

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC



Empower Your Meraki SD-WAN

Unleashing Unified SASE with Cloud-Driven Secure Connect

Anthony Netkow
Account Executive - Networking
BRKENT-2123

CISCO *Live!*

#CiscoLiveAPJC

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

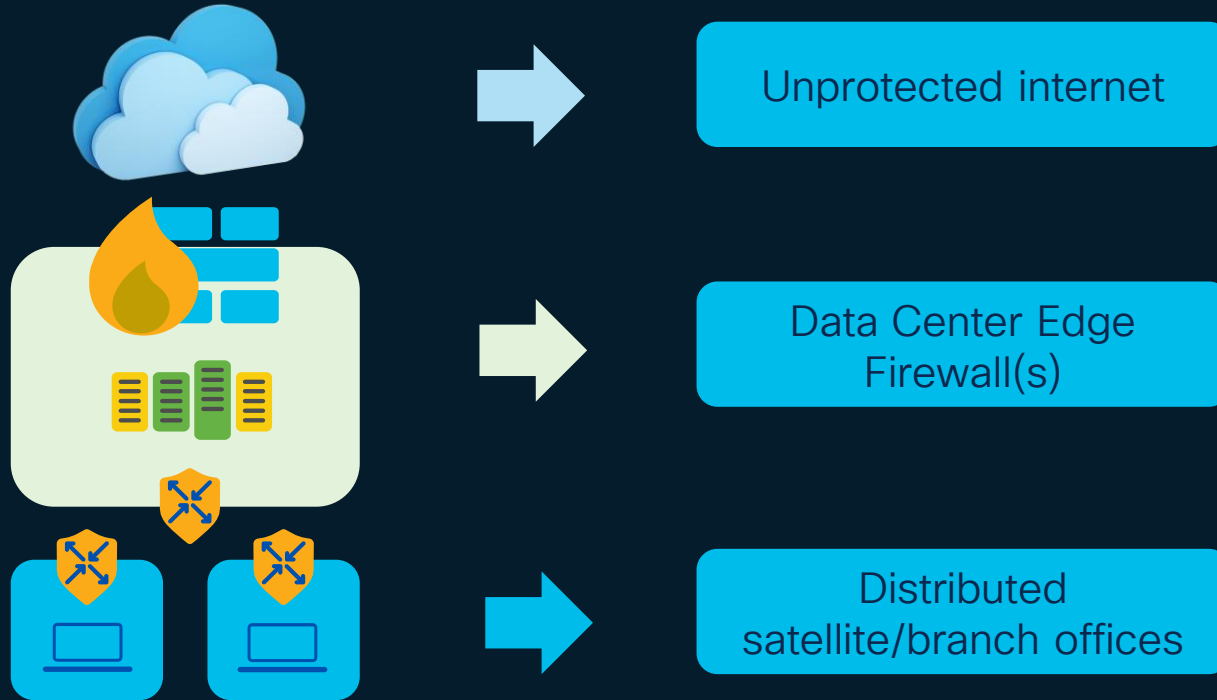
Webex spaces will be moderated by the speaker until November 15, 2024.



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKENT-2123>



Castle-and-Moat Security



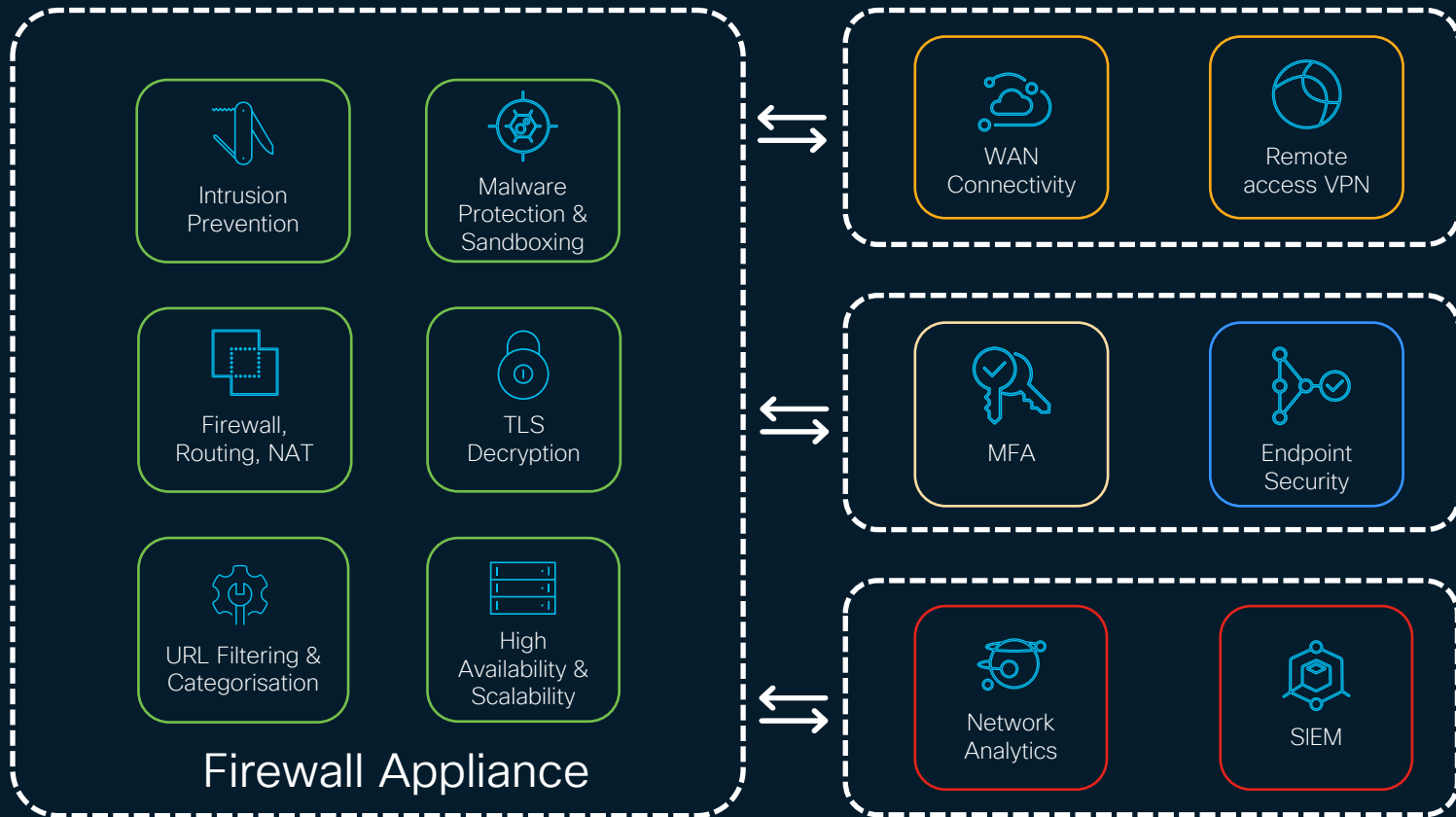
Castle-and-Moat Security



Multiple Disparate Security Solutions



Multiple Failure Domains



2024 Cisco Cybersecurity Readiness Index

Underprepared and Overconfident: Companies Tackle an Evolving Landscape

Cisco's second annual Cybersecurity Readiness Index is an updated guide that addresses the current global cybersecurity landscape and assesses how ready organizations are to face today's cybersecurity risks.

[Download full report](#)

[Introduction](#)
[Measuring Readiness](#)
[Recommendations](#)
[Methodology](#)
[Learn More](#)

Are companies prepared to face today's cybersecurity risks?

In an era of hyperconnectivity, artificial intelligence (AI), distributed work environments, and advanced threat actors, companies face a complicated and diverse threat landscape that goes far beyond ransomware and phishing. In fact:

Attacked

54%

have experienced a cybersecurity incident in the past year.



73%

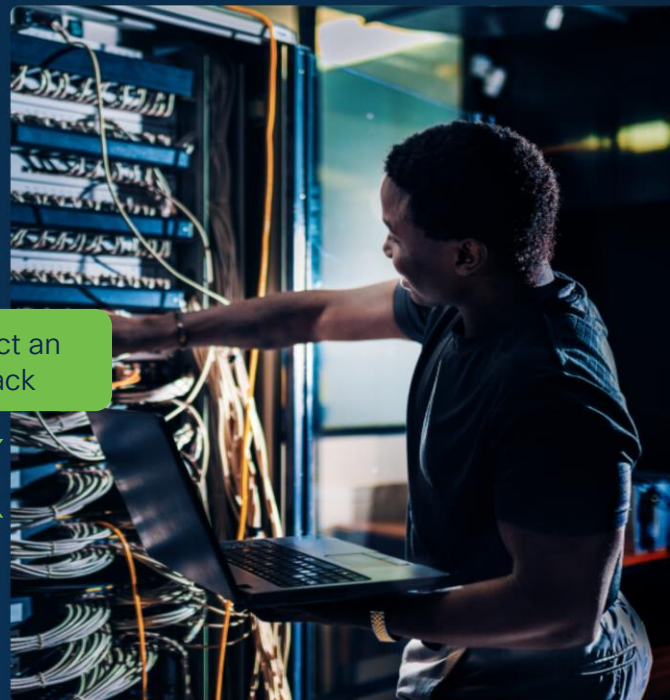
believe a cybersecurity incident will disrupt their business in the next 12-24 months.



Expect an attack

Despite this, **only 3% of organizations are assessed as having a Mature** stage of cybersecurity readiness in 2024. Additionally, 71% of organizations fall in the two least prepared categories.

The Cybersecurity Readiness Index provides a comprehensive view of what organizations need to tackle, in order to address the security challenges of the modern world. We found that the evolving threat landscape, resource challenges, and complexity of networks, cloud and applications are taking a toll on today's organizations.



Measuring Readiness

Cisco surveyed over 8,000 private sector business leaders who have cybersecurity responsibilities in their organizations across 30 global markets to gain insight into cybersecurity readiness based on the five pillars that are most relevant to securing today's organizations:



Identity
Intelligence



Network
Resilience



Machine
Trustworthiness



Cloud
Reinforcement



AI
Fortification

When it comes to global cybersecurity readiness...

80%

of companies feel moderately to very confident in their ability to stay resilient amidst this evolving cybersecurity landscape.

46%

of companies have more than 10 unfilled cybersecurity roles on their teams at the time of the survey.

80%

of companies admit that having multiple point solutions is slowing down their team's ability to detect, respond to, and recover from incidents.

36%

of companies rank Identity Protection as their organization's top cybersecurity challenge.

Too many solutions with fewer people to manage it



46%

of companies have more than 10 unfilled cybersecurity roles on their teams at the time of the survey.

fewer people



80%

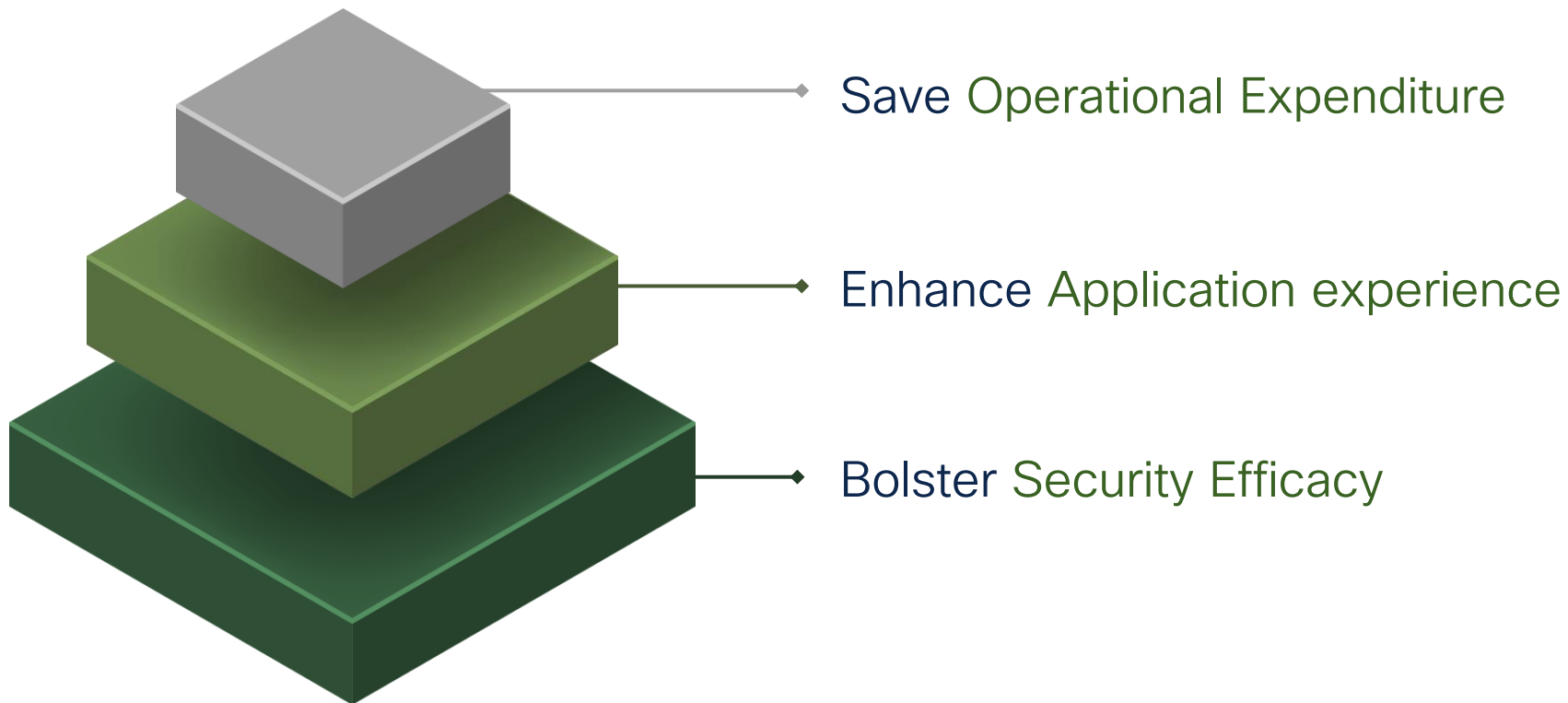
of companies admit that having multiple point solutions is slowing down their team's ability to detect, respond to, and recover from incidents.

