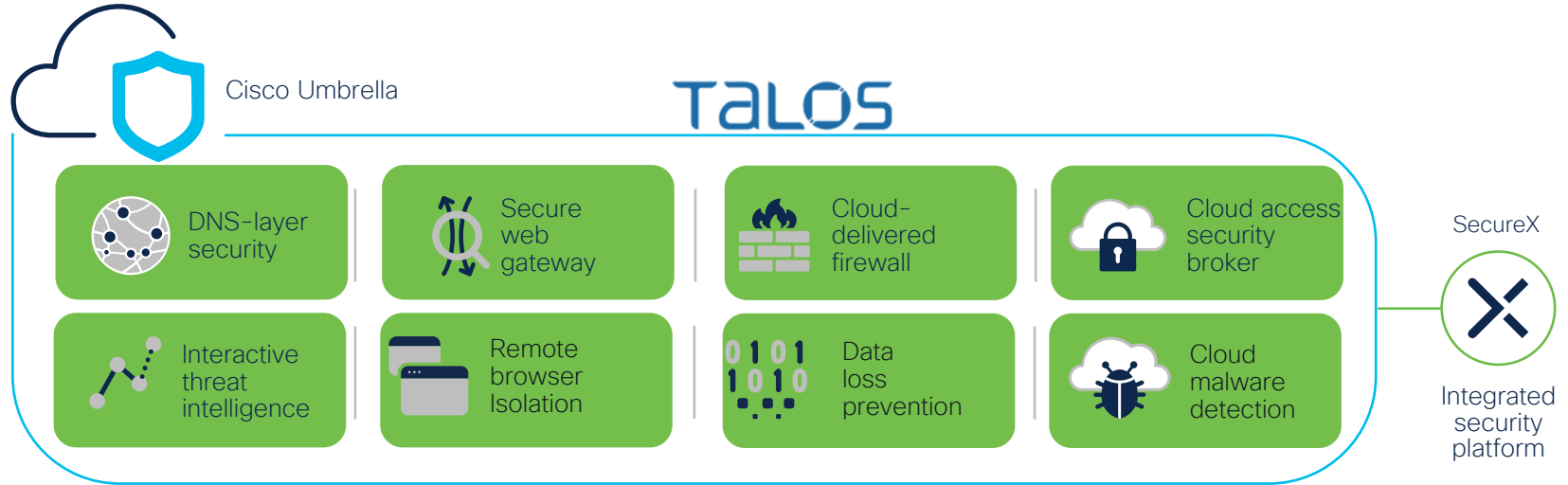
# Considerations for deployment

- With these DNS integrations, the DNS queries are intercepted by the MR/MX and sent to Umbrella.
- If you configure Umbrella resolvers, these are “known DNS resolvers” to the client (i.e. Chrome, Edge) and this can result in the browser auto-enabling DoH. Don’t do this.

# DNS Integrations Demo

# SIG Integrations

# Simplified connectivity from Meraki to Umbrella



# Cisco Umbrella key capabilities

Secure access to the internet & usage of cloud applications



## Visibility

- On & off corporate network
- All internet and web traffic
- All apps
- All devices
- SSL decryption
- Shadow IT
- Sensitive data transmitted

## Protection

- DNS-layer security
- Web inspection
- File inspection & sandboxing
- Non-web traffic inspection
- Remote browser isolation
- Data loss prevention
- Data at rest cloud malware scanning

## Control

- URL block/allow lists
- Port & protocol rules
- Granular app controls
- Content filtering
- App blocking
- Tenant controls



Built-in extended detection and response (XDR) platform with Cisco SecureX

# How do we help get you there? Flexibly

## Option I (Phase I)

---

Meraki MX + Umbrella SIG  
IPsec tunnel connectivity

Earlier



## Option II (Phase II)

---

Meraki MX + Umbrella SIG  
SD-WAN connectivity  
leveraging **Meraki AutoVPN**

2022



## Secure Connect Foundation

---

Meraki MX + Umbrella SIG  
SD-WAN connectivity  
leveraging **Meraki AutoVPN**  
Unified dashboard  
Unified support  
Increased scalability

Quotable

# Option I: How to

- Create Umbrella tunnels
  - Specify different credentials for each instance to tunnel
- Create Meraki IPsec tunnels
- Failover handled by AnyCast