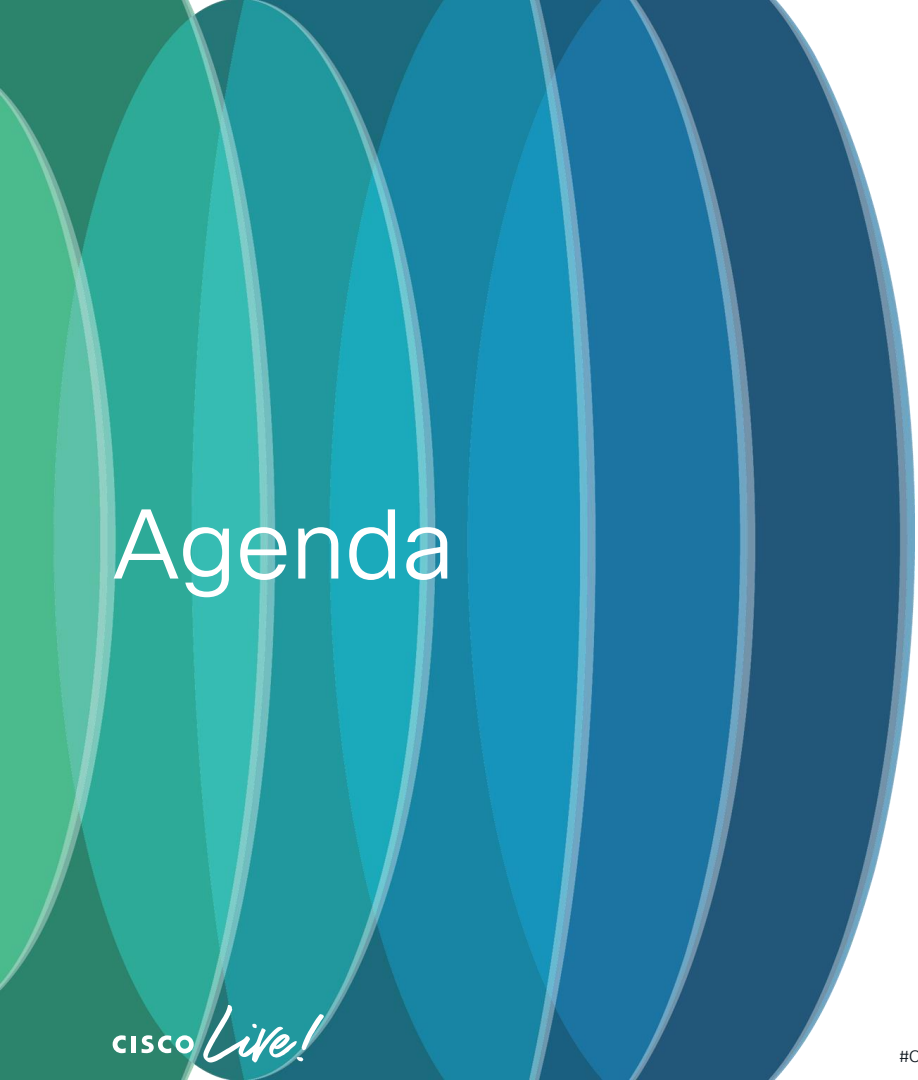
Too many solutions

Source : [Cisco cybersecurity readiness index 2024](#)

Cisco wants to

Simplify Network and Security operations





Agenda

Save **Operational Expenditure**

Enhance **Application experience**

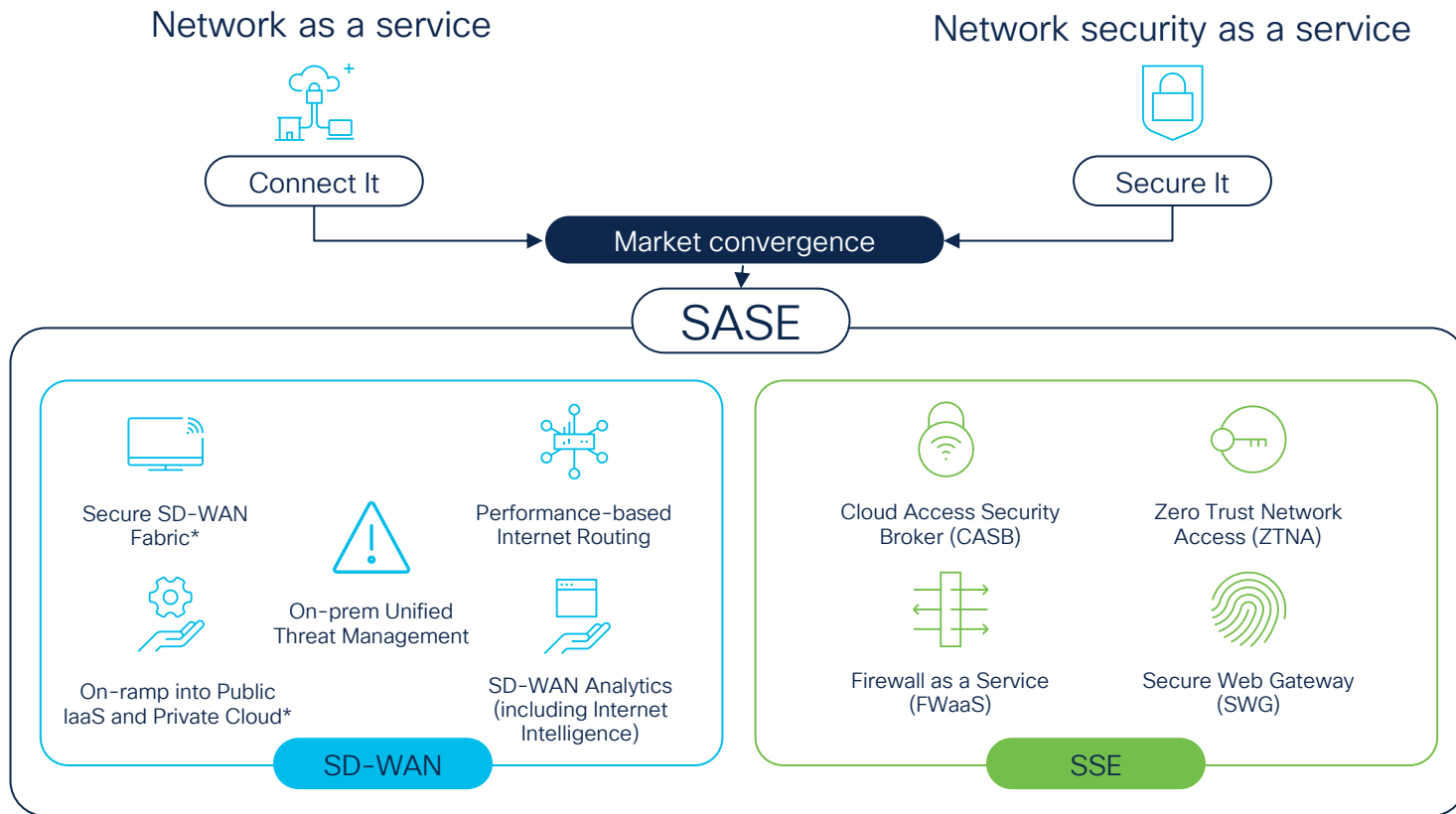
Bolster **Security Efficacy**

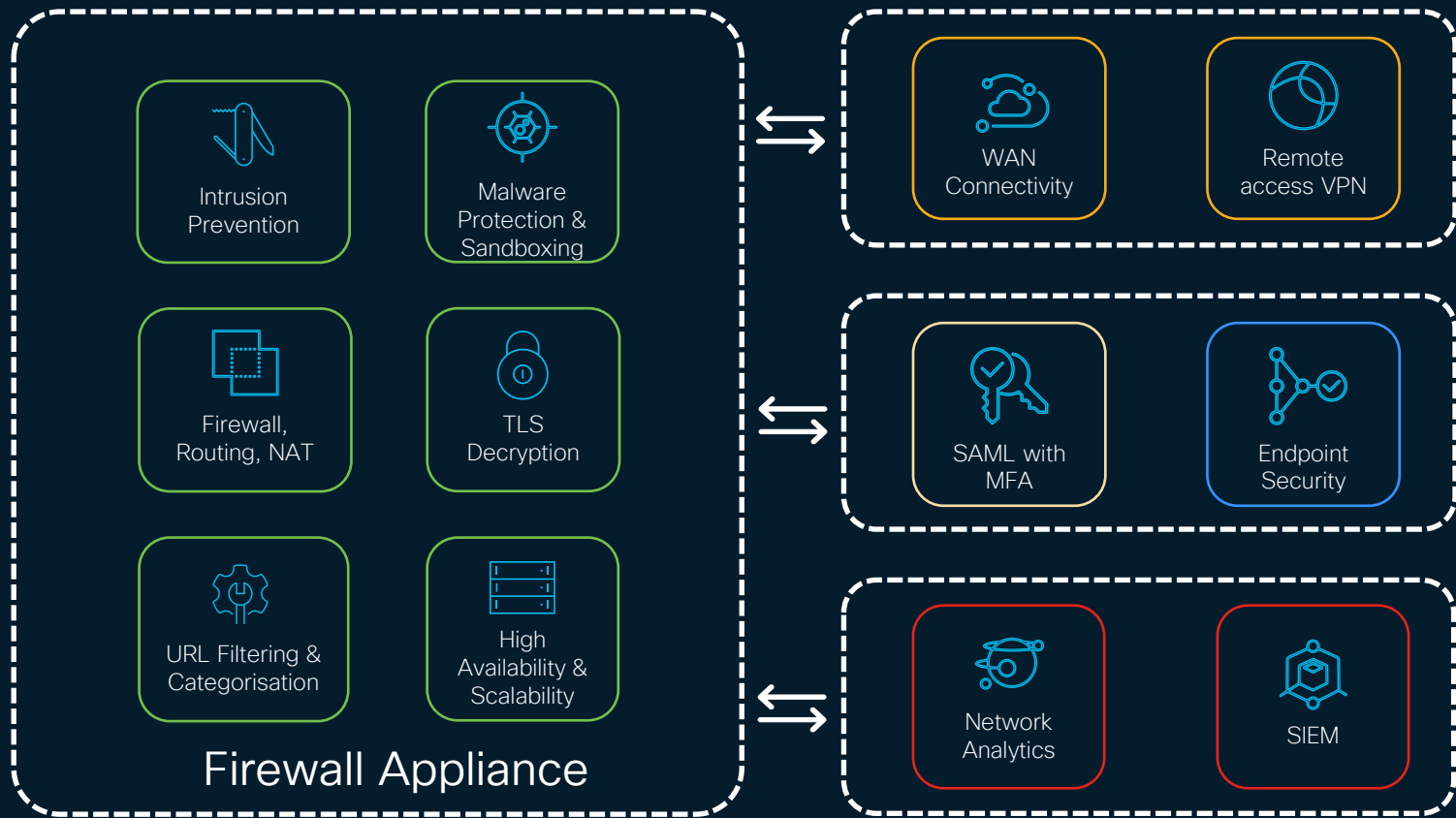
Anthony Netkow



- Cisco Live veteran – 10+ years
- Austin, Texas → Melbourne
- Account Executive covering VIC/SA Commercial, Enterprise, and Public Sector
- Former Meraki SE
- Please talk to me about
 - All things Meraki & Catalyst
 - Solar/Battery Tech
 - EVs
 - Cycling

Secure Access Service Edge (SASE) Architecture





Cisco Meraki and
Catalyst SD-WAN

Cisco Umbrella Cloud
Security

Multiple services wrapped into one product
Cisco Secure Malware
Analytics

Cisco Secure Client
VPN

Cisco Secure Access



Intrusion
Prevention



Malware
Protection &
Sandboxing



WAN
Connectivity



Remote
access VPN



DNS Filter



Firewall,
Routing, NAT



TLS
Decryption



SAML with
MFA



Endpoint
Security



CASB and
DLP



URL Filtering &
Categorisation



High
Availability &
Scalability



Network
Analytics



SSE Engine



ZTNA

Cisco Meraki Platform

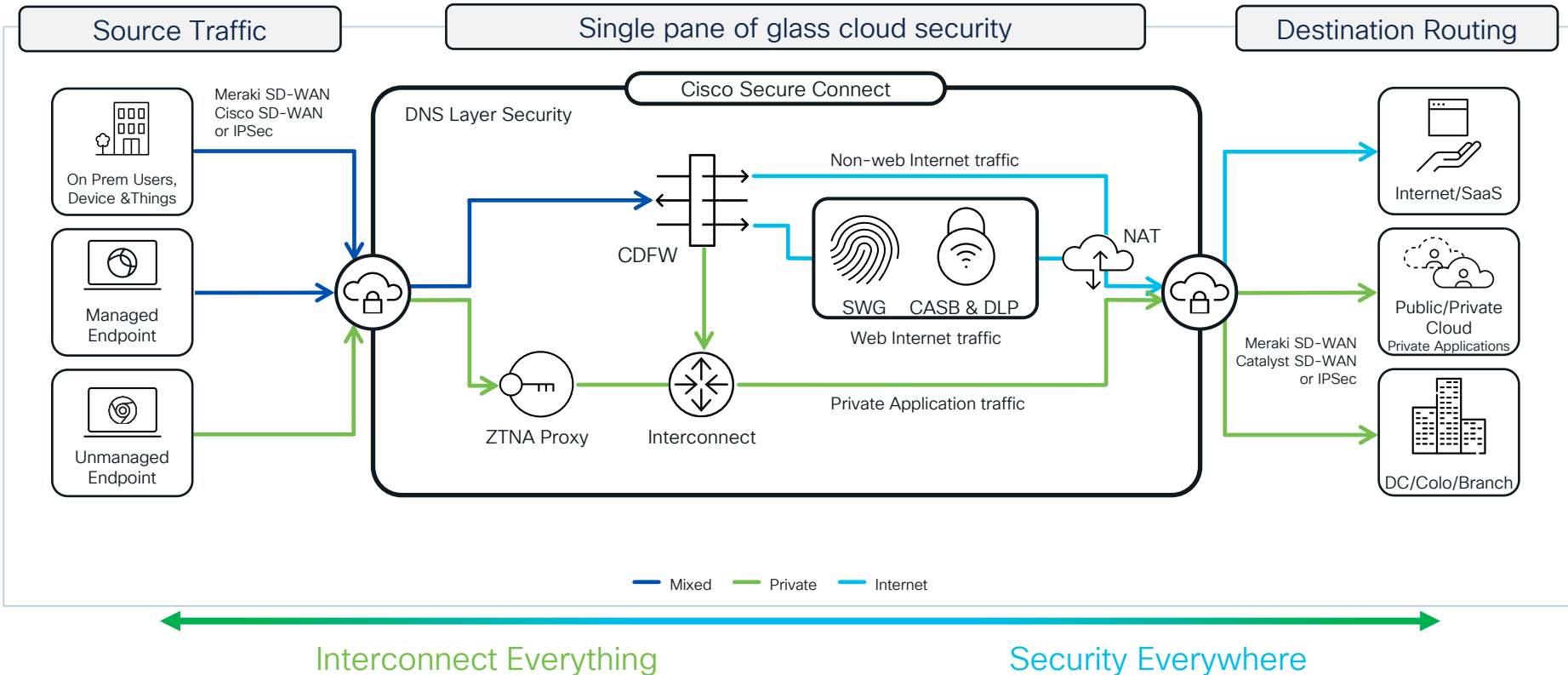
Secure Connect architecture

Secure Internet Access

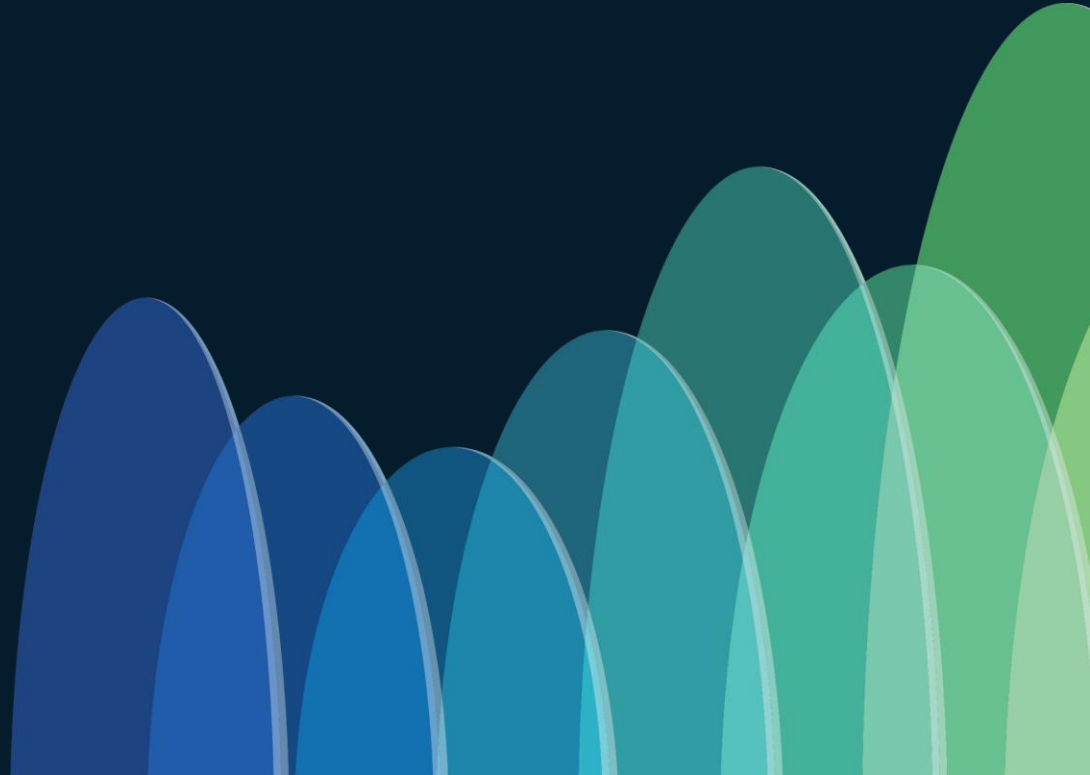
Secure Remote Access

Site Interconnect

Secure Private Access



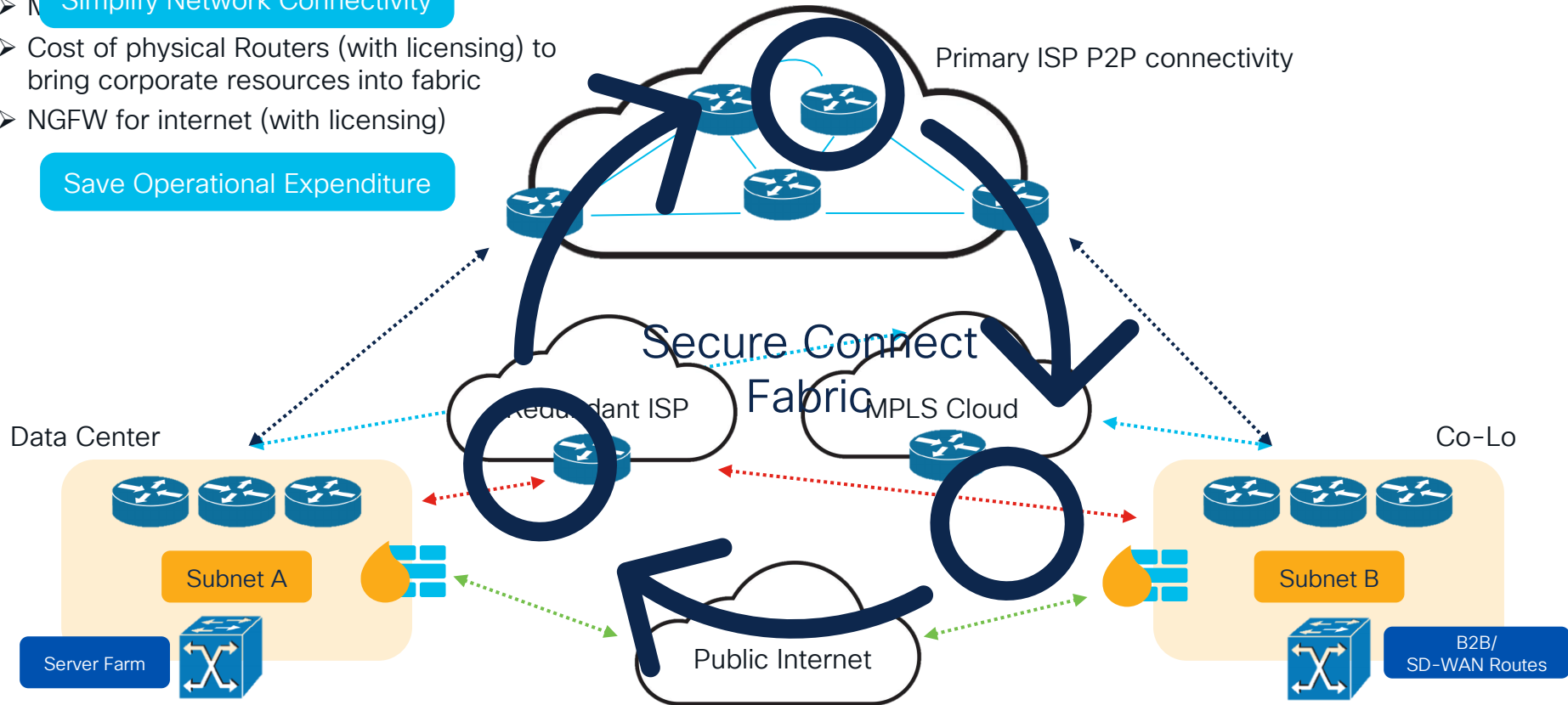
Branch and Hub connectivity



- Primary ISP Service cost
- Secondary ISP Service cost
- **Simplify Network Connectivity**
- Cost of physical Routers (with licensing) to bring corporate resources into fabric
- NGFW for internet (with licensing)

Save Operational Expenditure

DC-DR interconnects



Over 1000 extensive
and expanding
Peering Relationships

Proximity to Internet
Exchange Points
(IXPs)

Self-healing; Highly
automated
architecture using
global load balancers
and auto-scale
technology

Data centers meet or
exceed standards for
security and uptime



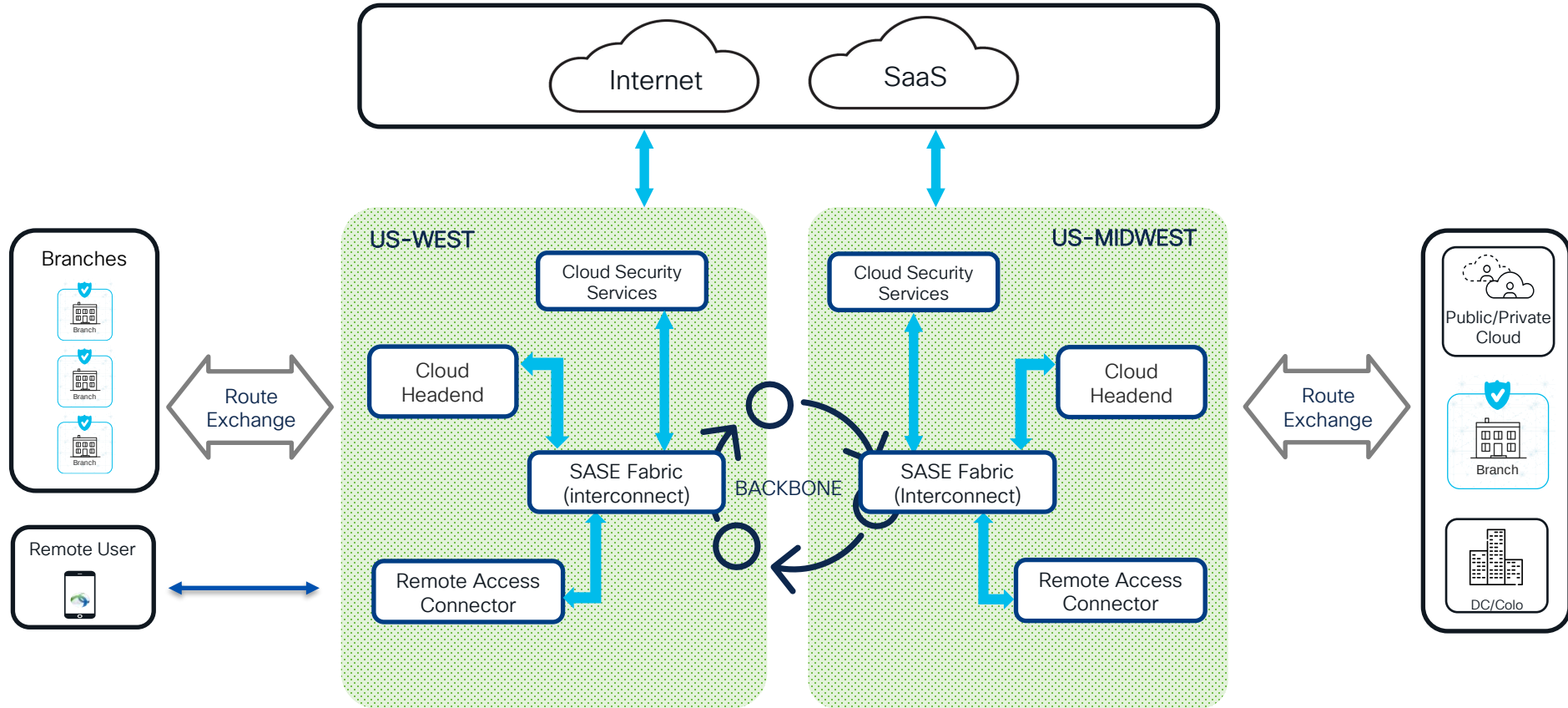
Some of our peering partners



Sources :
[Cisco Umbrella Global Cloud Architecture](#)
[Anycast Routing and Cisco Umbrella](#)

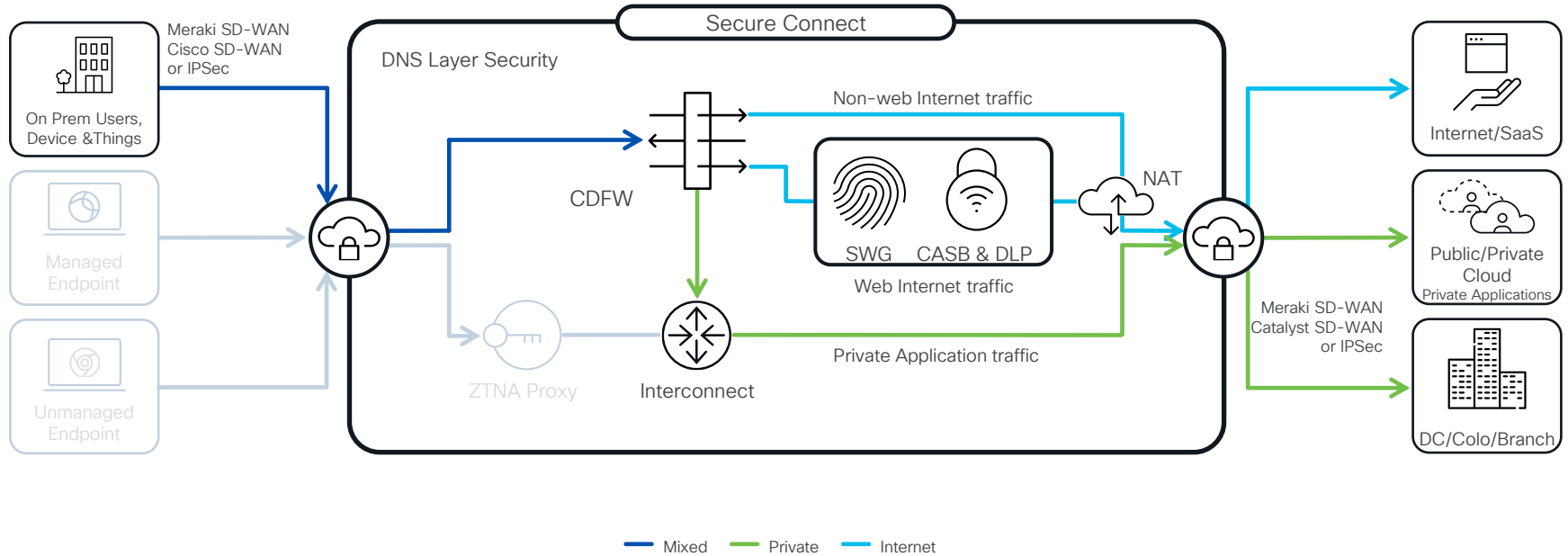
CISCO *Live!*

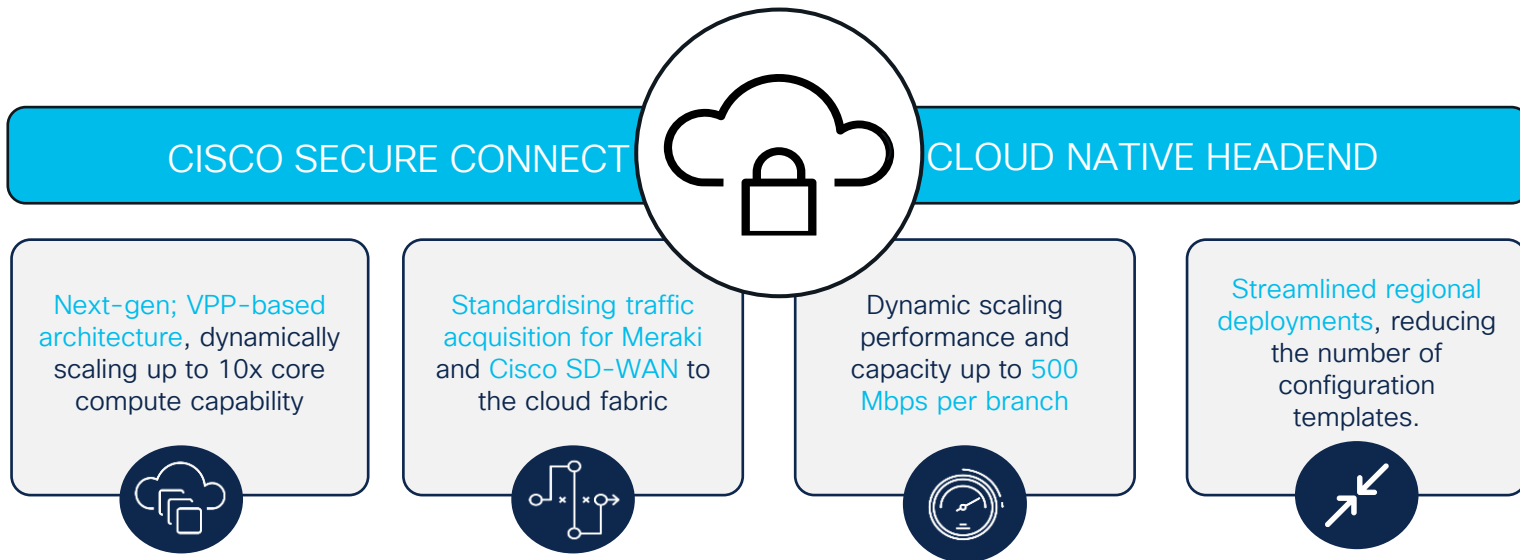
Secure Connect multi-region interconnect



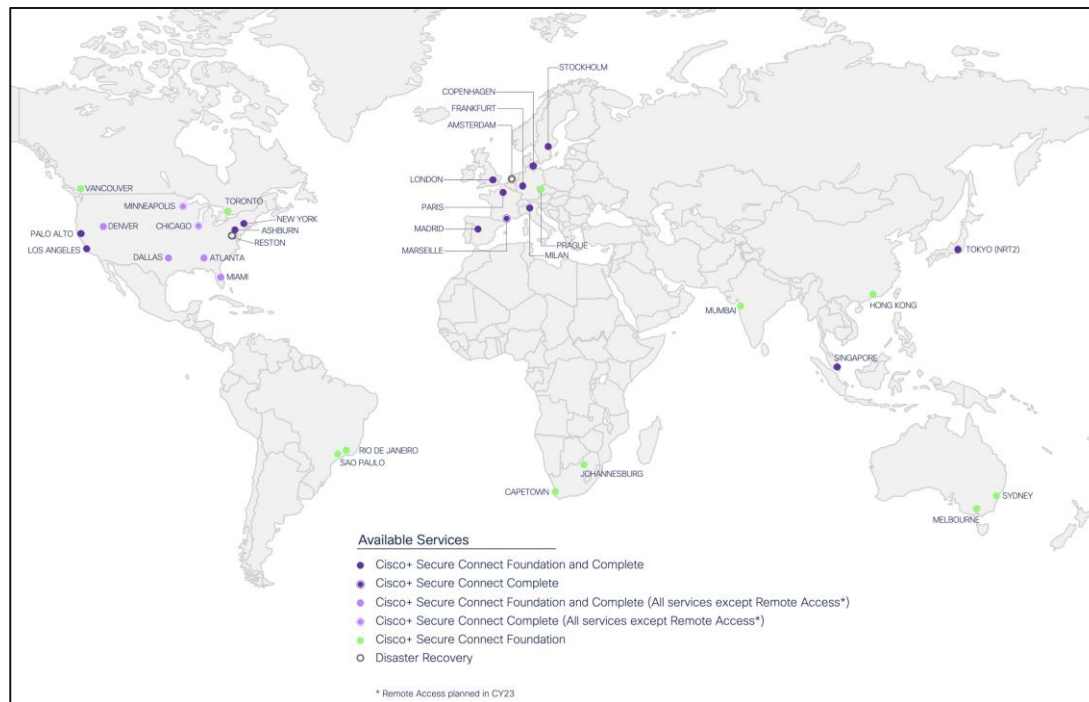
SecureConnect

Secure Branch Traffic





Cisco Secure Connect SD-WAN Data Centers



Cancel Assign to Region or Cloud Hub ▾

Assign site directly to these regions
Internet & Private App Access

US West
Los Angeles/Palo Alto

US Northeast
New York/Ashburn

US Central
Denver/Dallas

US Southeast
Atlanta/Miami

US Midwest
Minneapolis/Chicago

Europe-1
London/Frankfurt

Europe-2
Paris/Marseille

Europe-3
Madrid/Milan

Europe-4
Stockholm/Copenhagen

Asia-1
Narita/Singapore

Australia-1
Melbourne/Sydney

Assign site to Cloud Hub in these regions
Up to 22 Cloud Hubs can be deployed.