### 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

CANCEL SAVE

### Organization-wide settings

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

Non-Meraki VPN peers ⓘ

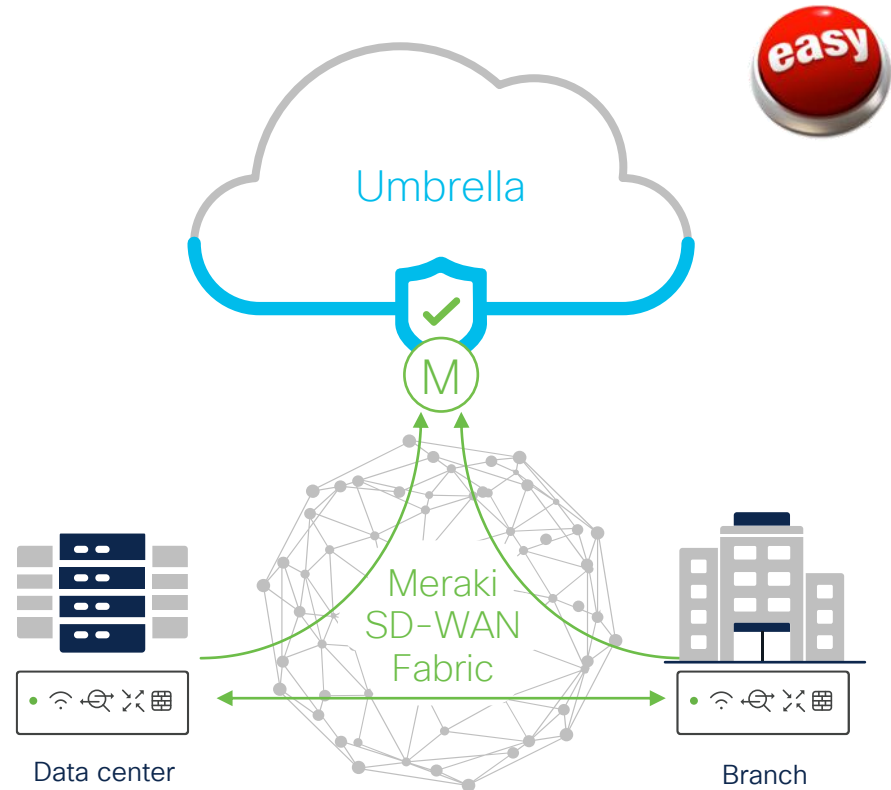
Name	IKE Version <small>BETA</small>	IPsec policies	Public IP	Local ID	Remote ID ⓘ	Private subnets	Preshared secret	Availability ⓘ	Actions
SIG1	IKEv2	Umbrella	146.112.82.8	TEST-SIG-MX1@2365:		0.0.0.0/0	.....	SIG x	⊕ ✕

[Add a peer](#)



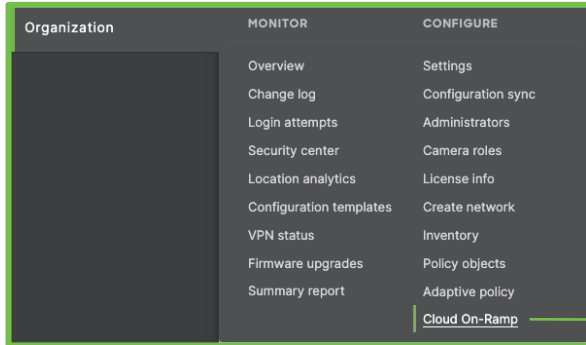
# Option II: Extend Meraki's SD-WAN into the Umbrella cloud

- Meraki SD-WAN directly to Umbrella with **Auto VPN** in < 5 minutes!
- Flexible security options
- Native SD-WAN traffic engineering
- More intelligent path selection with zero additional cost
- Global coverage