Configure Cloud Hubs for Internet Access in additional regions like Canada, Asia, and more

[Configure Cloud Hubs](#)

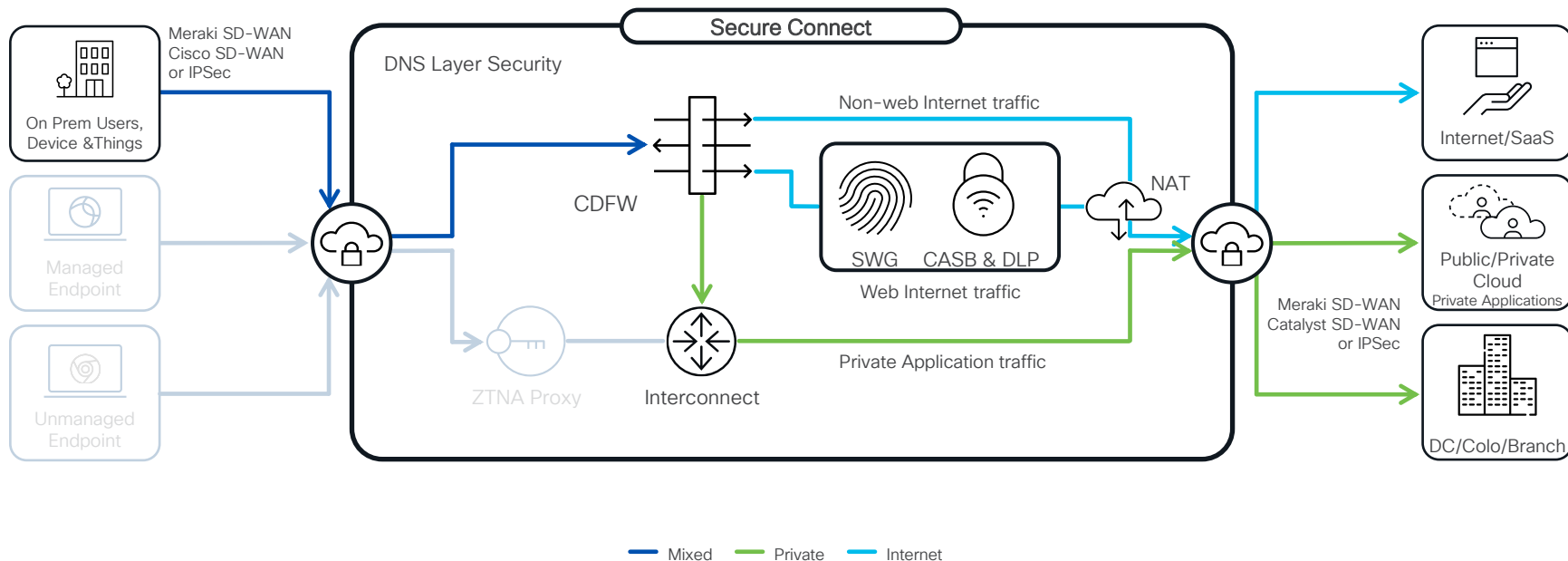
Internet & Private
Access with
Enhance SC Cloud
Headend



Internet Access Only
with Cloud Hubs

[Link](#) to updated Meraki documentation page

Bringing sites into Secure Connect



Meraki SD-WAN to Secure Connect region

Region : US Northeast

Traffic Shaping

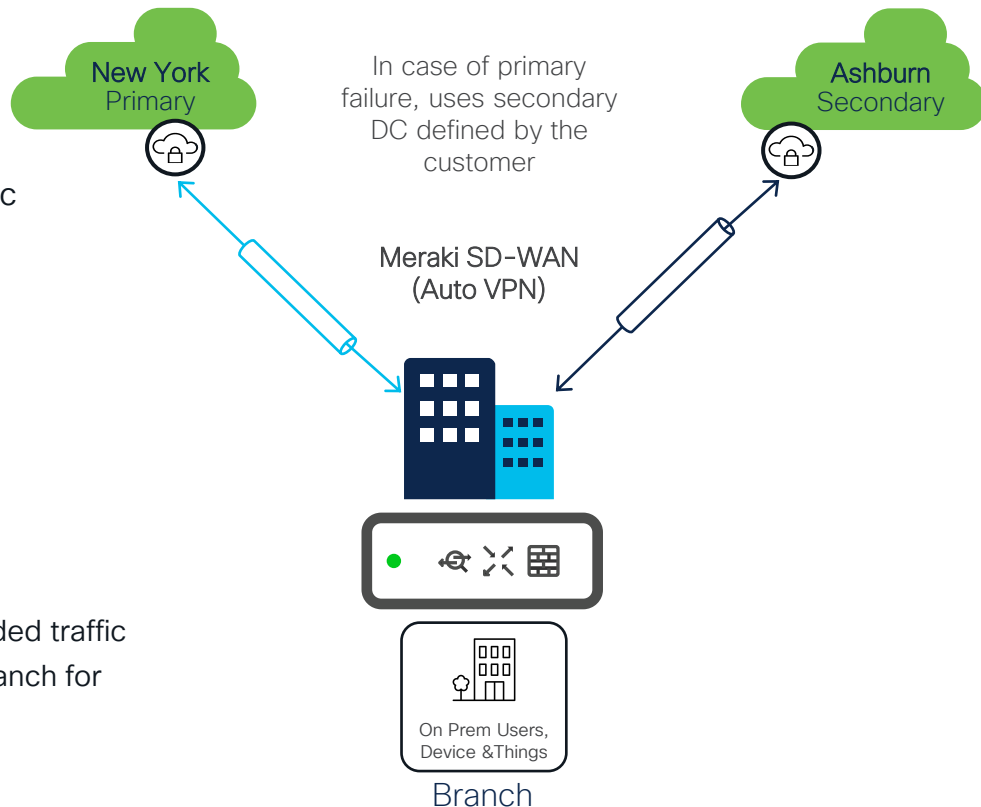
- Supports [VPN exclusions](#) for direct Internet access and use of inbound NAT
- [Automatic intelligent path selection](#) based on traffic

High Availability

- [Predefined DC pairs](#), a primary and a secondary
- [Failover handled](#) by the Meraki SD-WAN fabric

Security and Observability

- [Flexible security](#) options at MX and Headend
- [NGFW feature set at the branch](#) for Guest/SASE excluded traffic
- [Meraki Insight](#) and [Thousand Eyes integration](#) at the branch for application performance and visibility data



Under the hood

STEP 1 : Assign Branch to Secure Connect region

Assign region to onboard network

Choose which Meraki Networks to onboard as Secure Connect Sites by assigning a region to the network

Unassigned 10 Assigned 0

1 Item selected [Select all 10 items](#)

Cancel

[Assign to Region or Cloud Hub](#) ▾

☐	Networks & Templates	VPN	Type	Add
☐	Datacenter-CA iBGP 172.16.50.0/24	Off	VMX-M	230
☐	Datacenter-NA - appliance	Off	MX100-HW	600
☐	London - appliance	Spoke	MX105-HW	10 King
☒	NW-Branch	Spoke	MX84-HW	
☐	Retail Stores - appliance	Spoke	Template	

Assign site directly to these regions

Internet & Private App Access

US West
Los Angeles/Palo Alto

US Northeast
New York/Ashburn

US Central
Denver/Dallas

US Southeast
Atlanta/Miami

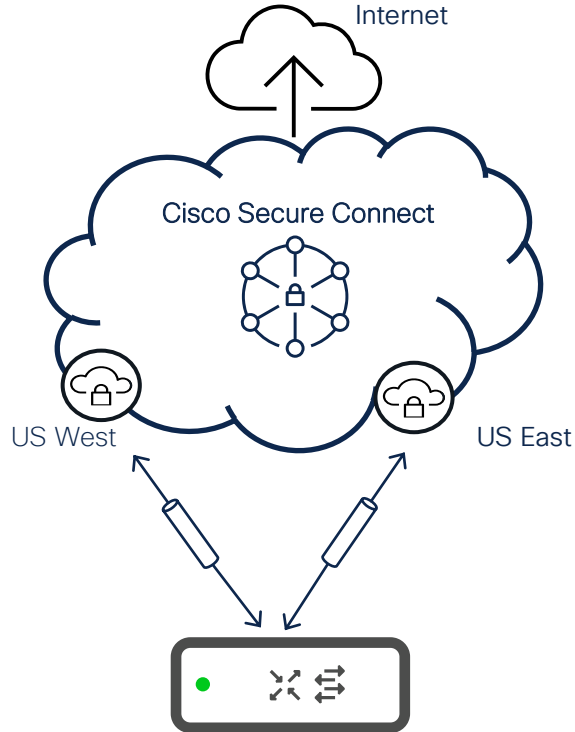
US Midwest
Minneapolis/Chicago

Europe-1

Actions



Meraki SD-WAN Hub Integration with Secure Connect (default behavior)



Meraki Hub (OAC or NAT mode)

VLAN

10.0.25.0/24



PRE-REQUISITE :

Make sure the Meraki **hub-to-hub mesh feature** is **not** disabled for the organisation



ADD THE HUB TO SECURE CONNECT

Add the **hub site** into the **Secure Connect** region on the sites page



ROUTE EXCHANGE BEHAVIOR

- ✓ The Hub **will exchange directly connected routes** into the Secure Connect fabric
- ✓ (Unlike Spokes) The hub will **not** learn the 0.0.0.0/0 route from Secure Connect by default
- ✓ The hub will learn **all private subnets from other hubs and spokes** connected to Secure Connect regions

Sites

☾ Last 2 hours ▾



ADD THE HUB TO SECURE CONNECT

Add the hub site into the **Secure Connect** region on the sites page and enable the default route

Sites 9

☐	Site name	Region / Cloud Hub	Site Features	Connectivity ⓘ
☐	Perth branch 105 - appliance	Australia-1 Region	Meraki network Spoke	
☐		US Northeast	Meraki network Spoke	
☐	Montreal branch 131	Canada-1 Region	Meraki network Spoke	
☐	Paris branch 132	Europe-2 Region	Meraki network Spoke	
☐	Tokyo branch 103	Asia-1 Region	Meraki network Spoke	
☐	Los Angeles hub 144	US West Region	Meraki network Hub	
☐	_San Francisco branch 104 - appliance	US West Region	Meraki network Spoke	
☐	Dallas branch 106	US Central Region	Meraki network Spoke	
☐	San Francisco Lab	US West Region	Meraki network Spoke	

iBGP

0.0.0.0/0

iBGP

0.0.0.0/0



ADD THE HUB TO SECURE CONNECT

Add the hub site into the **Secure Connect** region on the sites page and enable the default route

ROUTE EXCHANGE BEHAVIOR WITH DEFAULT ROUTES

✓ The Hub will exchange directly connected routes into the Secure Connect fabric

✓ The hub will learn the 0.0.0.0/0 route from Secure Connect

✓ The hub will learn all private subnets from other hubs and spokes connected to Secure Connect regions

Los Angeles hub 144

MX devices

Device	Model
08:f1:b3:db:22:4e	MX75-HW

[Full details in Meraki Appliance Status →](#)

Local networks

Local networks announced to Secure Connect

10.144.0.0/24

[Enable or disable Meraki network subnets →](#)

Remote Routes

Route settings for this Meraki Hub in relation to Secure Connect

Default Route: **Disabled**

Region

The Secure Connect region where traffic enters and exits. Regions can be changed per tunnel

US West - CH Hub 0

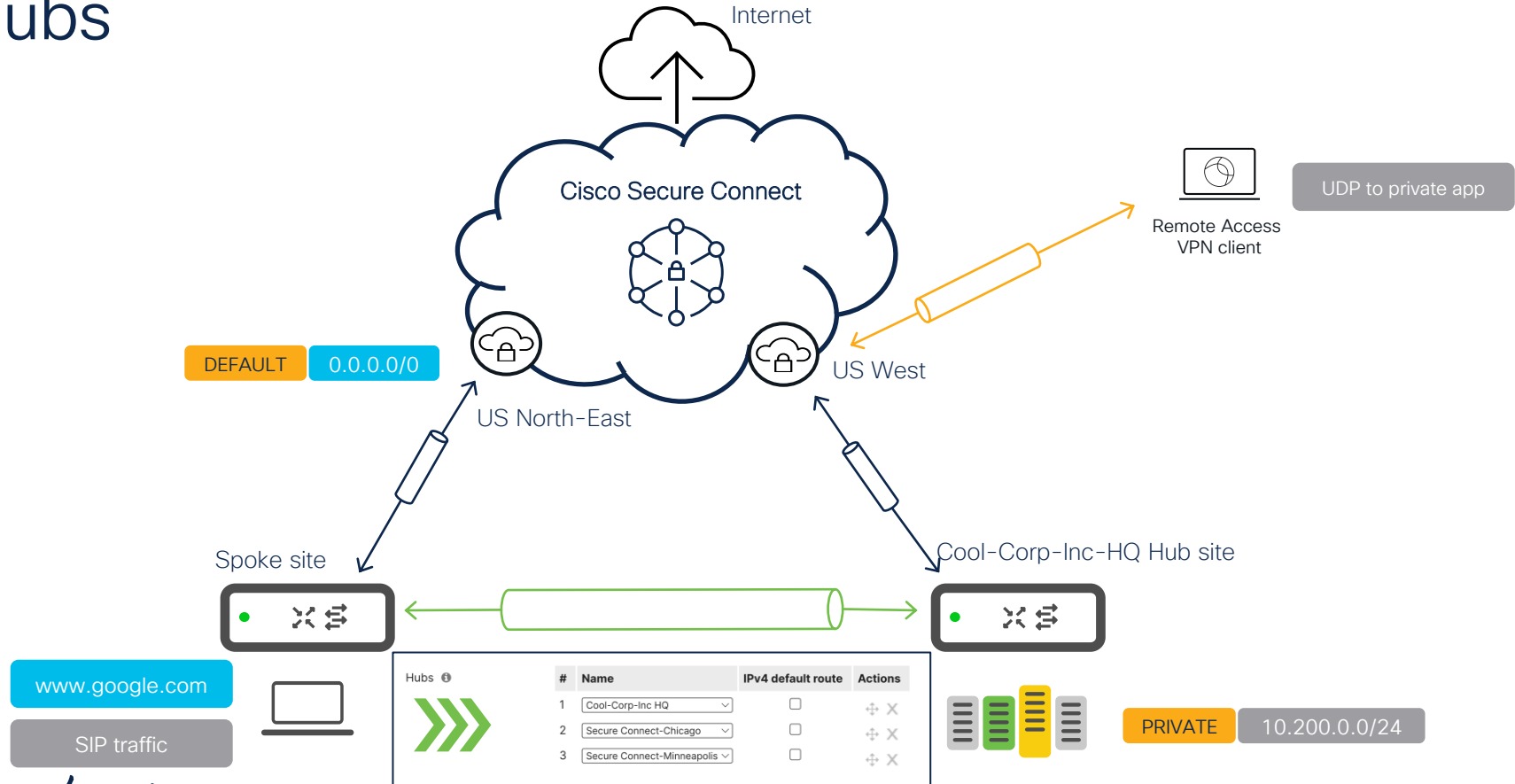
Security Events

Security events in the last 2 hours

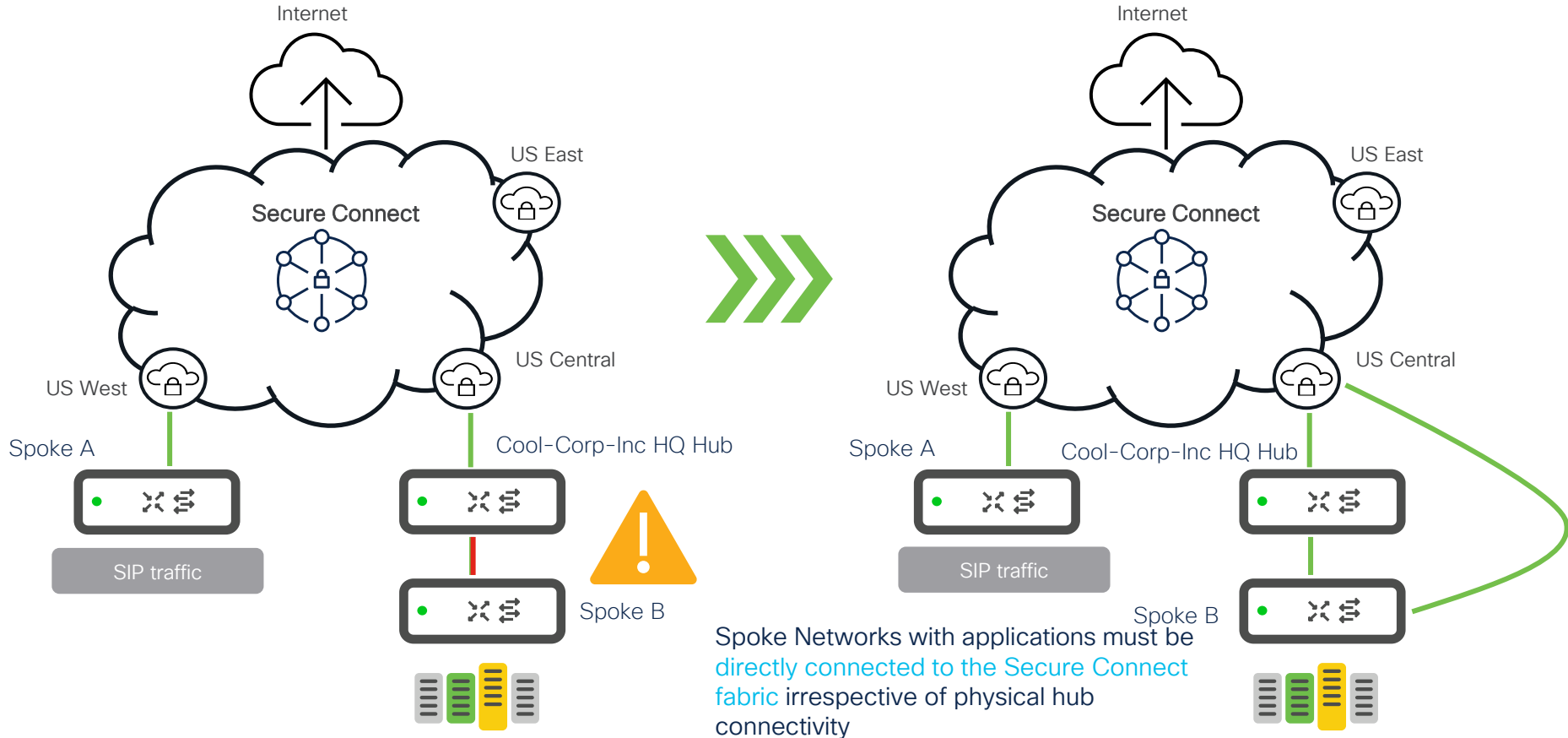
Total: 0

[View DNS and CDFW events in Umbrella ↗](#)

Secure Connect HUBs coexisting with Meraki MX hubs



Supported Hub design with multiple spokes



Global Overview

Organization
Demo-2-Fadv-TME

Network
Apps - Denver - 140

Secure Connect

Network-wide

Security & SD-WAN

Cameras [Learn more](#)

Insight

Organization

Overview

Last week

Security

Linear

39.5K total requests

Allowed Blocked Proxied



Policy count

- 1 DNS
- 2 firewall
- 2 web
- 1 data loss prevention
- 2 browser access

Sites

3 / 3 sites healthy

3 healthy sites

Network tunnels

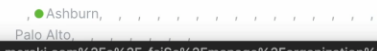
Configure and monitor tunnels for app and network access.

6 private access tunnels

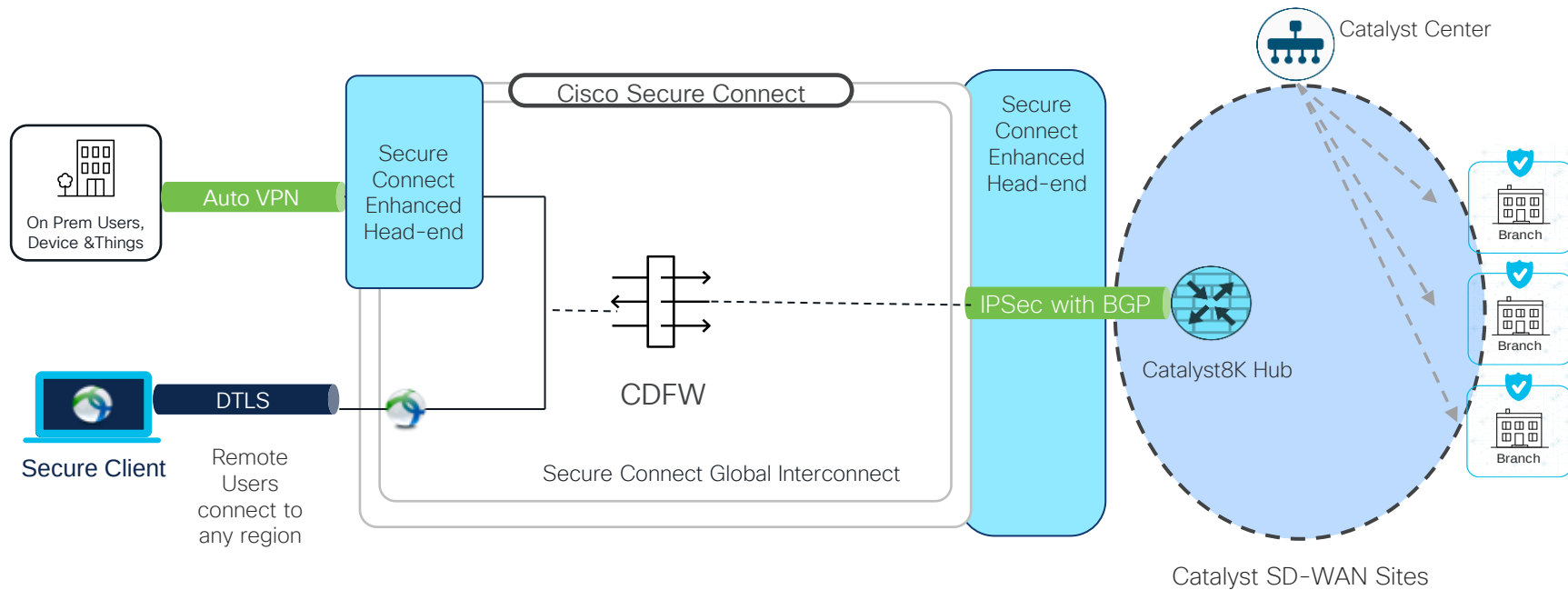
Remote access

0 clients connected

24 remote access locations



Catalyst SD-WAN Integration Private Access



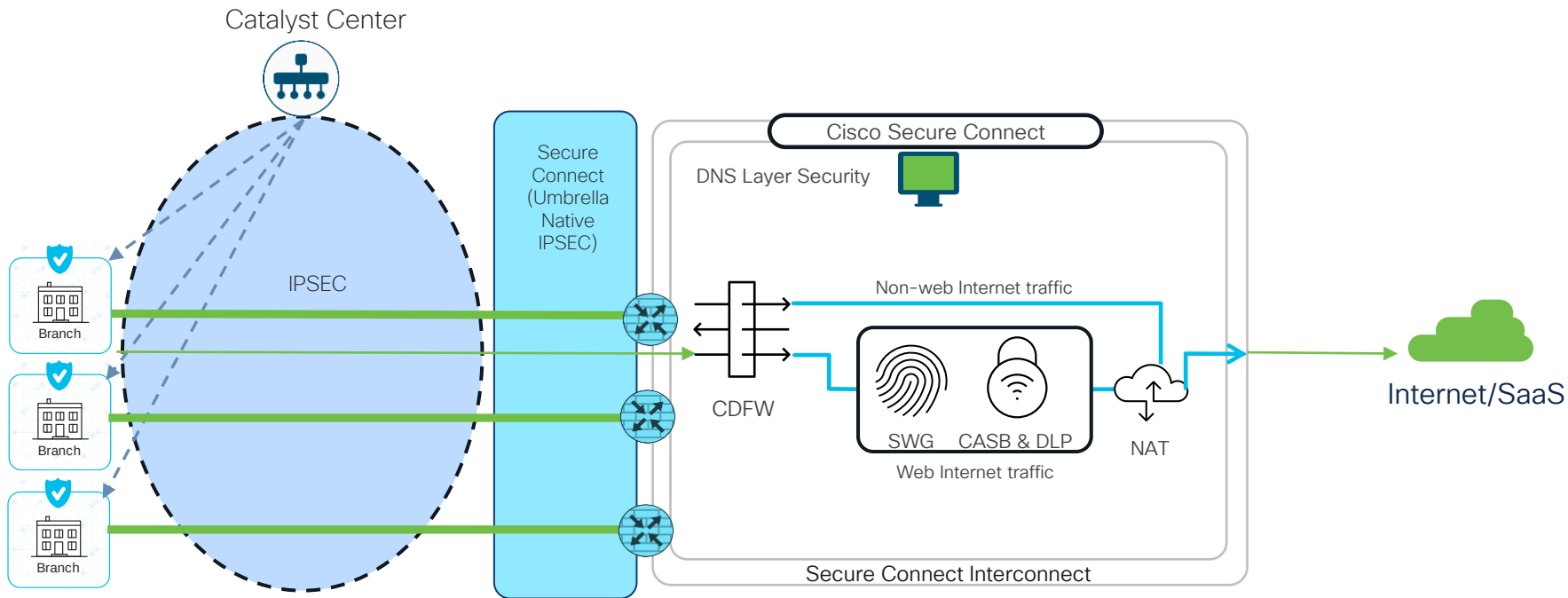
Unified user experience

NEW!

Meraki Catalyst SD-WAN Interconnect

Enhanced bandwidth with auto resiliency

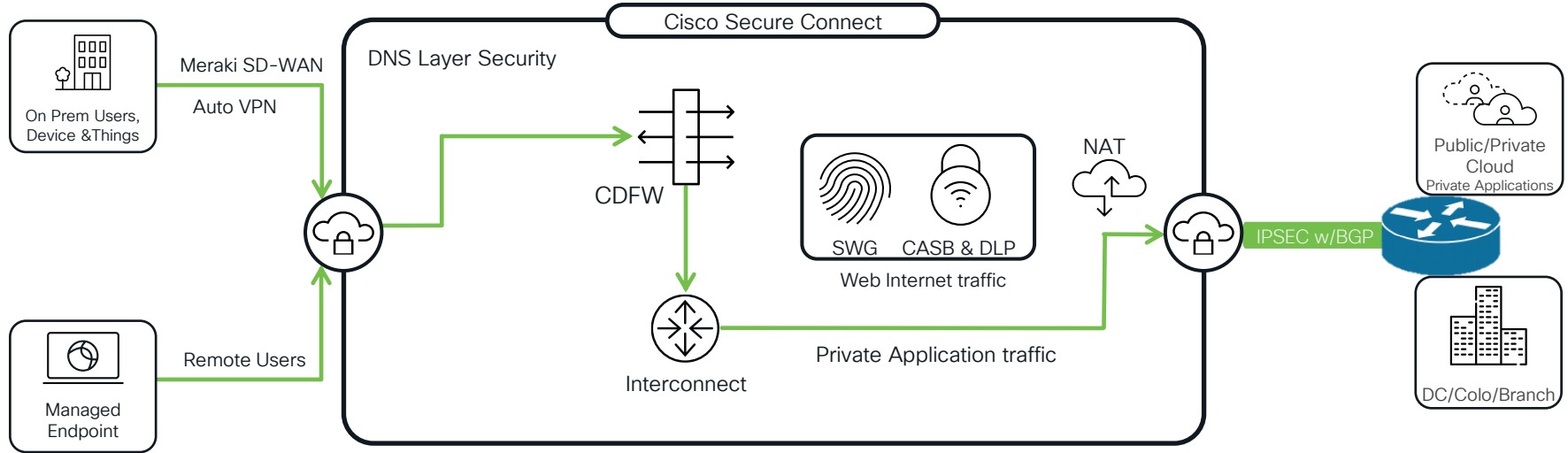
Catalyst SD-WAN Direct Internet Access



Catalyst SD-WAN branches

3rd Party IPSEC Sites Integration

NEW FEATURE



3rd Party IPSEC Sites Integration

NEW FEATURE

Secure Connect
Cloud native headend

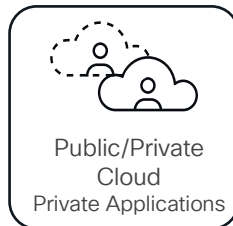


NEW!

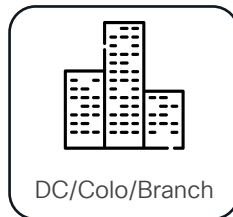
IPSec with BGP



IPSec Connection into
private sites



Public/Private
Cloud
Private Applications



DC/Colo/Branch

Enhanced
Bandwidth of 500
Mbps per tunnel

Auto resiliency
with built-in HA

Unified single
pane of glass
user experience

Secure Meraki to
3rd Party
Interconnect

Network
 Acme-HQ-AUS ▾

Sites 15

Last 24 hours ▾

Configure Cloud Hubs

+ Connect site ▾

Secure Connect

Network-wide

Cellular Gateway

Security & SD-WAN

Switch

Wireless

Systems Manager

Cameras

Environmental

Insight

Organization

0 Offline

0 Degraded

15 Healthy

0 Pending

Status ▾

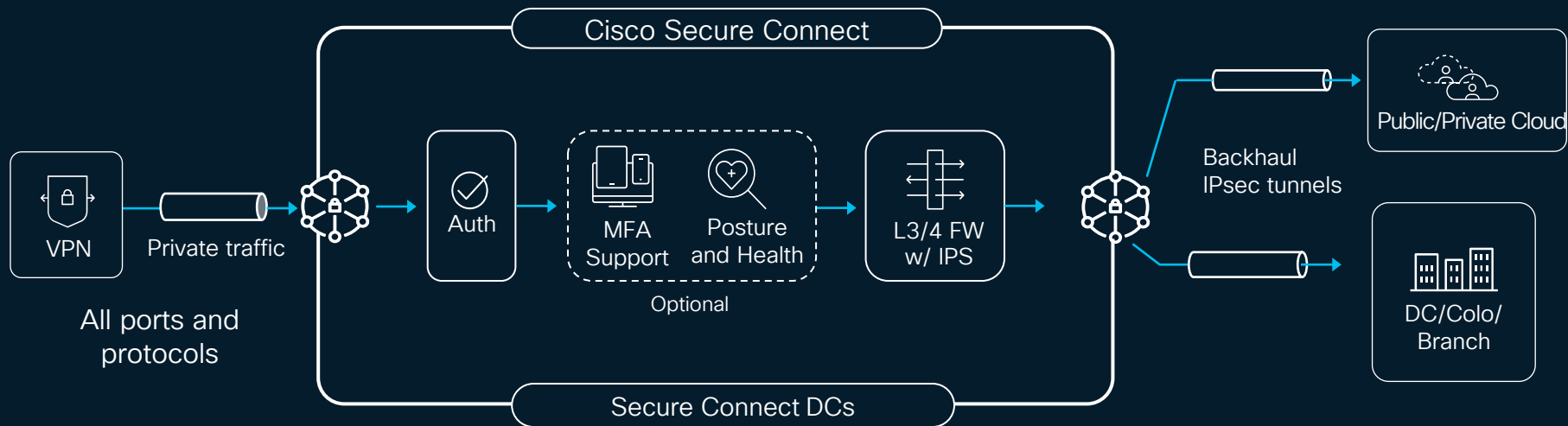
Type ▾

☐	Status	Name ↕	Type	Region/Cloud Hub	Site Features	Connectivity
☐		Atlanta Datacenter	Meraki Hub	US South East Cloud Hub	SIG	<div><div></div><div></div><div></div></div>
☐		Atlanta Branch 1	Meraki Spoke	US South East Cloud Hub	SIG	<div><div></div><div></div><div></div></div>
☐		Atlanta Branch 2	Meraki Spoke	US South East Cloud Hub	SIG	<div><div></div><div></div><div></div></div>
☐		San Francisco HQ	Meraki Hub	US West Coast Region	SIG & Private Access	<div><div></div><div></div><div></div></div>
☐		San Francisco DC	Meraki Spoke	US West Coast Region	SIG & Private Access	<div><div></div><div></div><div></div></div>
☐		San Jose Building 1	Meraki Spoke	US West Coast Region	SIG & Private Access	<div><div></div><div></div><div></div></div>
☐		San Jose Building 2	Meraki Spoke	US West Coast Region	SIG & Private Access	<div><div></div><div></div><div></div></div>
☐		San Jose Building 3	Meraki Spoke	US West Coast Region	SIG & Private Access	<div><div></div><div></div><div></div></div>
☐		San Jose Building 4	Meraki Spoke	US West Coast Region	SIG & Private Access	<div><div></div><div></div><div></div></div>
☐		San Jose Building 5	Meraki Spoke	US West Coast Region	SIG & Private Access	<div><div></div><div></div><div></div></div>