# A few clicks to connect Meraki MX to Umbrella

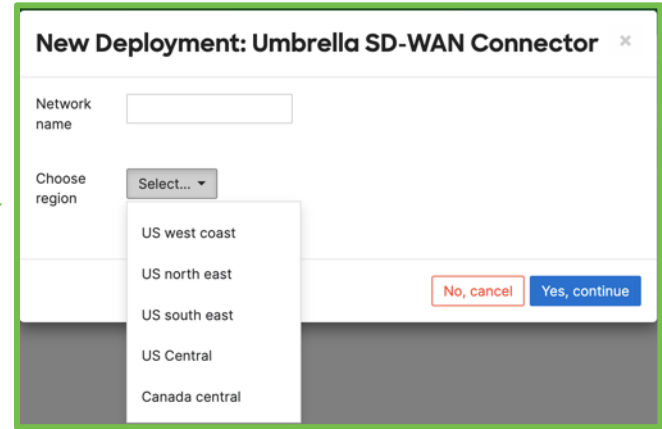
- Connect to Cisco Umbrella
- Choose your region
- Establish Auto VPN tunnel to Umbrella
- Establish the connections in S2S VPN



## Cloud On-Ramps

Configuration Deployments

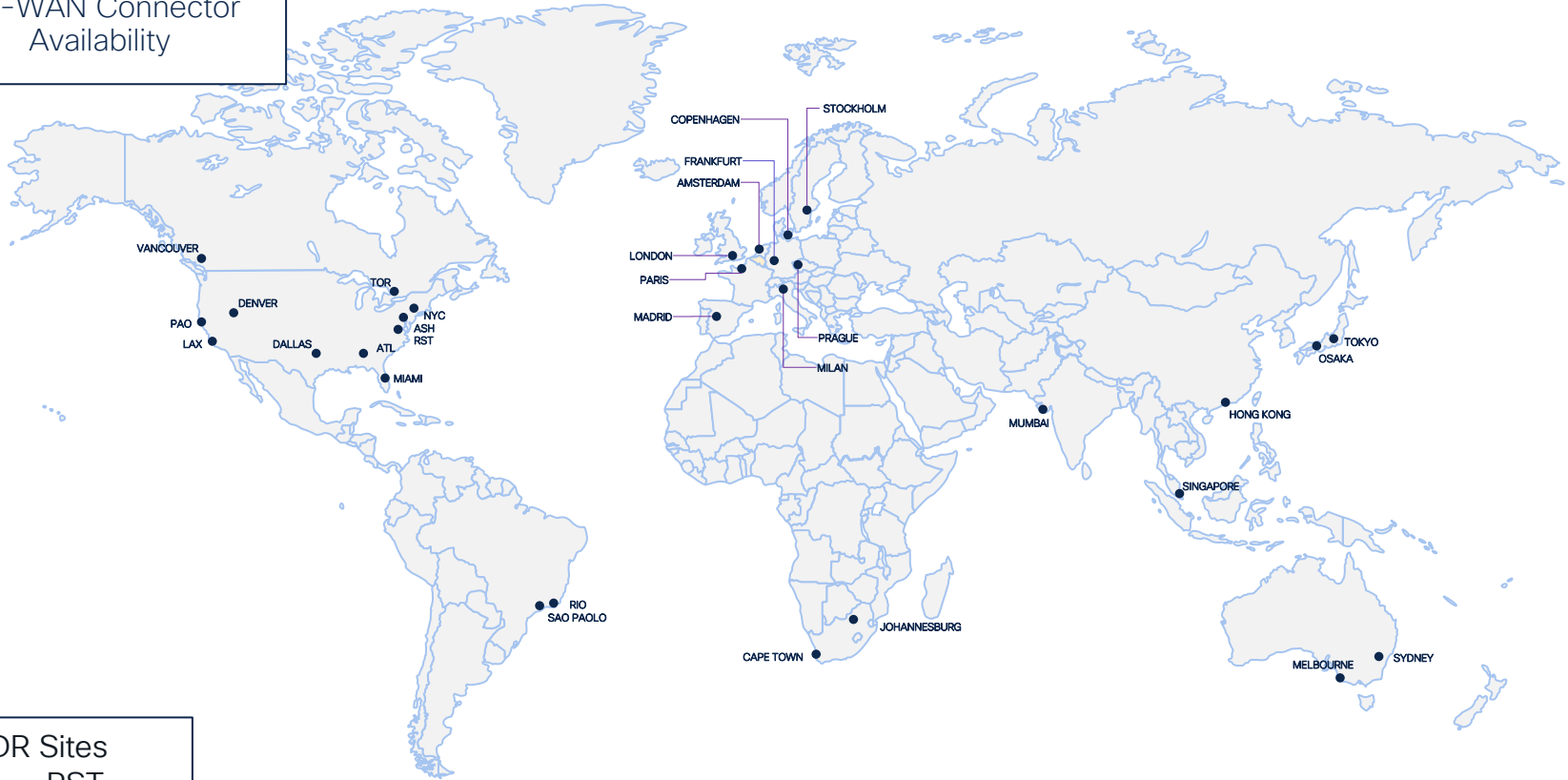
### Umbrella SD-WAN Connector



# Capacity and scaling recommendations

- The Meraki SD-WAN deployment limit is dynamic and dependent on the number of networks in the Meraki organization
- We recommend 1 deployment for organizations with less than or equal to 20 networks (sites). Additional deployments are automatically available for every 20 networks up to 400 networks
- If a customer's environment exceeds this threshold or if exceptions to this automated scaling are required, reach out to your sales/support team for additional deployments
- **Note:** A deployment is two connectors for high availability purposes, one primary and one secondary. Each pair supports up to 250Mbps.

# SD-WAN Connector Availability



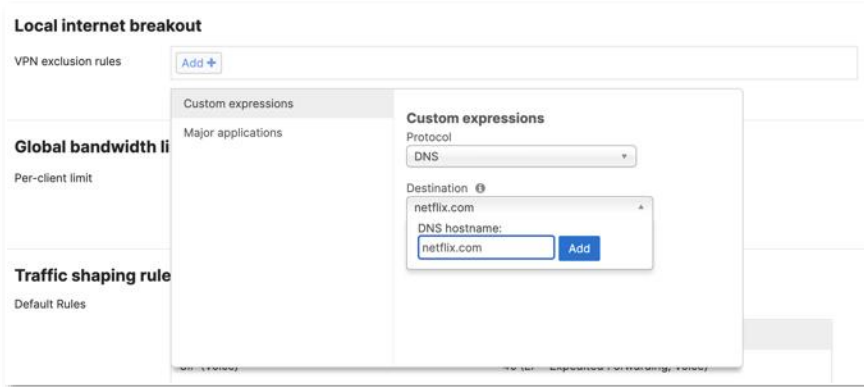