Rows per page 10 ▾
 < 1 2 ... 10 >

Cloud-delivered Remote access VPN

VPN-as-a-Service



SAML 2.0
based
authentication

Identity-based
access
orchestrated
through CDFW

Posture
assessment
through Secure
Client - Secure
Firewall module

Geography-
based
deployment
enables client
connection to
closest headend

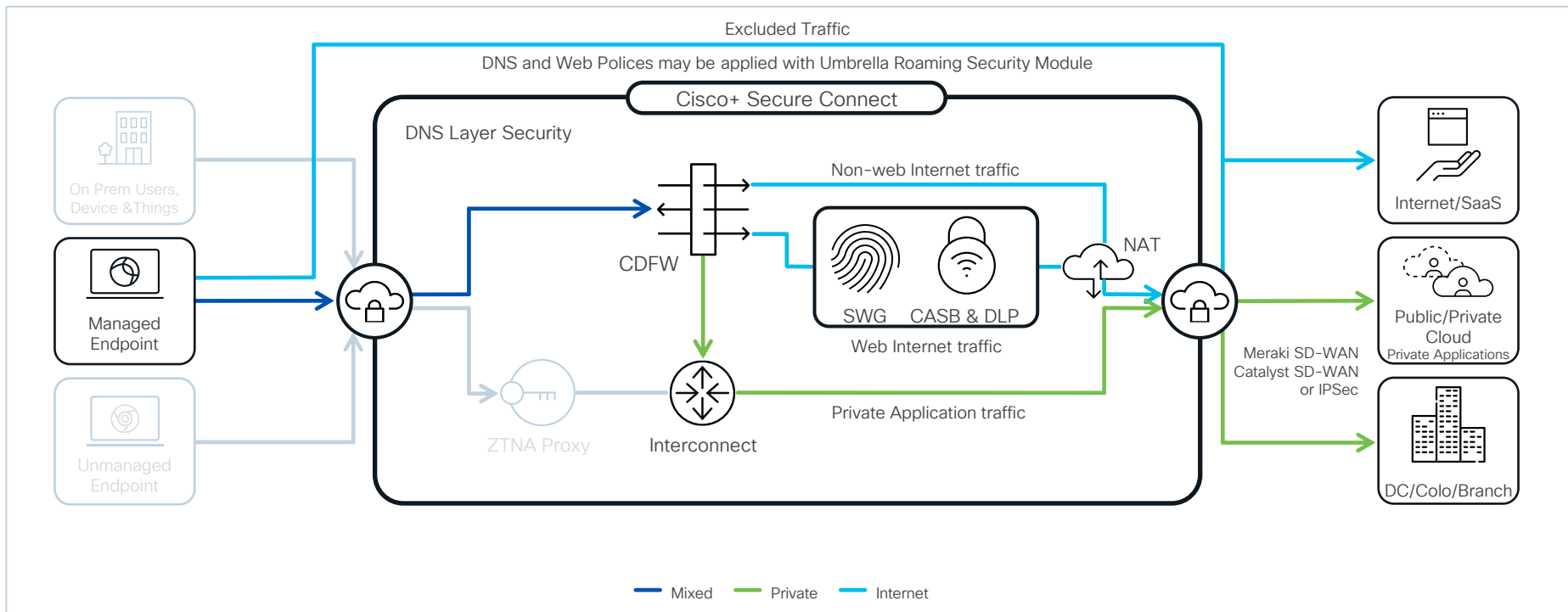
Flexible security
with Umbrella
Roaming
Security module
in Secure Client

Flexible traffic
steering
options

Remote Access – Client with Traffic Steering

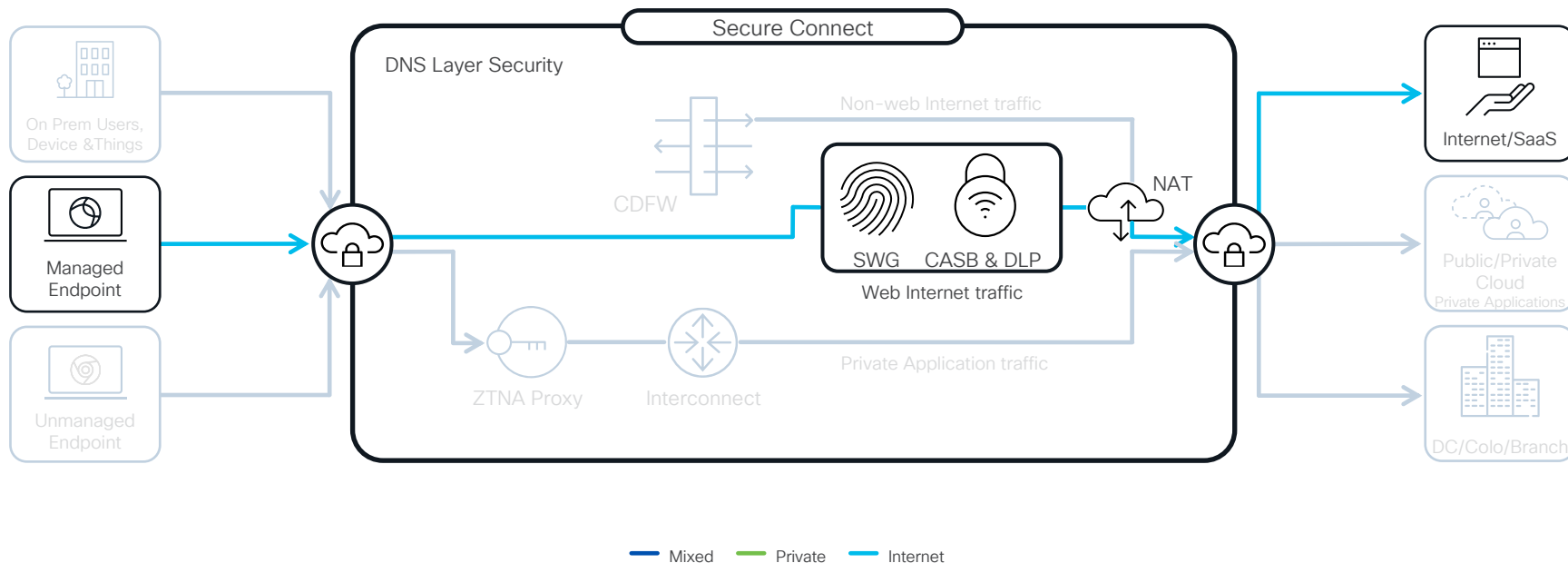
Secure Internet Access

Secure Private Access

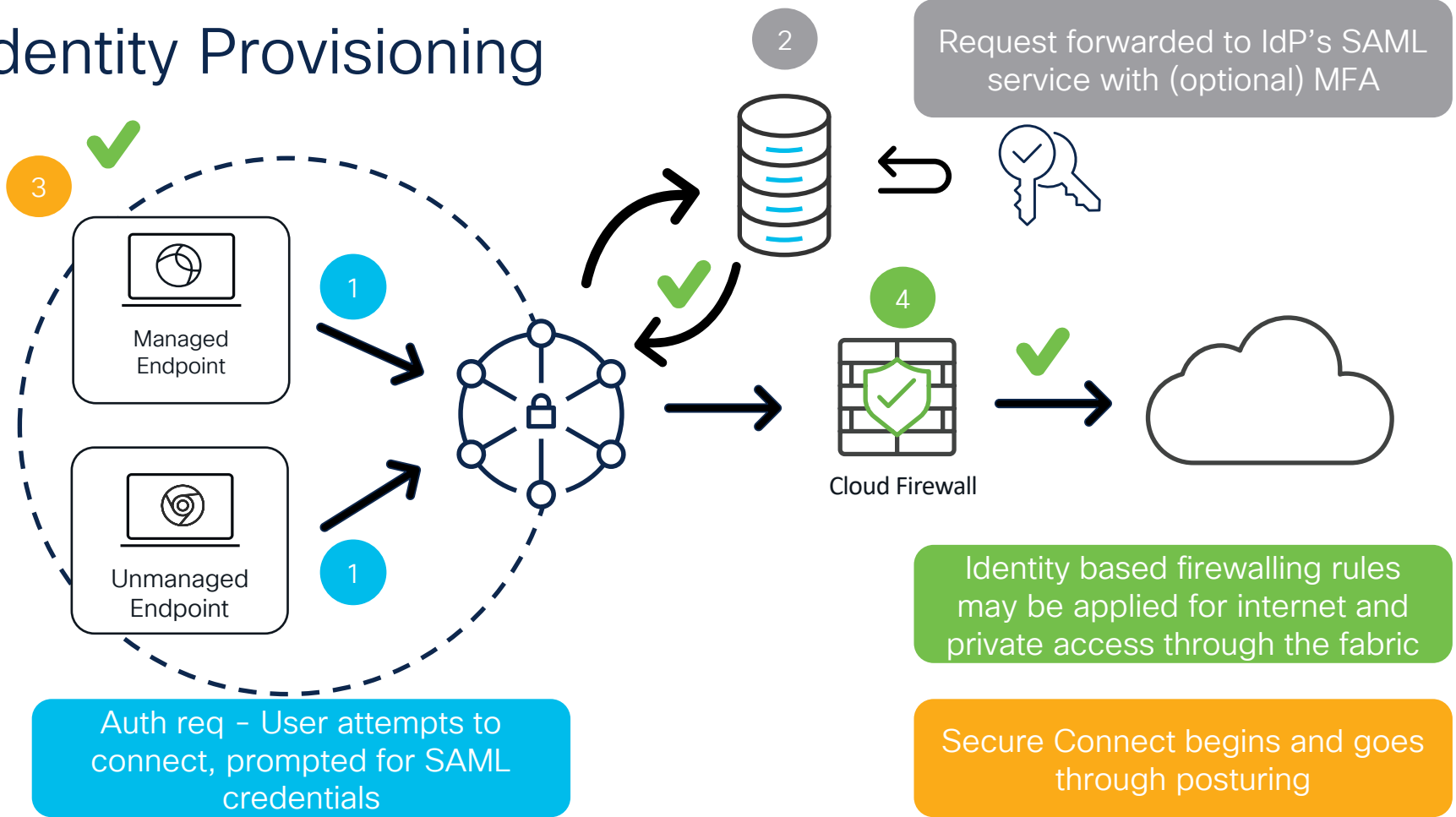


Remote Access –with Roaming Security Module

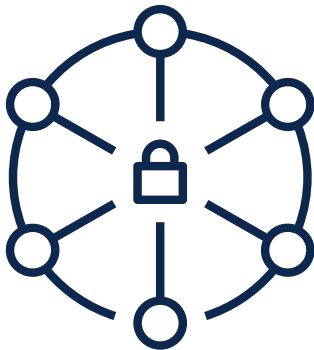
Secure Internet Access



Identity Provisioning



Identity Management & Providers



Duo

Microsoft Entra ID

Okta

On-premise AD

SCIM/Manual ID Entry

* Secure Connect supports any SAML 2.0 based identity provider with or without a SCIM integration (used for auto import of users into SC)

* AD connectors are used with Umbrella virtual appliances (VA) to get the identity of branch users' DNS requests

* Secure Connect supports manual addition of new identities into the Users page when the IdP does not have a SCIM integration available

Remote Access Log Export

Secure Connect -> Remote Access

Get started with Secure Connect Remote Access

Secure Connect enables remote users to access resources securely from anywhere through the Secure Client. Learn more in the [Secure Connect Remote Access Documentation](#).

3/4

- Configure remote access service
Configure details for the Remote Access service, and select what data center regions to deploy Remote Access.
[Edit configuration](#)
- Enable application connectivity
Meraki network
Add your Meraki network as a Secure Connect site to connect Remote Access users to internal applications.
[Manage sites](#)
Non-Meraki network
Connect network devices through IPsec tunnels to connect Remote Access users to internal applications.
[Edit tunnels](#)
- Configure and provision users
Enable Secure Connect to authenticate and authorize users.
[Edit configuration](#)
- Apply policies
[Import policies from MX client VPN](#)
Import Internet Security (Intrusion) rules with affecting MX VPN remote access users.
[Create new firewall rules](#)
Create network access policies to manage Remote Access users.
- Deploy Secure Client to Users
Users need Secure Client to access Secure Connect. Download the Secure Client app and configuration files to send to your users.

Remote Access
Remote Access enables you to onboard your remote users. For more information, see [Remote access service](#)

Overview

Secure Tunnels
2
[Update](#)

Connected users
0
[View all](#)

Endpoint compliance criteria
0
[Configure](#)

Remote access logs
[Pick a Range](#)
2 hours
24 hours
One week
One month
Custom
[Logs](#) [Generate](#)

[Download the Secure Client](#)

Regions

Active locations
8

Fully Qualified Domain Name
C7AC.SC.CISCOPLUS.COM
[Learn more](#)

Region	Number of locations	Status
Europe	4	Active (4)
North America	4	Active (4)

[Done](#)

Connecting Applications & ZTNA

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

Unmanaged Device

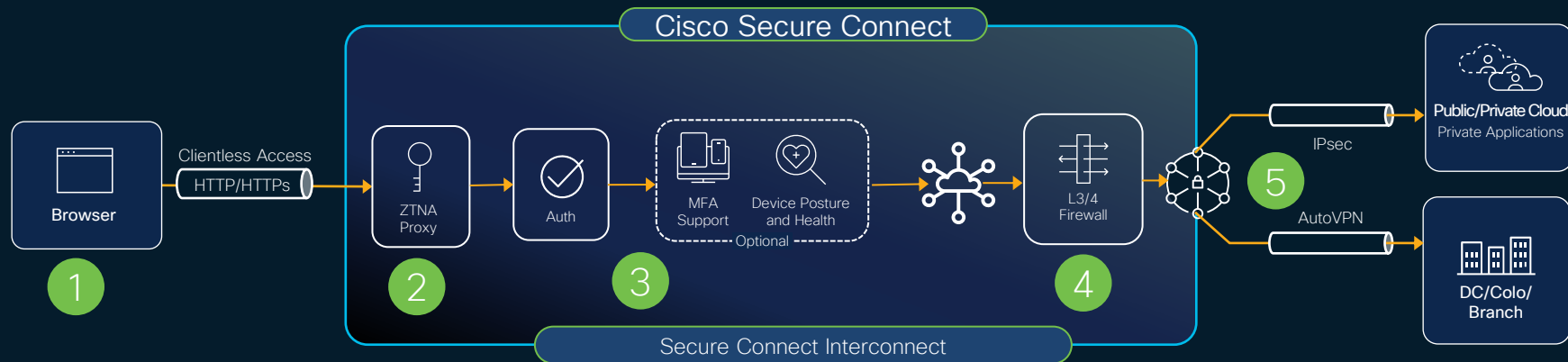
- Accessible from any browser that supports SAML/Cookies
- Request based posture (browser version, OS, geo-location)
- Web applications only



Client-based ZTA

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

Clientless or Browser-based ZTNA



1. Client connects to application's URL & request is redirected to nearest DC

2. ZTNA Proxy changes the traffic source to an address within 100.64.0.0/16

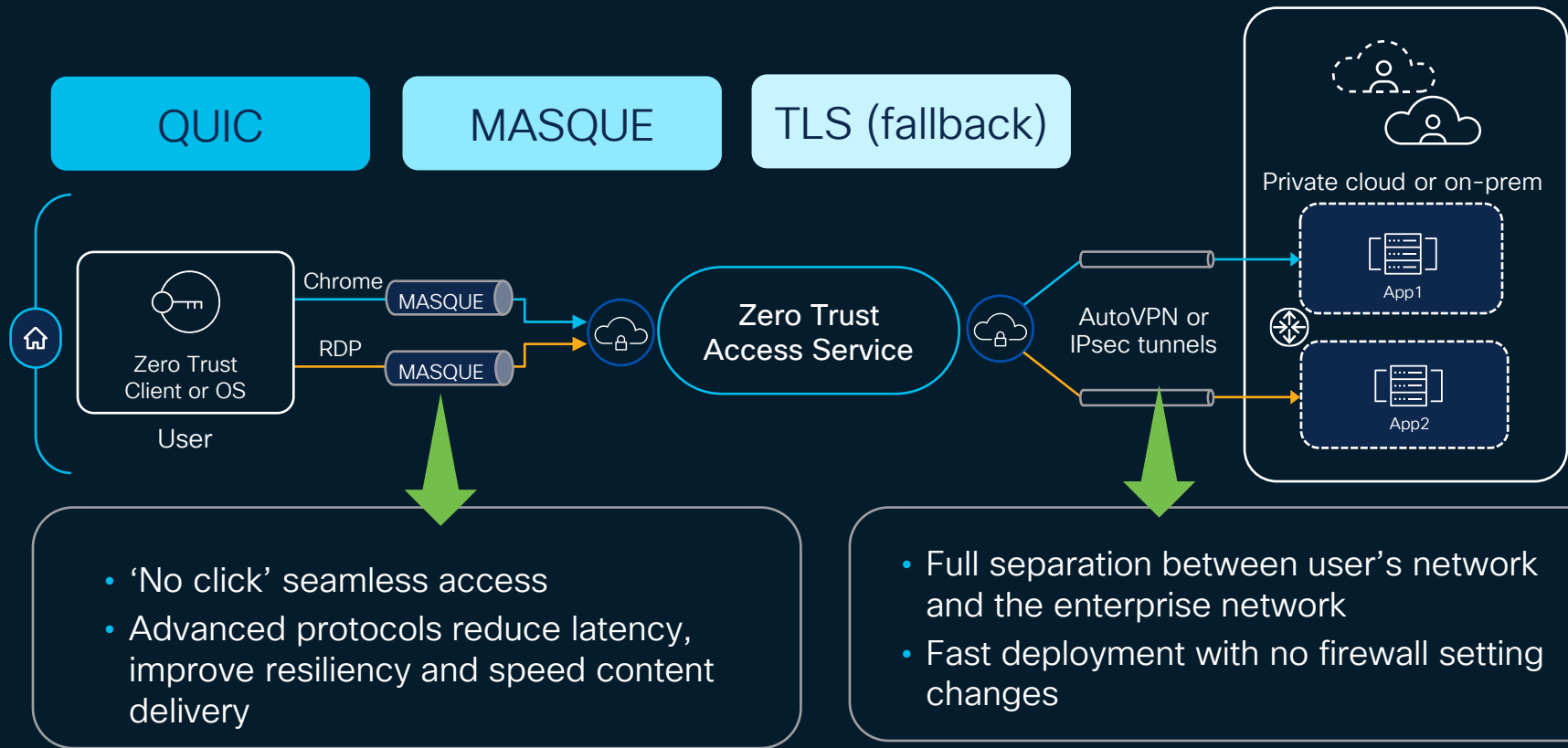
3. Request is sent for authentication and posture check

4. After authentication & authorisation, request is sent to policy engine to decide access

5. Once decided, request sent over interconnect to deliver traffic to the application correctly

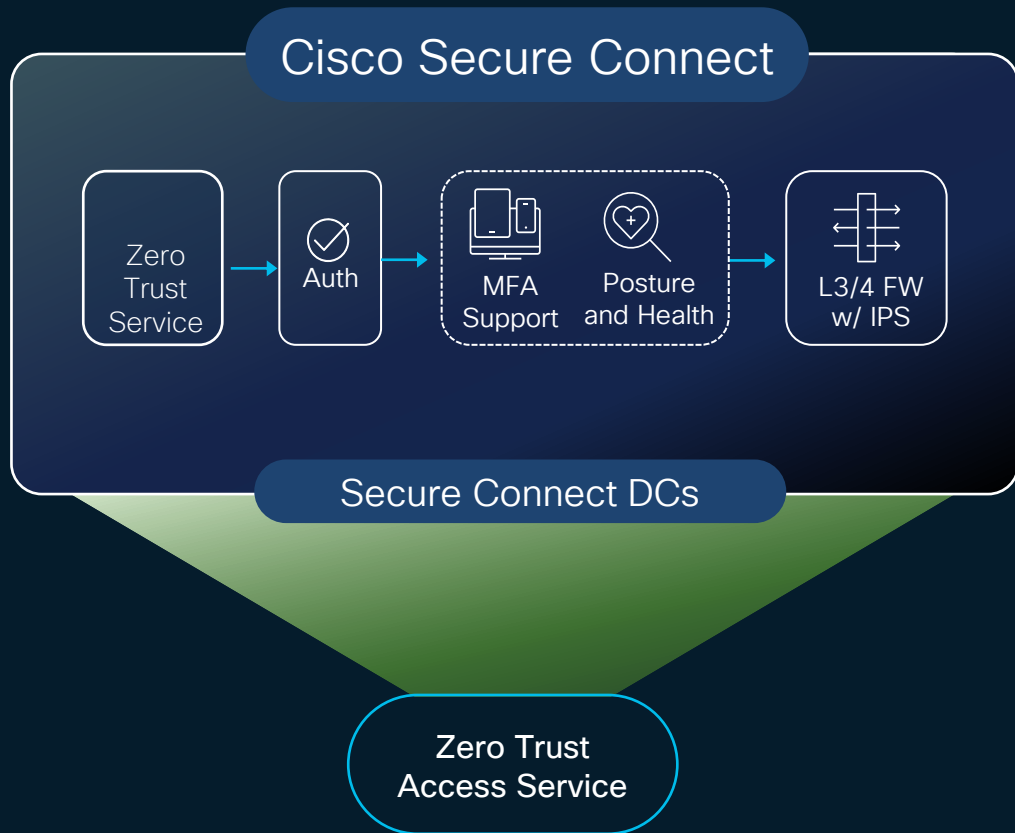
Introducing MASQUE – unlocking QUIC proxying

Seamless and Secure Access for all users

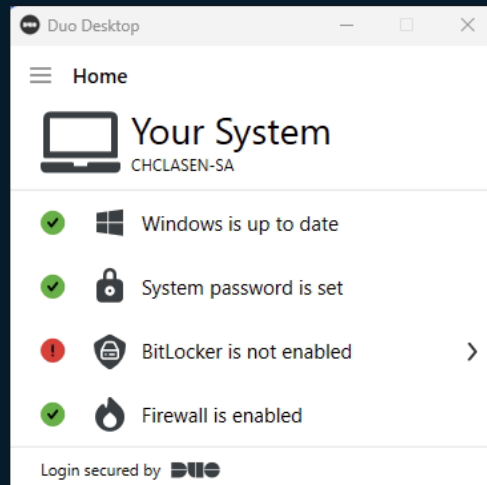


Client-based ZTNA in Secure Connect

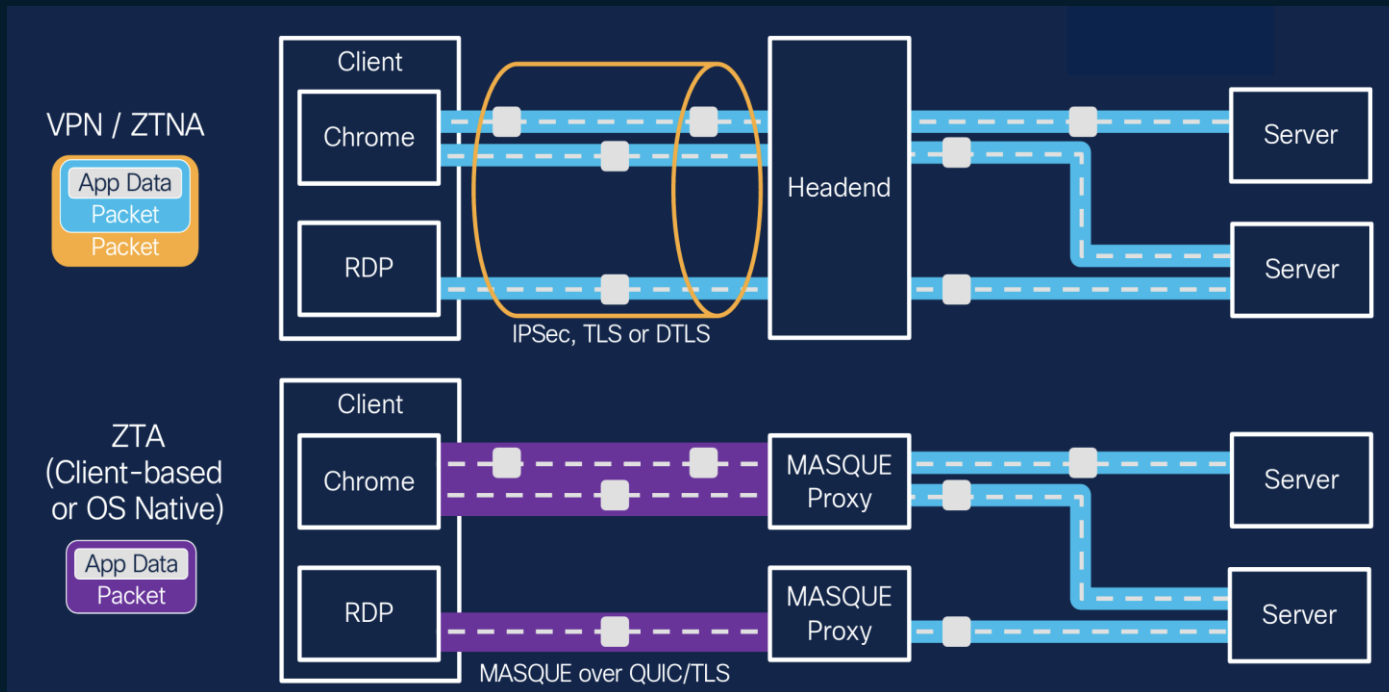
Authentication & Posture



- Authentication & Posture at Connect time
- DTLS Tunnel
- Carry Internet & Private Traffic (All ports & protocols)
- SAML 2.0 Authentication
- Posture based on Duo Health agent (embedded into client)

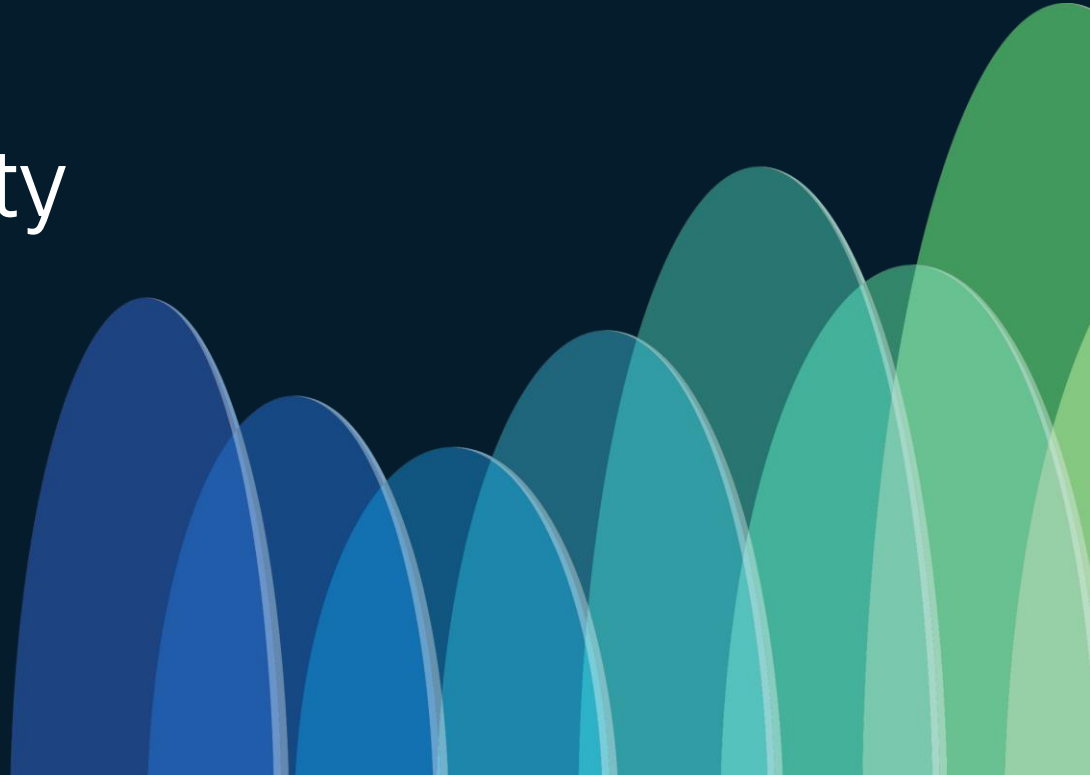


Client-based access to server using ZTNA



With ZTA, each process uses a unique MASQUE connection, even if the data streams are destined to different servers

Bolstering Security with SASE



Cisco Meraki MX Firewall

Go beyond core Firewall capabilities to better connect and protect your business

Core Platform



Centralised administration with role-based access control



Automated software and firmware upgrades



Zero touch deployment



Rich Reporting and analytics

Cisco delivers the core and more in a single subscription



Application Visibility and Control



Stateful Firewall



Identity-Based Firewall



Application Firewall



Content & URL Filtering



Advanced Malware Protection



Talos Threat Intelligence



SD-WAN (Auto-VPN)



Digital Experience Monitoring

Integrated Add-on Capabilities



LAN



WiFi6



Thousand Eyes



DNS Security



XDR

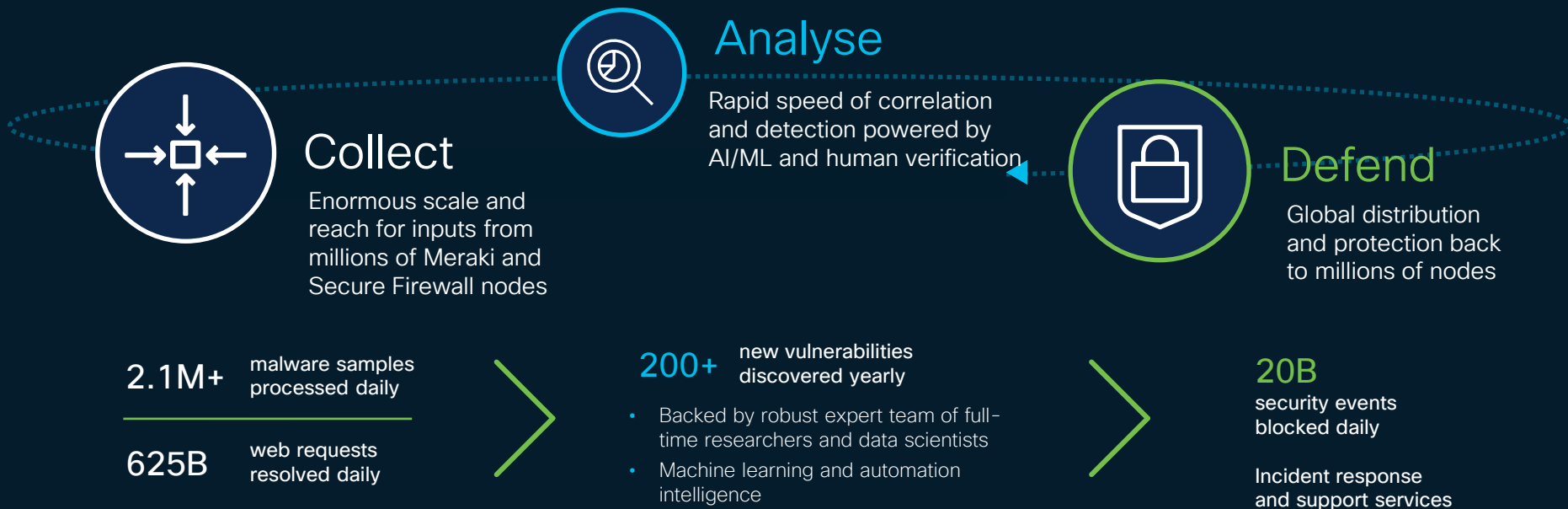


SSE



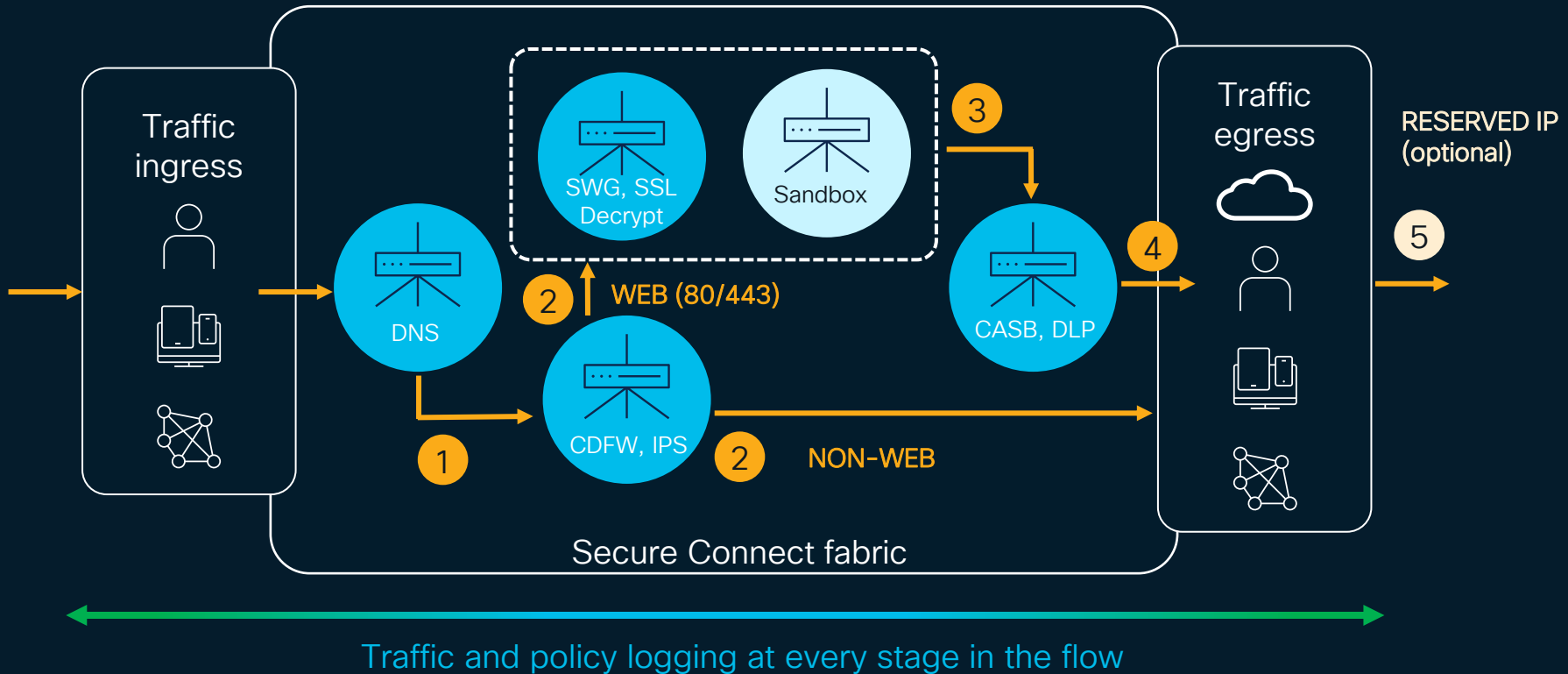
Sandboxing

Powered by Cisco Talos Threat Intelligence



We see more and automate more, so you can block more and respond faster to threats