## DR Sites

- RST
- AMS
- OSA

# Easily Exclude Traffic

- VPN Exclusions can be used to easily exclude traffic from going down the tunnel to Umbrella
- This traffic can still be protected at the DNS layer

## By traffic – DNS/TCP/UDP/ICMP

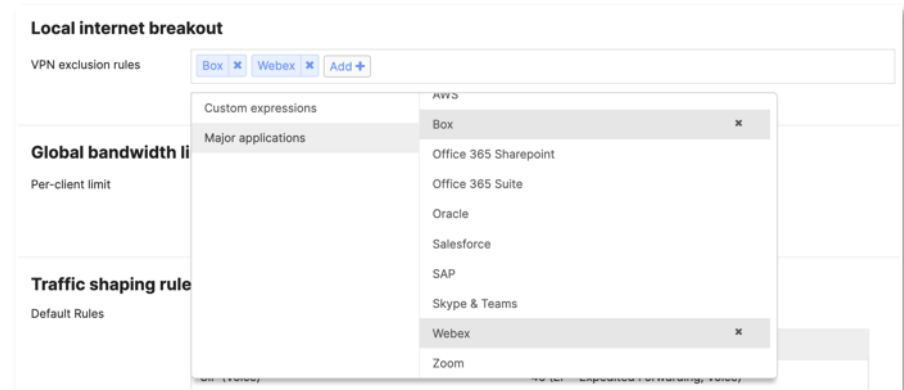


The screenshot shows the 'Local internet breakout' configuration page. Under 'VPN exclusion rules', there is an 'Add +' button. A 'Custom expressions' dialog box is open, showing the following configuration:

- Protocol: DNS
- Destination: netflix.com
- DNS hostname: netflix.com

The 'Add' button is highlighted in blue.

## By Application (with SDWAN+ License)



The screenshot shows the 'Local internet breakout' configuration page. Under 'VPN exclusion rules', there are buttons for 'Box', 'Webex', and 'Add +'. A list of applications is displayed, including:

- Box
- Office 365 Sharepoint
- Office 365 Suite
- Oracle
- Salesforce
- SAP
- Skype & Teams
- Webex
- Zoom

The 'Box' and 'Webex' buttons are highlighted in blue.

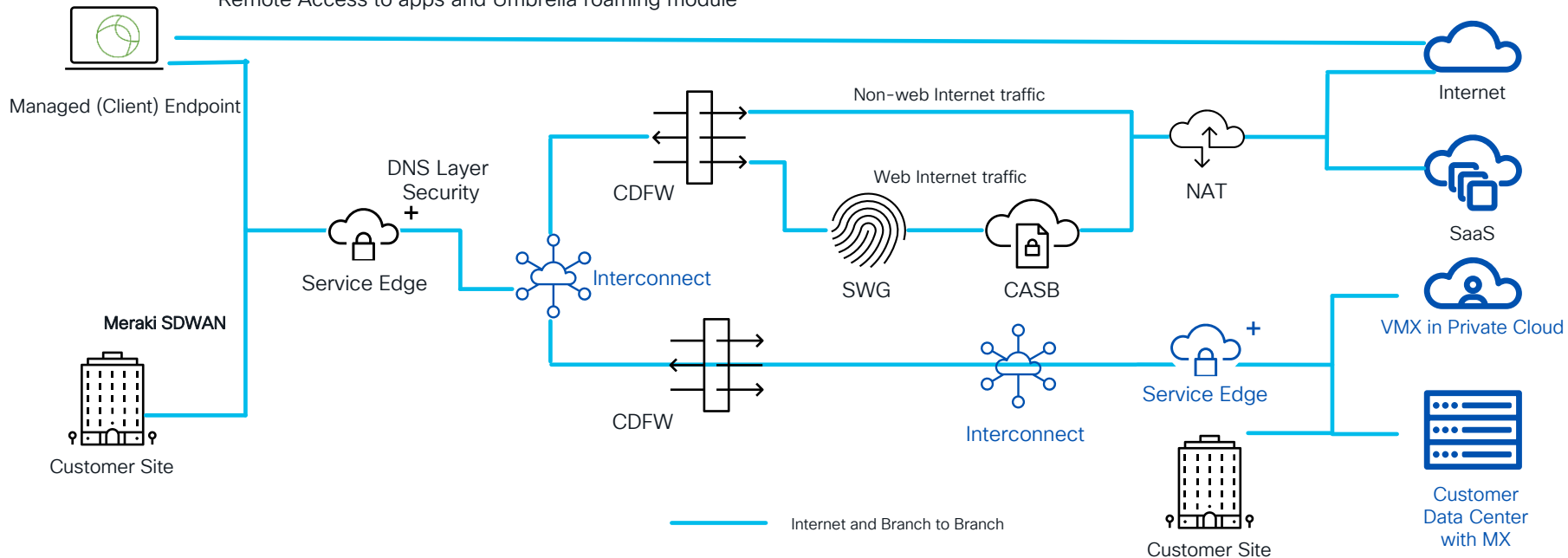
# Secure Connect Foundation

- Secure Internet Access (SIA) and Meraki Secure branch-to-branch Access
- Streamlined dashboard experience for Meraki and Umbrella
- Quick onboarding with Meraki Auto-VPN
- Enables enhanced bandwidth with ability to scale dynamically up to 500 Mbps per Meraki branch integrating using AutoVPN
- One 24/7 support for Cisco+ Secure Connect

Note: Migrate to Foundation license from Umbrella SD-WAN Connector (SIG license) at no cost

# Foundation Overview

Enable remote access trial with 10 free users on Client-based Remote Access to apps and Umbrella roaming module



# Meraki Branch Interconnect (cont'd)

## Capabilities

- Supports VPN exclusions for direct internet access
- Automatic intelligent path selection based on traffic

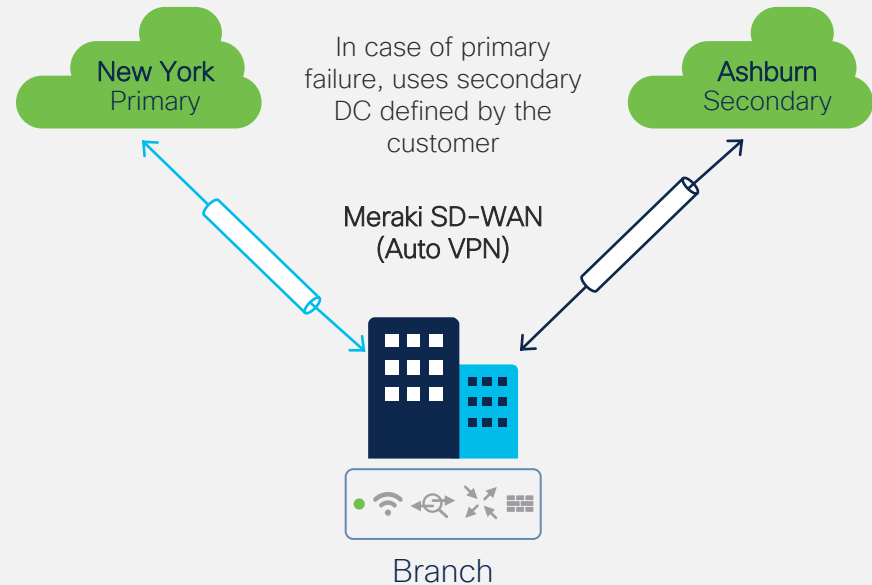
## High availability

- Predefined DC pairs, a primary and a secondary
- Failover handled by the Meraki® SD-WAN fabric

## Security

- Flexible security options  
**Example:** Block unwanted traffic at the MX and inspect the rest in Secure Connect

## Example: US-2





# Traffic Acquisition

Increased performance and scalability with lower footprint



Enhanced performance and optimized capacity with dynamic bandwidth scaling of up to 500Mbps per branch



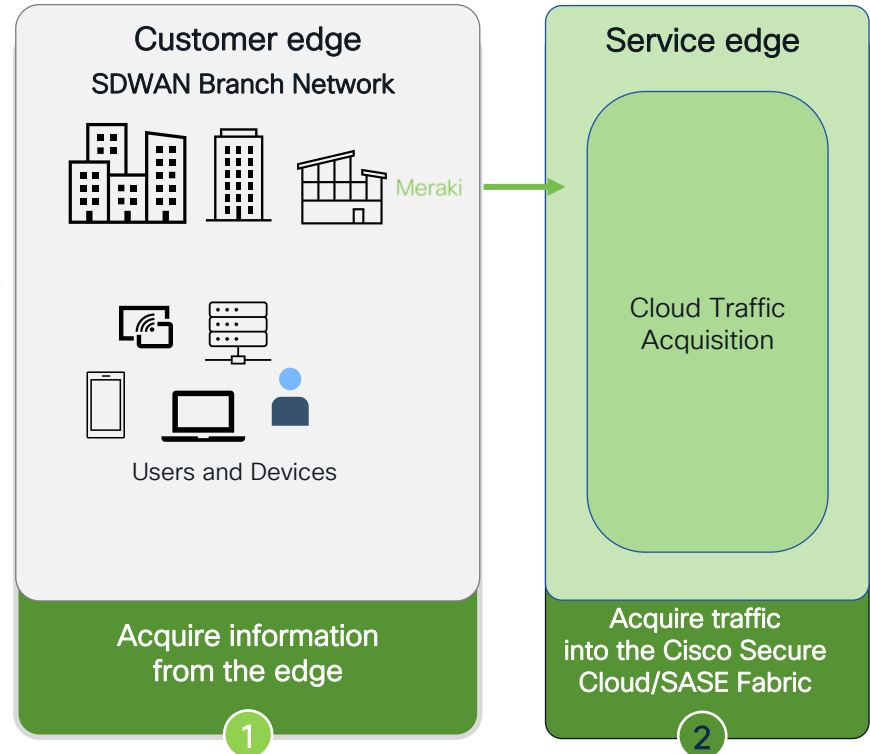
Standardizing traffic acquisition for SD-WAN and any other connectivity to the cloud fabric



Simplifying admin experience, reducing manual deployments and load balancing



Streamlined regional deployments, reducing the number of configuration templates.



# Cisco+ Secure Connect Use Cases

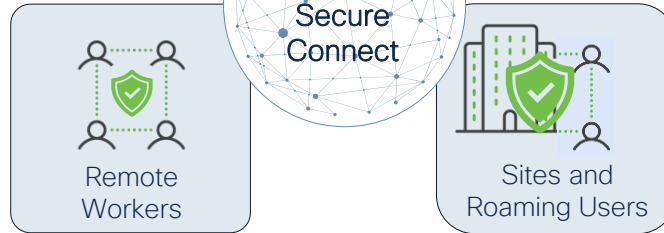
## Secure Internet Access

Enhance security for all Internet access with cloud-based advanced protection from malware, phishing attacks, and other advanced threats.



## Secure Remote Access

Remote workers consume Internet and corporate apps via global cloud fabric. Managed devices tunnel traffic with Secure Client while unmanaged devices use a browser to safely access private apps.



## Secure Private Access
























Define policy to control branch workers access to private apps behind data center, private or public cloud, or branches.

## Site Interconnect

Interconnect sites, branch users, and apps using native Cisco SD-WAN integrations, standard IPsec VPN support and direct SaaS and IaaS Peering.

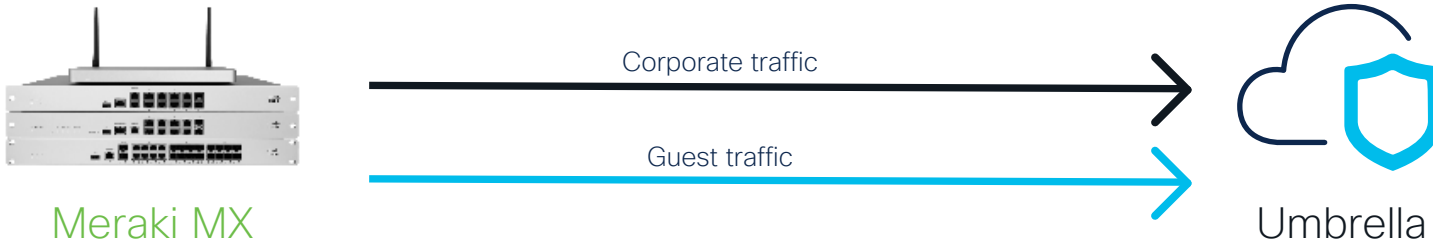
# Secure Connect Foundation Demo

# Meraki Network Integrations Comparison

	Customizable DNS Policies	Umbrella Dashboard	Remote User Protection	Encrypted Traffic	Additional Visibility	SIG Integration	SD-WAN Capabilities	VPN Exclusions
MR-ADV					SSID, internal IP			
MR/MX & Umbrella DNS					SSID, internal IP			
Option 1 / IP SEC Tunnels					Internal IP, tunnel ID, user (SAML)			
Option 2 / AutoVPN / SCF					Internal IP, tunnel ID, user (SAML)			Yes, by hostname, IP, application

# Flexible deployment & policies to meet needs

## Competitive advantage



Traffic type	Deployment	Feature requirements
Corporate traffic	Option I, Option II, Secure Connect Foundation	Full logging Deep inspection and controls
Trusted high performance sites	DNS security (license required)	Threat protection and attribution
Guest traffic	DNS security (license required)	Threat protection and attribution

# Better Together

SD-WAN	●
East-west security filtering	●
Layer 7 firewall	●
IDS/IPS	●
Content filtering	●
Malware protection	●
Sandboxing	●
Centralized enforcement, policy & reporting	●
Remote User Protection	●
DNS Security	●
Unlimited SSL decryption/inspection	●
Data loss prevention (DLP)	●
Remote Browser Isolation (RBI)	●
Granular app security controls	●
File type control	●
SaaS Tenant Restrictions	●
CASB	●



# Security Technologies

## Secure Access Service Edge (SASE)

Learn how Secure Access Service Edge combines networking and security functions in the Cloud to deliver seamless, secure access to applications, anywhere users work. Core functions include software-defined wide area network, secure web gateway, firewall as a service, cloud access security broker, and zero-trust network access. The SASE model aims to consolidate these functions in a single, integrated cloud service.

START

Feb 6 | 08:30

### **TECSEC-3780**

Cisco SASE for Architects and Implementation Engineers

Feb 7 | 08:30

### **BRKSEC-2128**

SASE the SOCs New Best Friend

Feb 7 | 14:45

### **BRKSEC-2238**

Getting SASE with Umbrella and Meraki - Understand best practices for simple and flexible integrations between Meraki and Umbrella

Feb 7 | 15:30

### **BRKSEC-2143**

Do You Know Where Your Data Is? A Deep Dive on Cisco Umbrella CASB and DLP and How to Protect your Locations, Data and Users

Feb 7 | 15:30

### **BRKSEC-2129**

Deploy & Scale SASE for Secure Remote Worker in the Cloud with Cisco+ Secure Connect

Feb 7 | 17:00

### **BRKSEC-2438**

Solving Today's Challenges with the Newest Features in Cisco Umbrella

Feb 8 | 08:30

### **BRKOPS-2857**

Deploy Visibility in Your SASE Architecture With ThousandEyes

Feb 8 | 08:45

### **BRKSEC-2644**

Secure Access Service Edge - From Home to the Office with Cisco SASE!

Feb 8 | 10:30

### **BRKSEC-2287**

Who is Behind the Umbrella? A View on User Authentication with Cisco Umbrella



Feb 9 | 12:00

### **BRKENT-2312**

Evolution of Cisco SD-WAN Security and Journey Towards SASE

If you are unable to attend a live session, you can watch it [On Demand](#) after the event

BRKSEC-2238

**CISCO** *Live!*

# Engage with us. Become a **Cisco Meraki Insider**.



**Join**  
the community



**Complete**  
challenges



**Receive**  
rewards



# Fill out your session surveys!



Attendees who fill out a minimum of four session surveys and the overall event survey will get **Cisco Live-branded socks** (while supplies last)!



Attendees will also earn 100 points in the **Cisco Live Challenge** for every survey completed.



These points help you get on the leaderboard and increase your chances of winning daily and grand prizes

# Continue your education

CISCO *Live!*

- 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](http://www.CiscoLive.com/on-demand)



The bridge to possible

# Thank you

CISCO *Live!*

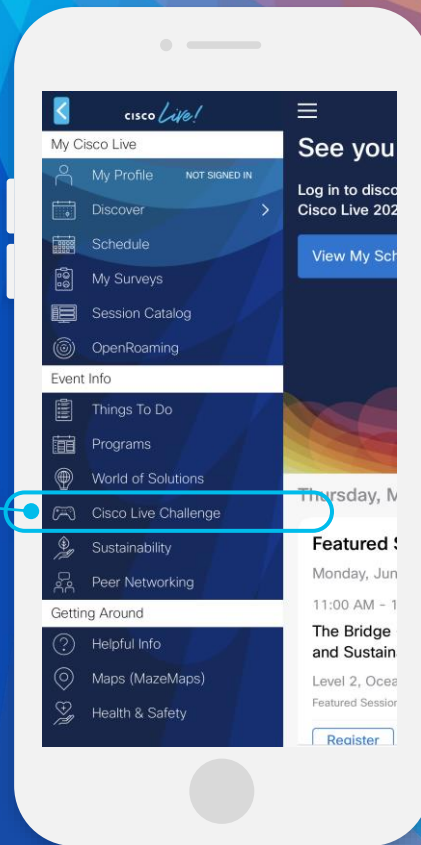
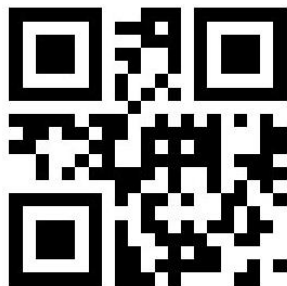
#CiscoLive

# Cisco Live Challenge

Gamify your Cisco Live experience!  
Get points for attending this session!

## How:

- 1 Open the Cisco Events App.
- 2 Click on 'Cisco Live Challenge' in the side menu.
- 3 Click on View Your Badges at the top.
- 4 Click the + at the bottom of the screen and scan the QR code:



The Cisco Live! logo features the word "CISCO" in a bold, black, sans-serif font, followed by "Live!" in a black, cursive script font. The background of the entire image is a vibrant, multi-colored abstract pattern of overlapping, wavy bands in shades of red, orange, yellow, green, and blue, radiating from a bright white center on the right side.

CISCO *Live!*

Let's go

#CiscoLive