Policy enforcement breakdown

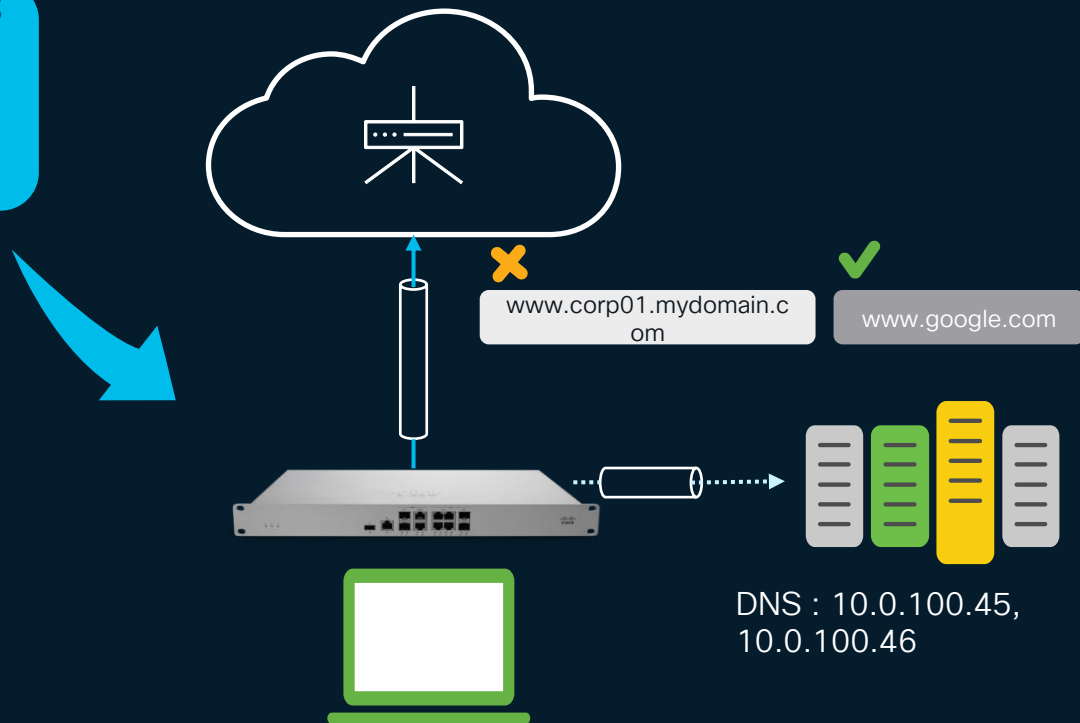


Private domain resolution and DNS protection

Resolve local domains while preserving DNS filtering across the internet

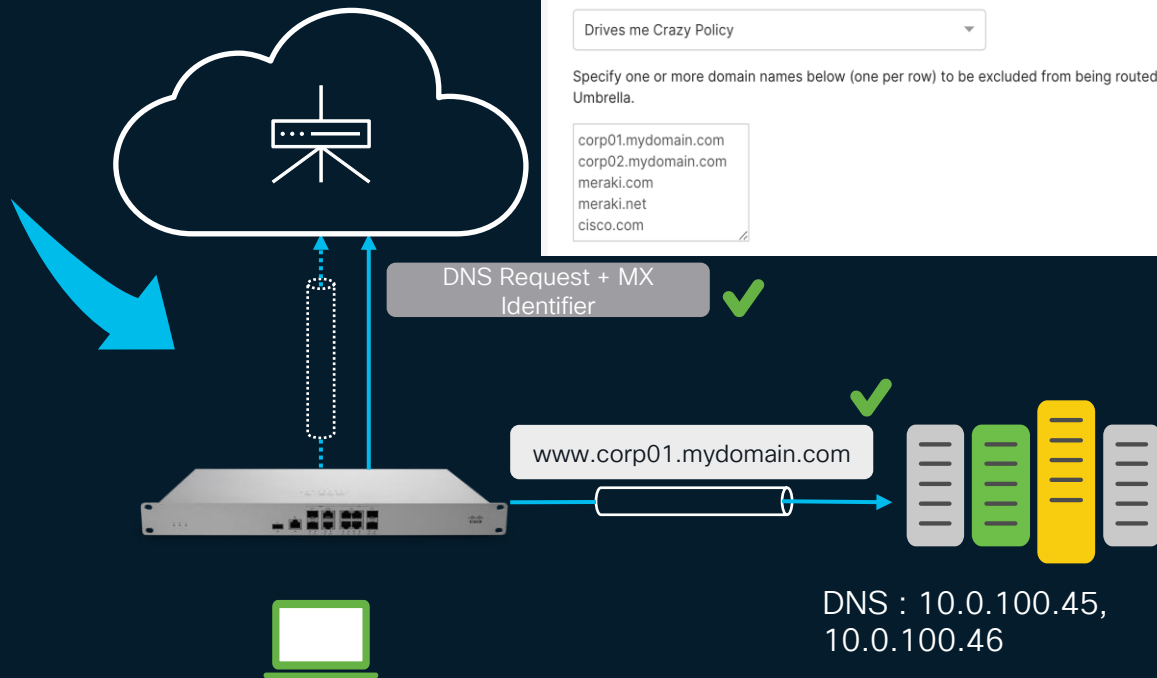
DEFAULT BEHAVIOR : Internal DNS forwarded to Secure Connect through a network tunnel irrespective of what is configured on the client

- When a site is connected to Secure Connect all DNS traffic goes through the tunnel to Secure Connect and is subjected to policy.
- A site is identified through the network tunnel that DNS is coming from
- Private domains cannot be resolved



SOLUTION : DNS exceptions on Meraki MX with native Umbrella DNS integration

- Umbrella API keys can be linked to an MX network.
- The MX intercepts all DNS traffic, wraps it with an identifier (DNSCrypt), and sends it through the internet to Umbrella OpenDNS servers
- Umbrella DNS exceptions can be configured on the MX to exclude private domains. DNS requests to these domains are directly sent to the private DNS server
- Policy can now be applied per network (because of the custom identifier)



My DNS server is : 10.0.100.45, 10.0.100.46

Event Logs and Reporting

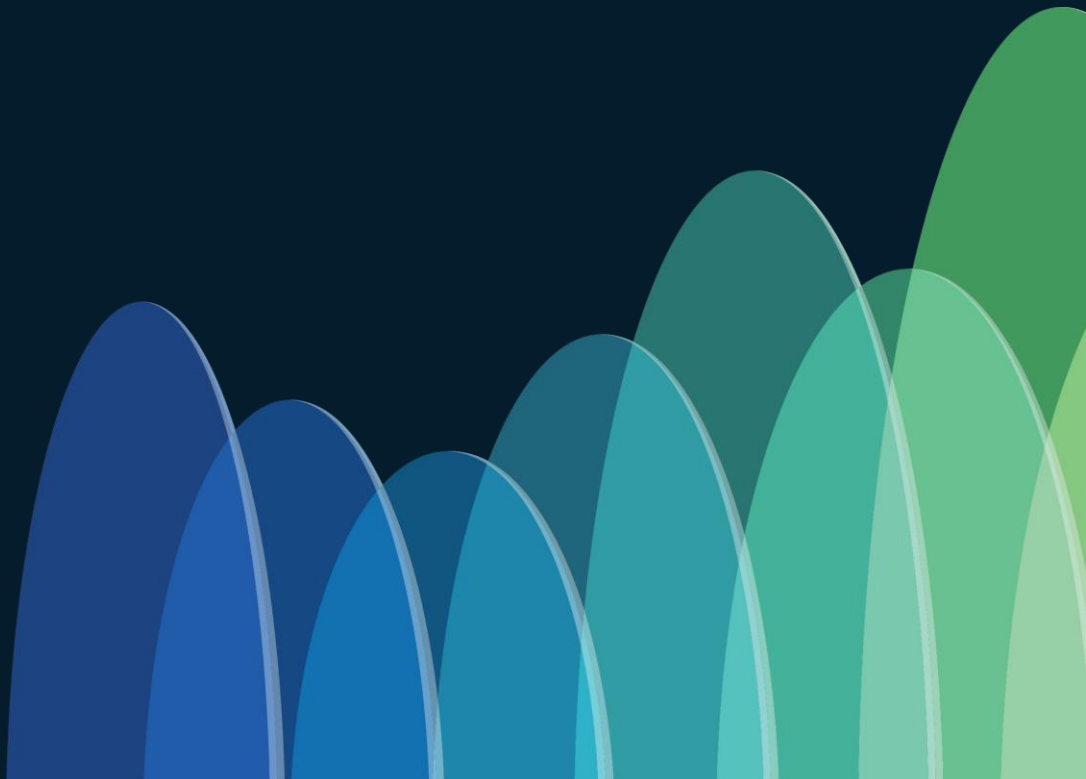
- Comprehensive, **end-to-end reporting** across all stages of policy enforcement and NAT
- Ability to consume metrics broken down by **top threats, volume, destinations, identities and categories**
- **Single vantage point** across multiple sites and users
- Ability to move logs to an **Amazon S3 bucket** (customer owned or Cisco owned)
- Amazon API can be used for integration with logging services or SIEM

The screenshot displays the Cisco Activity Search interface. On the left is a sidebar menu with the following sections:

- Core Reports**
 - Security Activity
 - Activity Search
 - App Discovery
 - Top Threats
- Additional Reports**
 - Total Requests
 - Activity Volume
 - Top Destinations
 - Top Categories
 - Top Identities
 - Remote Access Logs
 - Cloud Malware
 - Data Loss Prevention

The main content area shows the 'Activity Search' results. It includes a search bar, a 'Schedule' button, and a table of activity logs. The table has columns for Request, Identity, Policy or Ruleset Identity, and Description. The data shows multiple entries for 'Branch Access orgid:7478818' with various request types (FW, WEB) and a total count of 30,046.

Secure Connect Licensing



All Essential Security features with unlimited sandbox submissions and malware detection capabilities

Data Loss Prevention + L7 Cloud-delivered Firewall + IPS (Intrusion Prevention System)

Advantage

Complete

Used for [Private Access](#) (ZTNA or Secure Client RAVPN users)

Secure Connect Licensing

Foundation

Used for [Internet Access](#) (SD-WAN branch or IPSec branch users)

Essentials

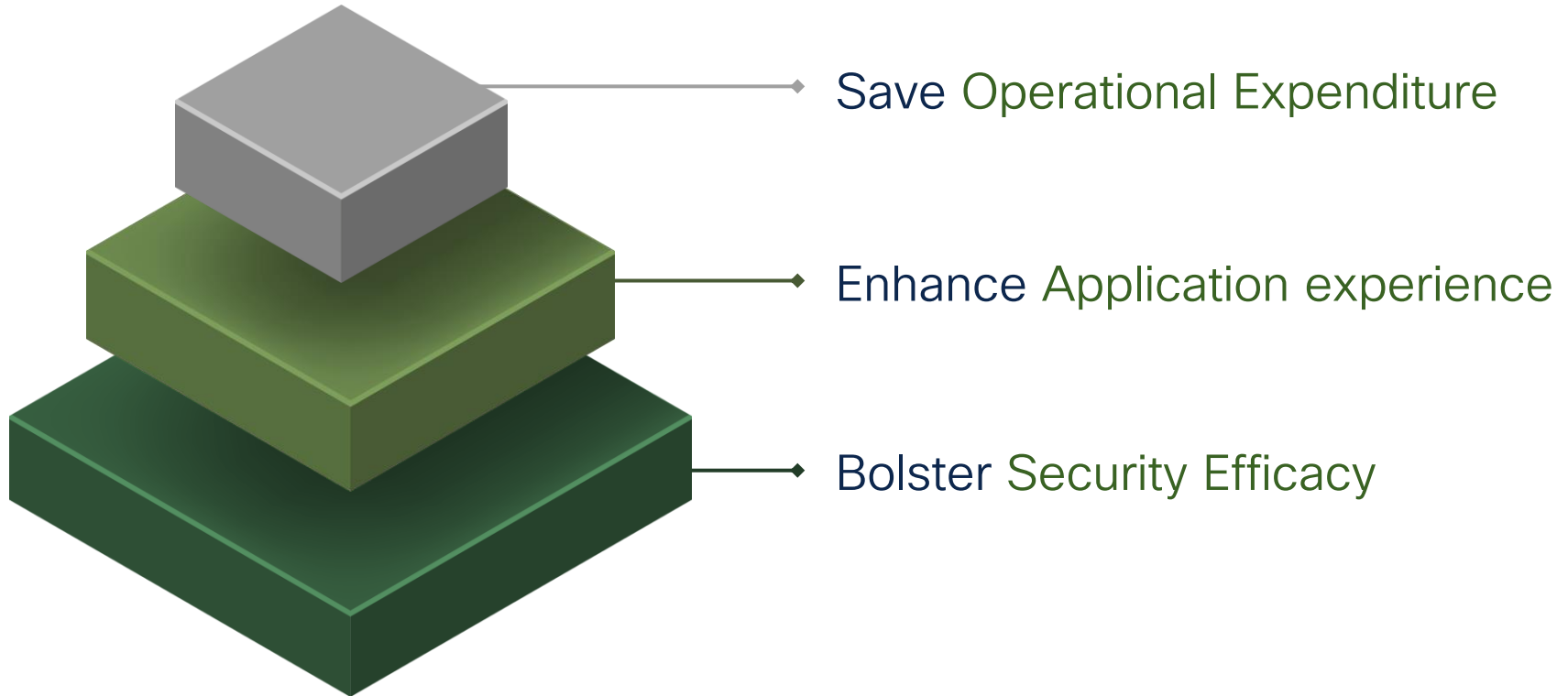
Essential Security feature set with limited sandbox submissions and malware detection capabilities

*1 Secure Connect licenses are per user passing through the fabric (20 GBs per user per month)

*2 Secure Connect licenses can be mixed so long as the security tier is the same (eg: 20 Complete Advantage + 30 Foundation Advantage)

Cisco wants to

Simplify Network and Security operations



Keynote Deep Dives

Wednesday
10:30am – 11:30am



Experiences Amplified:
How AI Can Fuel
Better Employee
and Customer
Experiences

Level 1
Room 106



Smart, Secure,
Seamless:
Transforming
Experiences with
Next-Generation
Networking

Level 2
Room 204



Harness a Bold
New Era:
Transform Data
Centre and
Service Provider
Connectivity

Level 2
Room 203



Securing User to
Application and
Everything in
Between

Level 2
Melbourne Room 2



Unlocking
Digital Resilience
through Unified
Observability

The HUB
Centre Stage

Complete Your Session Evaluations



Complete a minimum of 4 session surveys and the Overall Event Survey to claim a **Cisco Live T-Shirt**.



Complete your surveys in the **Cisco Live mobile app**.



Continue your education



- Visit the Cisco Stand for related demos
- Book your one-on-one Meet the Expert 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

Gracias

Danke

Merci

Mahalo

Grazie

Dhanyavaad

Xiexie

Arigato

Obrigado

Shukran

Thank You

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC