



Cisco Security

La chiave per un ambiente digitale più sicuro

4 Aprile 2025

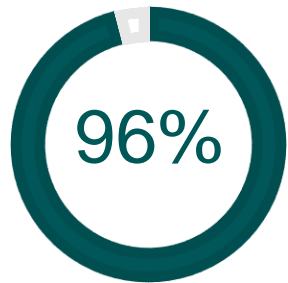
Webinar

Federico Frosini – Business Development Manager – TD SYNnex

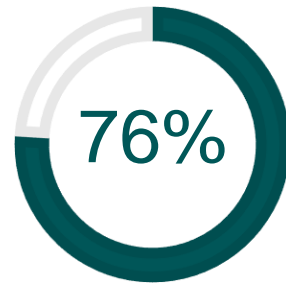
Giacomo Casati – Cisco Presales Specialist – TD SYNnex

Andrea Pezzoni – Security Presales Specialist – TD SYNnex

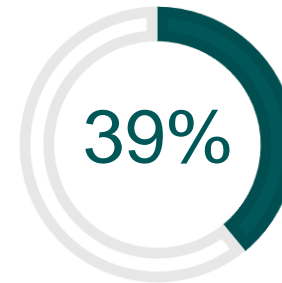
ERP e Cloud



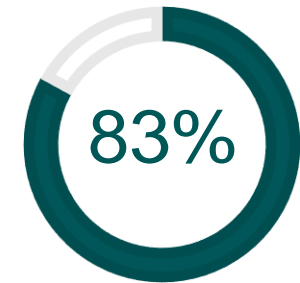
Percentuale di aziende che pensano ad una migrazione di tutti i dati aziendali in cloud in 5 anni



Aziende che hanno già spostato o stanno per spostare il loro ERP in Cloud



Aziende che valutano lo come prima ragione dello spostamento in cloud un miglioramento dei processi aziendali



Aziende che hanno aggiunto piattaforme SaaS nel 2023 rispetto al 2022

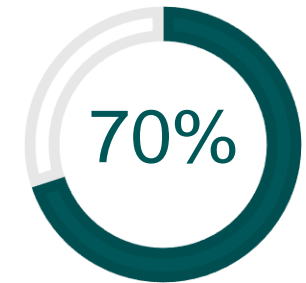
Bring Your Own Device



Organizzazioni che permettono uso di dispositivi personali



Gli incidenti di sicurezza che hanno coinvolto dispositivi smarriti o rubati hanno portato a una violazione non autorizzata dei dati.



Percentuale dei dispositivi BYOD che non sono mappati o censiti in ambito aziendale

SASE



- CASB + ZTNA + FWaaS + SWG
- Scalable
- Cloud Based
- Networking + Security



Cisco Security Strategy

Cisco Security Strategy

More products leads to more complexity within your business and IT environment

Exfiltration

Ransomware

Lateral movement

Web threats

Stolen credentials

Spam



76

Average number of security tools per enterprise

78%

Organizations report that high number of security tools is driving cybersecurity complexity*

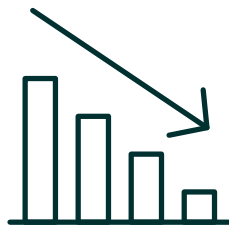
Cisco Security Strategy

Customer top priorities address the challenges



Boost Productivity

Empower users to
do their best work



Optimize Costs

Address inefficiencies



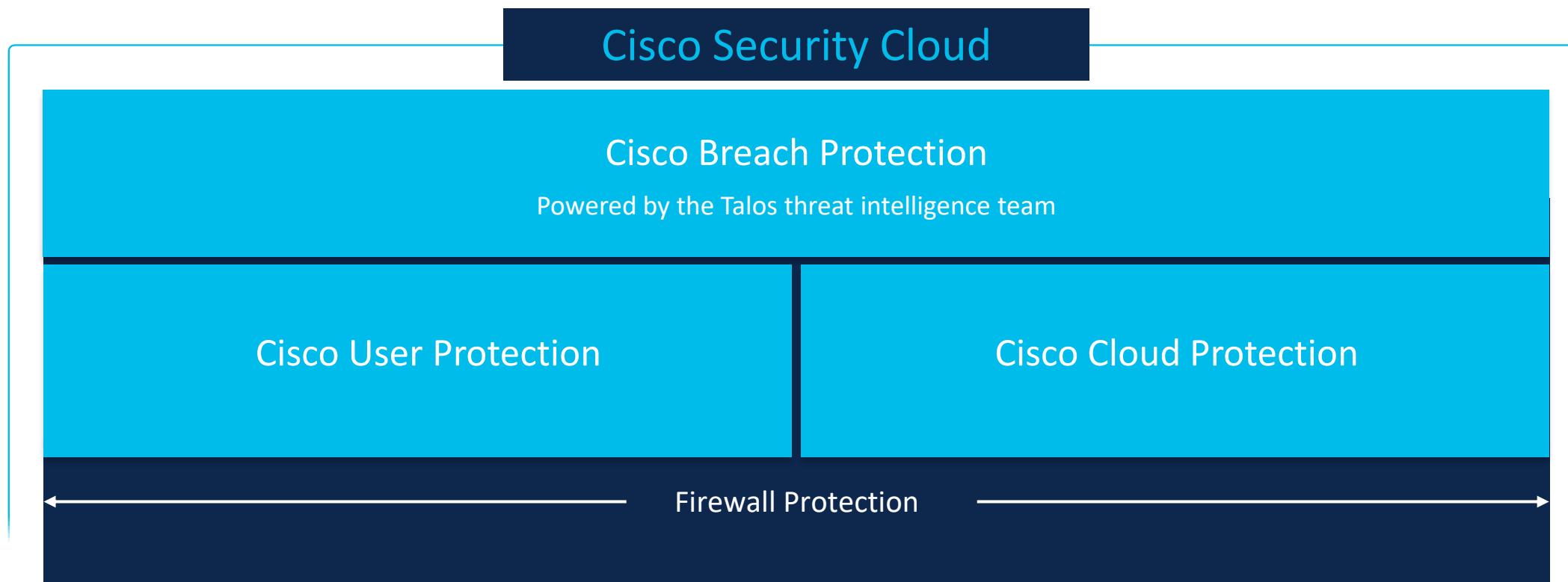
Minimize Risk

Secure your organization

Cisco Security Strategy



Cisco Security Strategy



Cisco Security Strategy

Cisco Security Cloud

Cisco Breach Protection

Extended Detection & Response

Cisco User Protection

Posture & Auth Management

Endpoint Security

Email Security

Experience Insights

Remote Browser Isolation

Network Access Control

Security Service Edge

Cisco Cloud Protection

Workload Security

Application Security

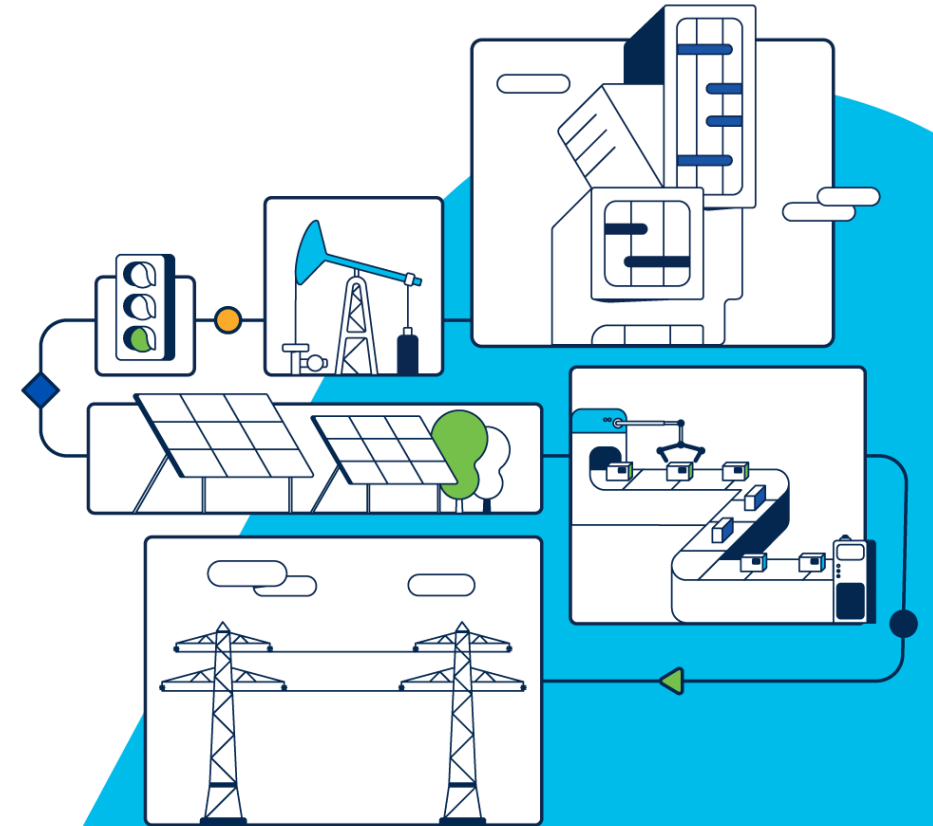
Vulnerability Management

Full Stack Observability

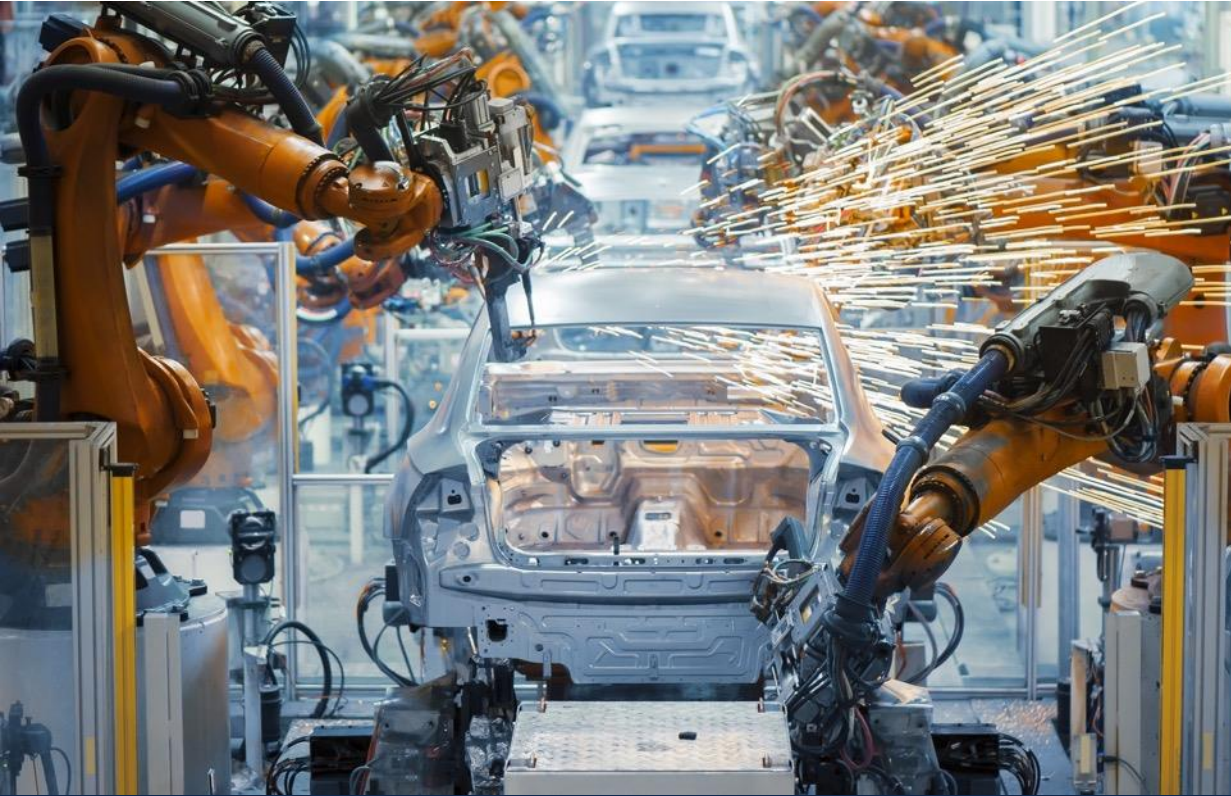
Multicloud Defense

Firewall Protection

Cisco Cyber Vision



Industry Digitization Increases the Threat Landscape

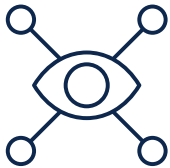


- More connected automation devices
- IoT devices accessing the cloud
- Shadow IT in industrial networks
- Remote access from third parties
- Malware intrusions
- New regulatory requirements

The role of IT is expanding to help secure industrial operations

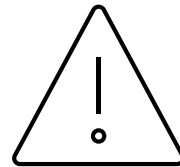
Cisco Cyber Vision

Visibility & Security Platform for the Industrial IoT



Visibility

OT asset inventory
Communication patterns



Security Posture

Device vulnerabilities
Risk scoring



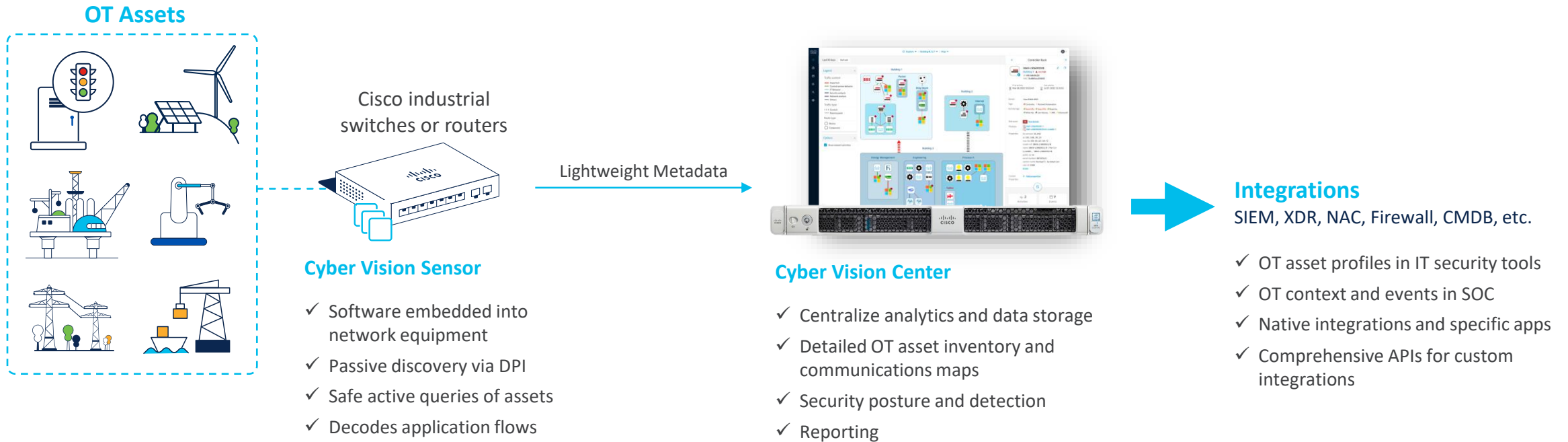
Operational Insights

Track process/device modifications
Record control system events

Context and insights that are foundational to building reliable and secure OT networks

Cisco Cyber Vision: Unique 2-Tier Architecture

OT visibility that can be deployed at scale



OT visibility sensors embedded into network equipment sees more and is easier to scale

Cisco Cyber Vision portfolio

Cyber Vision Center

Hardware Appliance

UCS based servers with Hardware RAID



- CV-CNTR-M6N
- 24 core CPU
 - 128 GB RAM
 - 3.2TB drives

Software Appliance

Virtual Machines



VMWare ESXi OVA



HyperV VHD

- Minimum requirements
- Intel Xeon, 10 cores
 - 32GB RAM and 1TB SSD
 - 1 or 2 network interfaces



Amazon Web Services



Microsoft Azure

- Minimum requirements
- Intel Xeon, 10 cores
 - 32GB RAM and 1TB SSD
 - 1 or 2 network interfaces

Cyber Vision Sensors



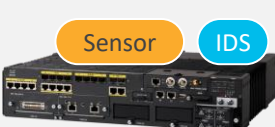
Catalyst IE3300 and IE3400 Switches



Catalyst IE3400HD IP67 Switch



Catalyst IR1101 LTE/5G Gateway



Catalyst IR8300 Multiservice Router



Catalyst IE9300 Rugged Aggregation Switches



Catalyst 9300/9400

Network-Sensors

Deep Packet Inspection built into network-elements eliminating the need for SPAN



IC3000 Industrial Compute

Hardware-Sensor

DPI via SPAN to support brownfield

What's Next?



nVIDIA

Partnership

**CISCO
HYPERSHIELD**

**CISCO
AI Defence**

splunk>
a **CISCO** company

**CISCO
Hybrid Mesh
Firewall**

Guardiani Digitali: Cisco Security Event

16 Aprile – MILANO – Ore 10.00

Agenda:

- Overview and Vision
- Ethical Hacker demo & Security Trends
- Cisco Security Innovations and AI
- Cisco Security & Firewalls
- Cisco 360: the new partnership e TD Synnex services
- Q&A

Registrati Subito!





Cisco SASE

Secure and seamless connectivity to any application, over any network. Anywhere.

Giacomo Casati

Technical Presales Specialist, TD SYNEX

giacomoalberto.casati@tdsynnex.com

Applications and users are **everywhere** making secure connectivity hard



Hyper-distributed environments are the new reality



85%

Organizations aren't adequately prepared to handle cybersecurity threats



78%

Organizations report that high number of security tools is driving complexity

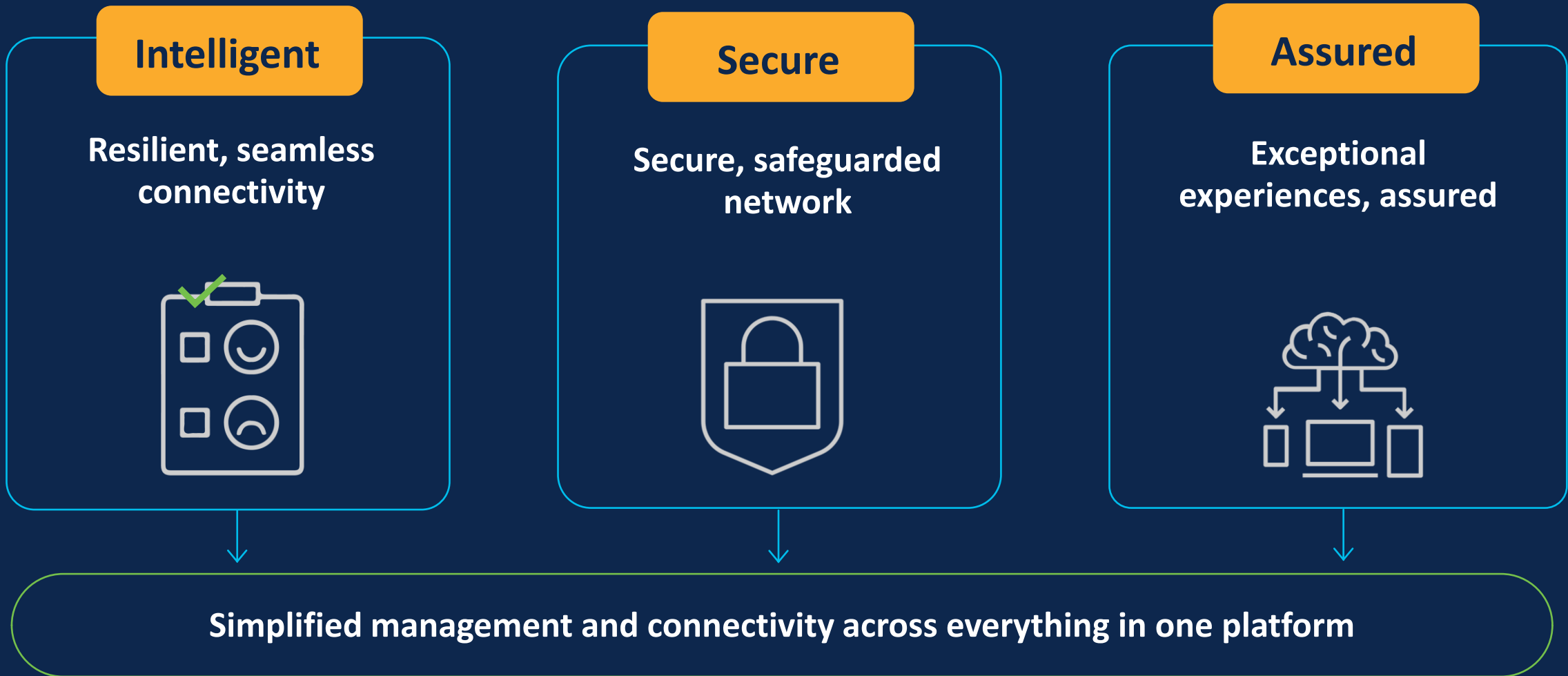


94%

IT leaders report that users bypass their current VPN solution

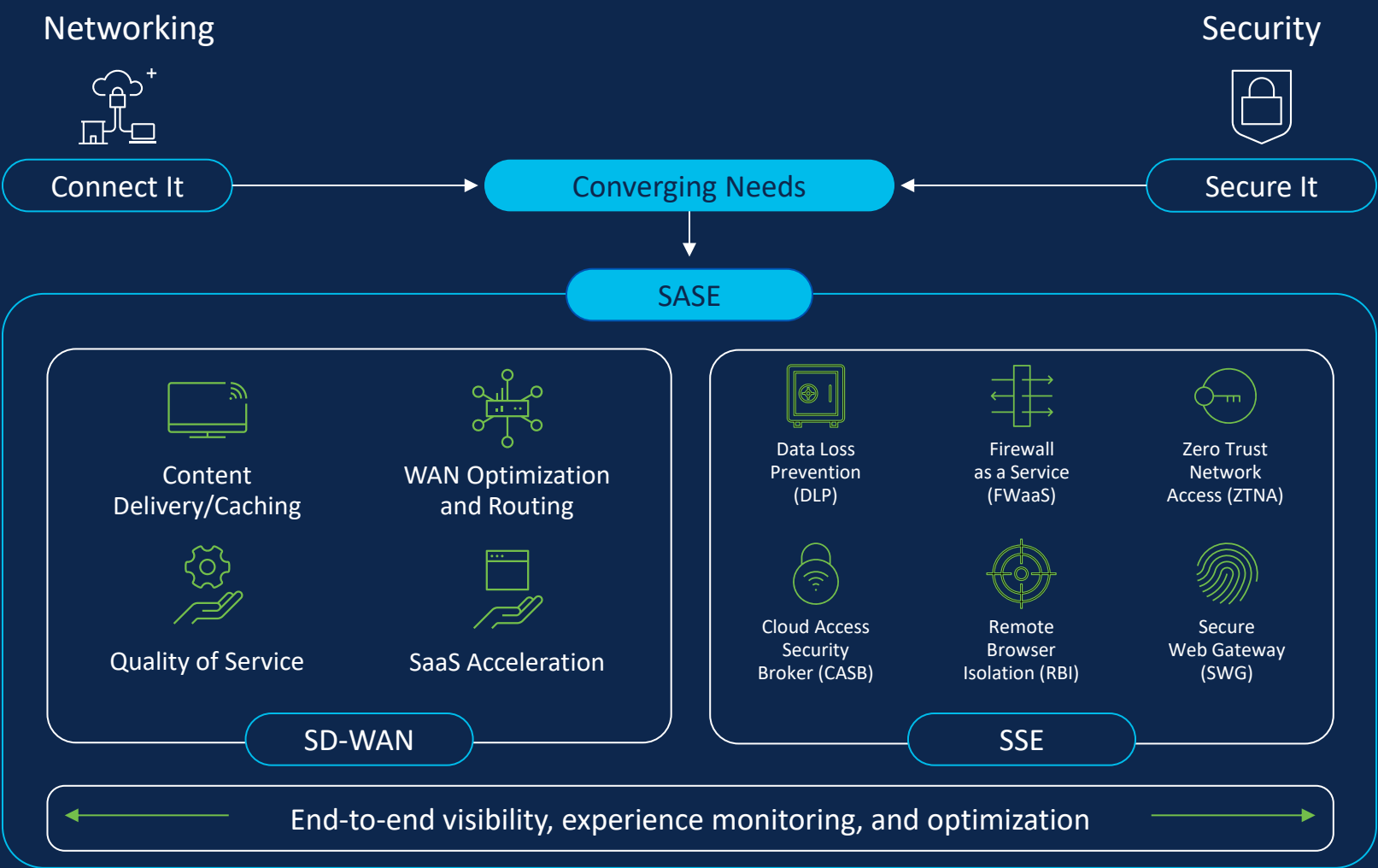
Diverse IT landscapes make secure connectivity hard

3 key qualities of an end-to end trusted experience



Secure Access Service Edge (SASE)

The architecture for a securely connected experience in today’s hyper-distributed environment



SASE your way

Cisco solutions designed to meet you on your journey to secure connectivity, anywhere

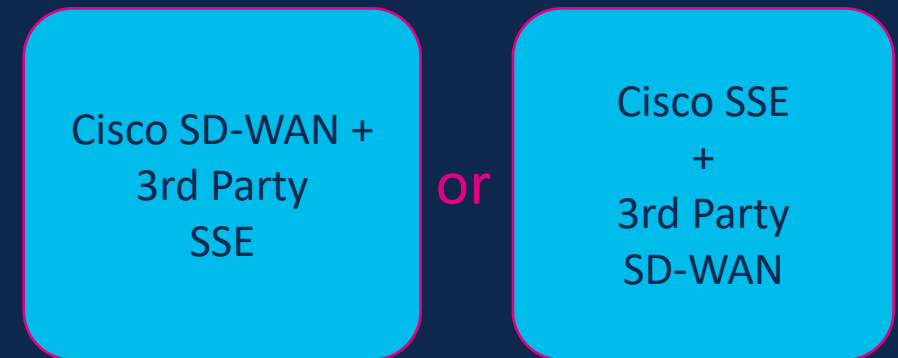
Cisco SASE

Powerful, flexible, and intelligent



Open SASE

Open, validated integrations



Cisco SASE powers secure connectivity, everywhere

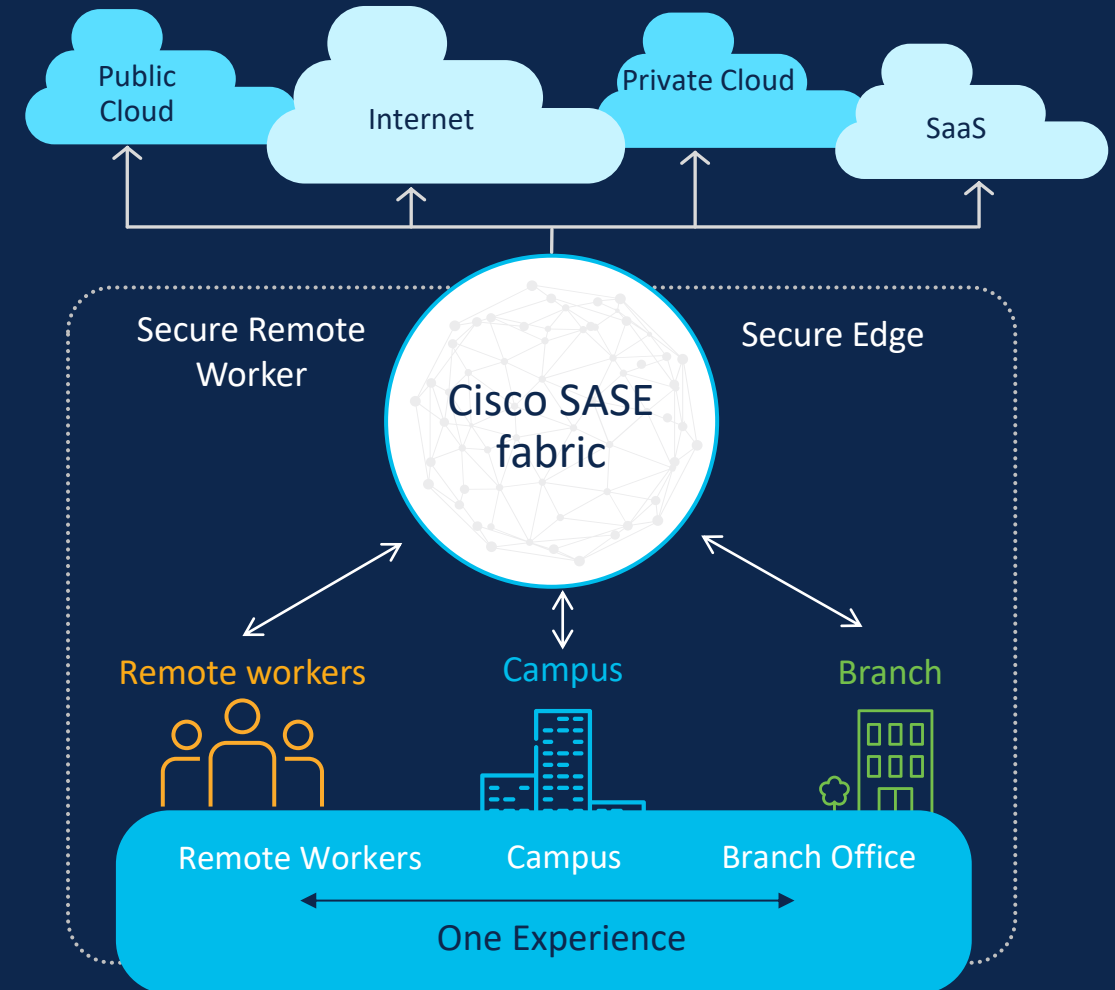
Use cases designed with always-on cloud security for an elevated remote worker experience

Secure Remote Worker

- Enables identity-based security to connect remote users from anywhere
- Applies zero-trust policies that establish least privileged access
- Provides visibility across the digital environment

Secure Edge

- Securely connects places—like branch offices and branch users—as well as IoT and OT to public Internet, SaaS, and private applications
- Easily manage policy enforcement at the source for user, application and device
- Secure orgs in a way that is simple yet highly reliable by natively extending the SD-WAN fabric



Powering Cisco SASE

Cisco Secure SD-WAN

Connected and protected

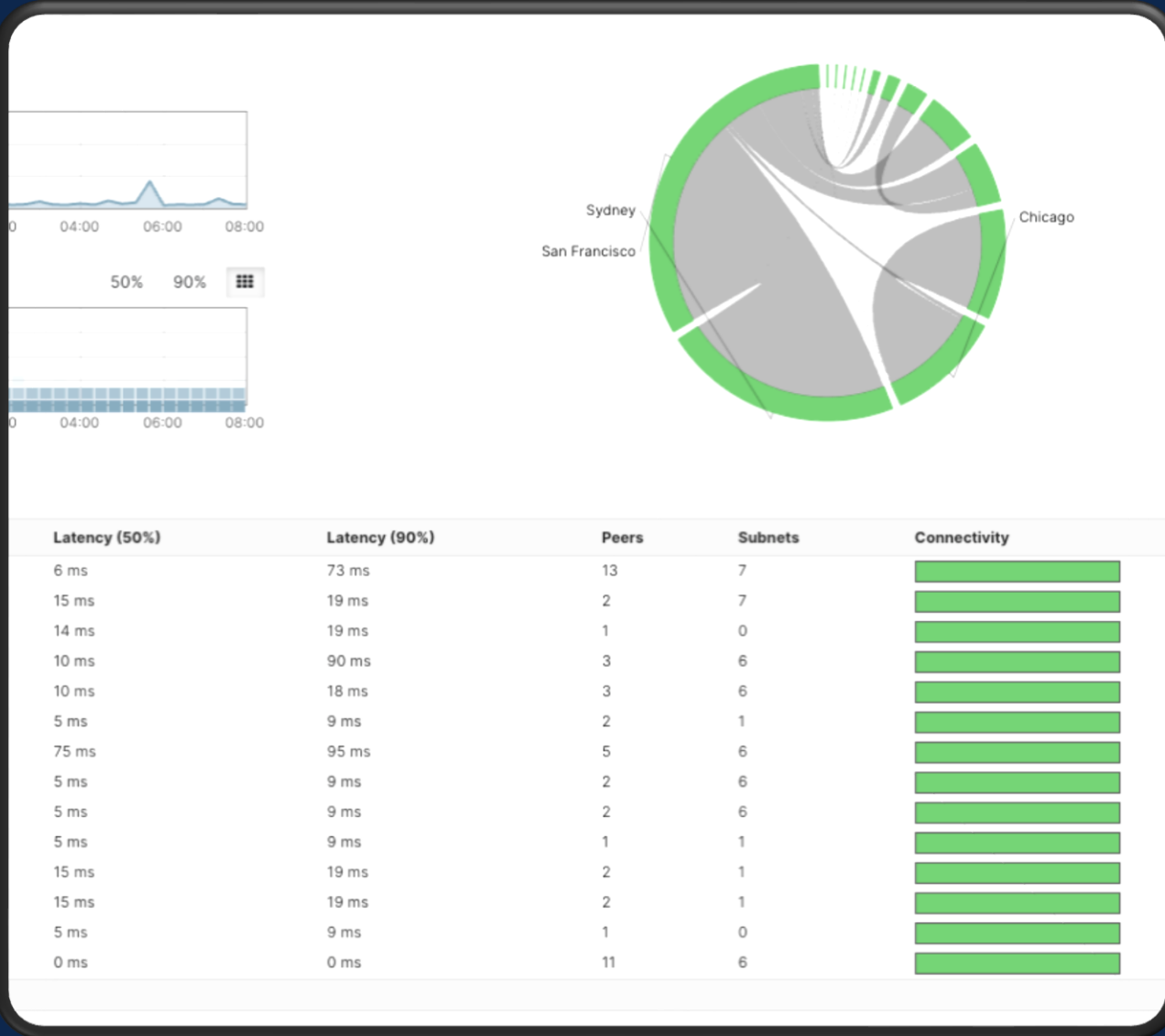
- Access to any device or application
- Seamlessly integrated security

Simple and easy

- Cloud-agnostic connectivity
- Easily managed and automated

Streamlined operations

- Centralized management
- Single dashboard



Cisco Security Service Edge (SSE)

Most comprehensive SSE solution

- 3x the SSE capabilities in one cloud service and subscription
- AI-first Security Service Edge (SSE)

Universal user experience

- Seamless, secure access connecting to anything from anywhere
- High performance zero trust

Simplified IT operations

- Converged security in one console, one client, one cloud-based platform
- AI-guidance for configuration



Cisco SASE

Designed for simplicity and flexibility

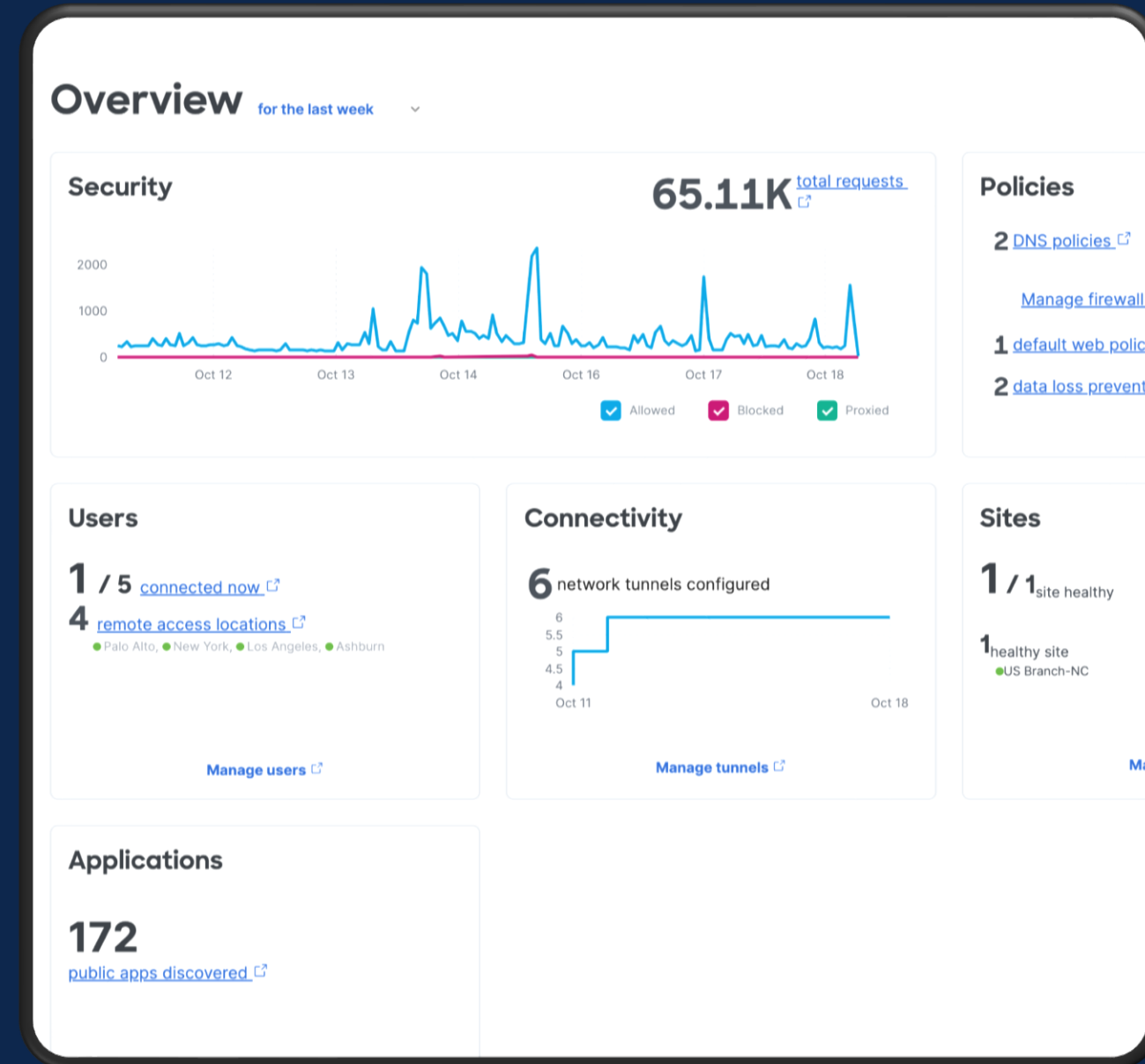
- Consistent UX across premises to cloud
- Caters for organizations of all sizes

Interconnects everything

- Networking and security management for NetOps, SecOps or converged NetSecOps
- Integrating SD-WAN and SSE in a single SASE platform

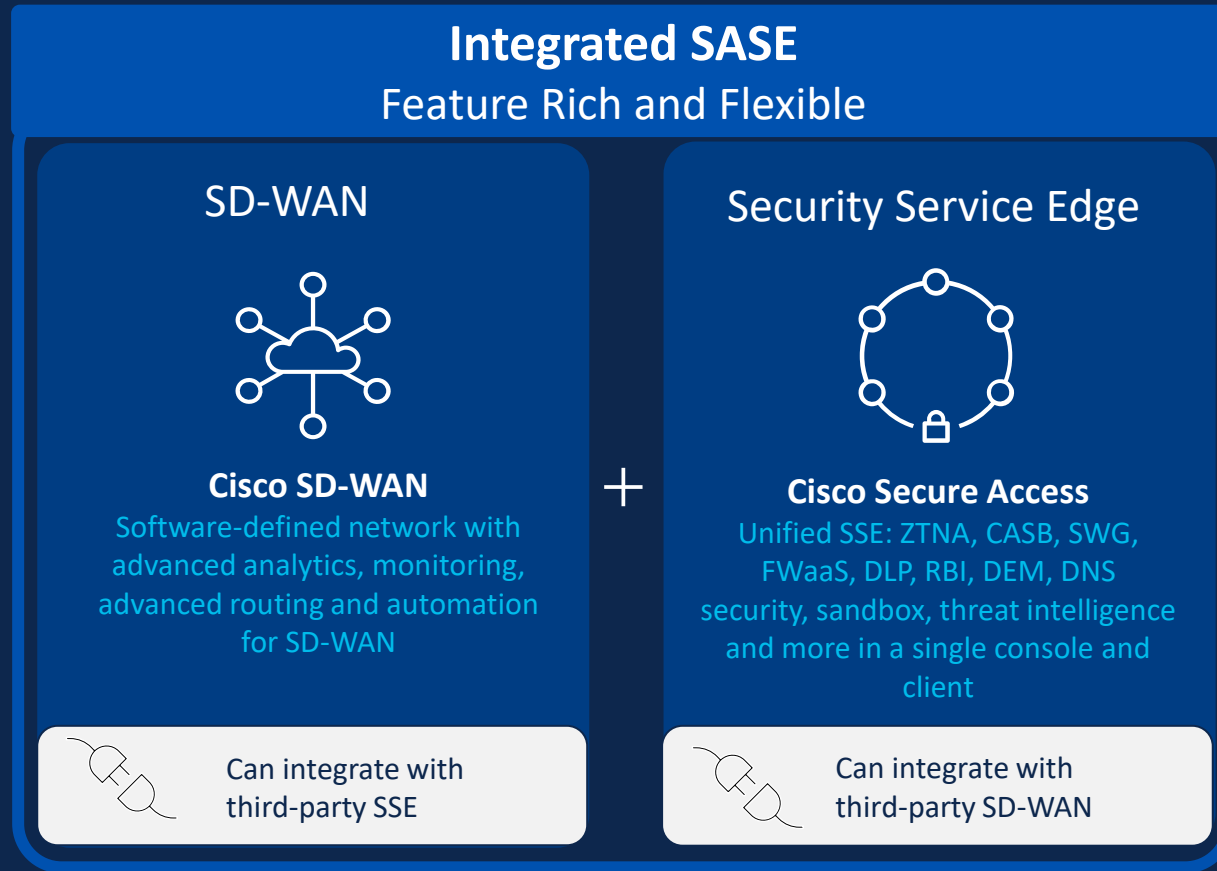
Secure everywhere

- Centralized management with distributed enforcement
- Advanced zero trust capabilities



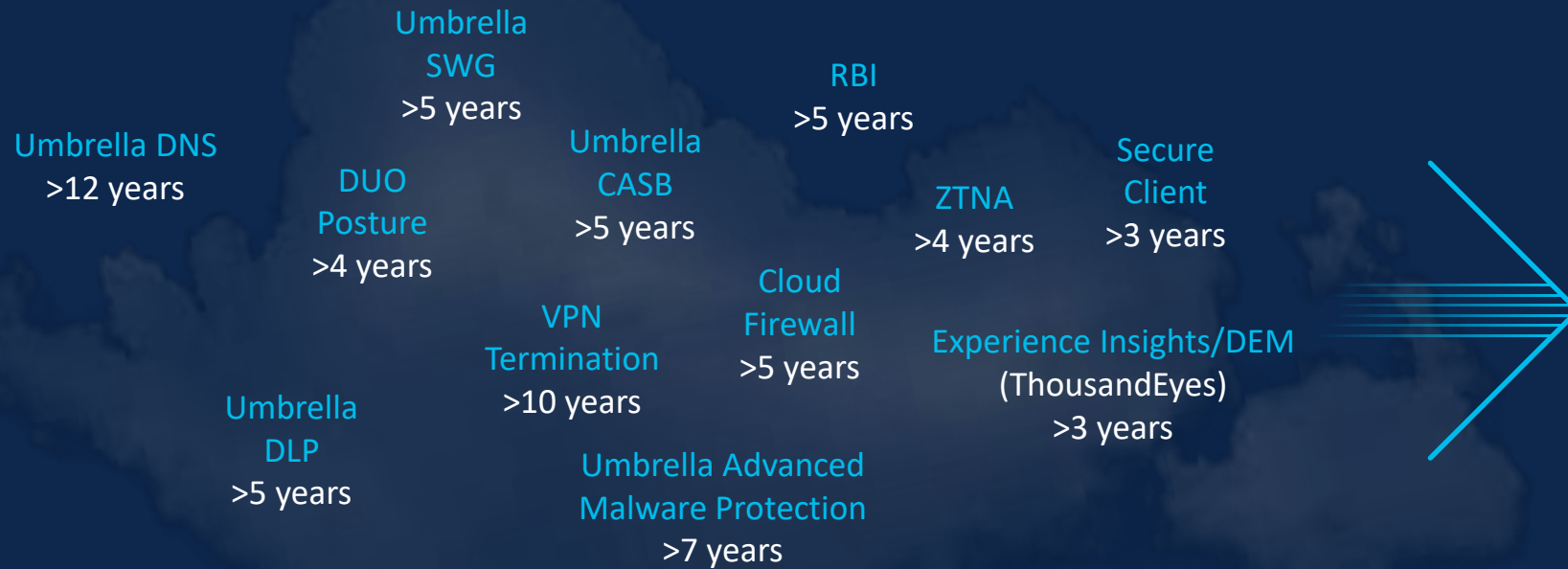
Cisco SASE Your Way

Single-vendor Cisco solutions designed for secure connectivity, anywhere



Introducing Cisco Secure Access

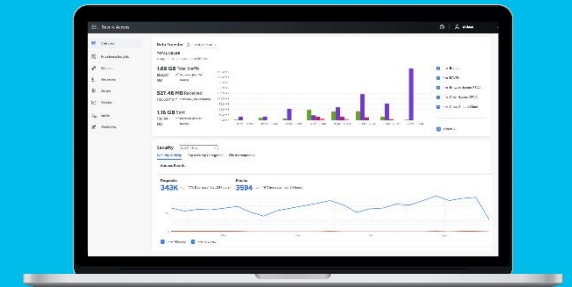
Proven cloud-native security converged into one service



Protecting 70,000+ customers

More than 220M endpoints

Cisco Secure Access



- Single Console
- Single Client
- Unified Policies

Modernize your defense with Cisco Secure Access

Converged cloud-native security grounded in zero trust



Cisco Secure Access

Go beyond core Secure Service Edge (SSE) to better connect and protect your business

Core SSE



Secure Web
Gateway
(SWG)



Cloud Access Security
Broker (CASB) and
DLP



Zero Trust
Network
Access (ZTA)



Firewall as a
Service (FWaaS)
and IPS

Cisco delivers the core and more in a single subscription...



DNS
Security



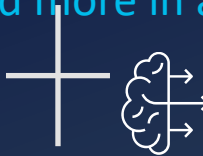
Multimode
DLP



Advanced
Malware
protection



Sandbox



Talos Threat
Intelligence



VPN as a
Service



Digital
Experience
Monitoring*



Remote
Browser
Isolation*

* Included in the unified experience / separate license (optional)

Add-on solutions



SD-WAN



XDR



DUO MFA/
SSO



CSPM

AI-first Secure Access

AI powered algorithms

- Efficient threat hunting
- Quicker detection
- Faster blocking of attacks

NEW!

AI Assistant

- Speed policy administration by up to 70%
- Reduce complexity
- Mitigate human error

NEW!

DLP Generative AI

- Threat visibility
- reduced exposure
- data protection

Cisco Talos Threat Intelligence

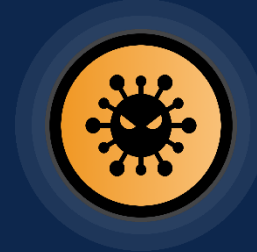
Unmatched visibility
across the threat
landscape
powered by experts,
data, and Gen AI



550B security events/**day**



~9M emails blocked/**hour**

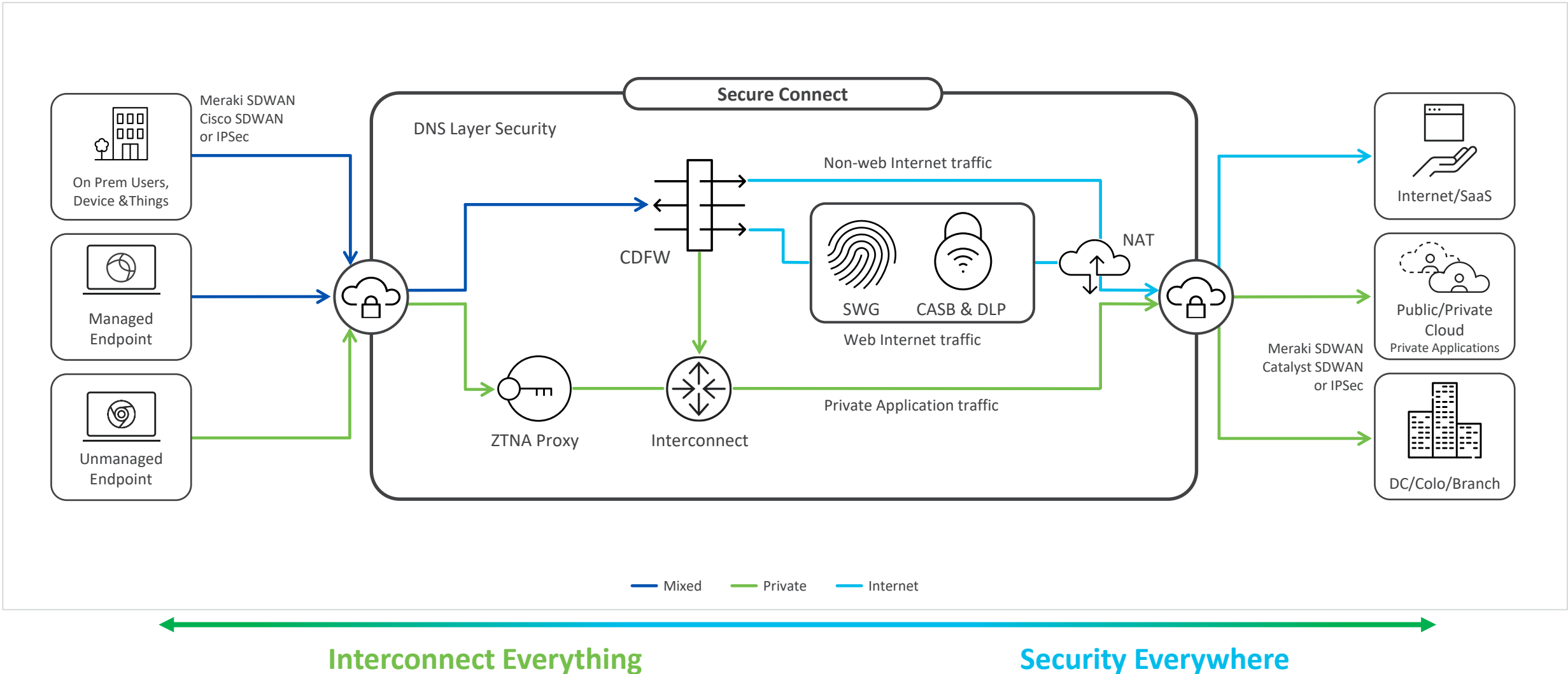


~2,000 new samples/**minute**

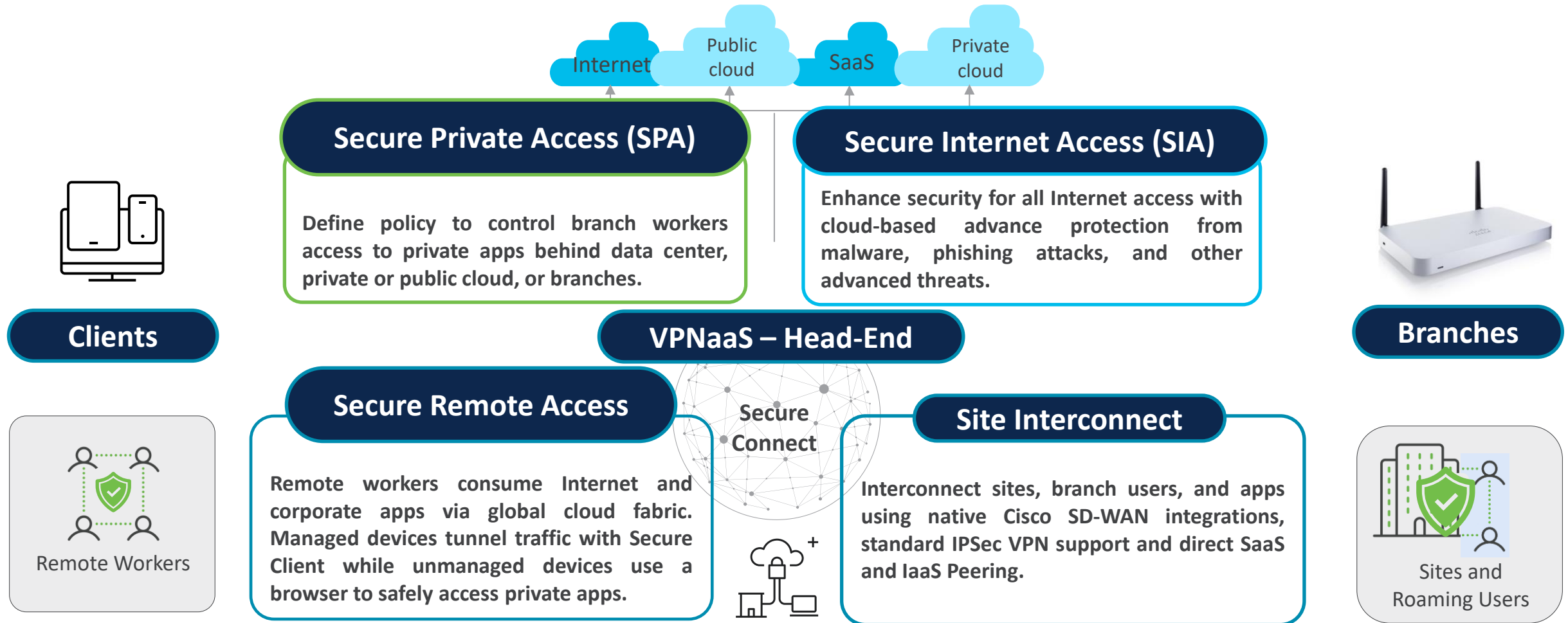


~2,000 domains blocked/**second**

Unlocking the Power of the Unified SASE with Secure Connect



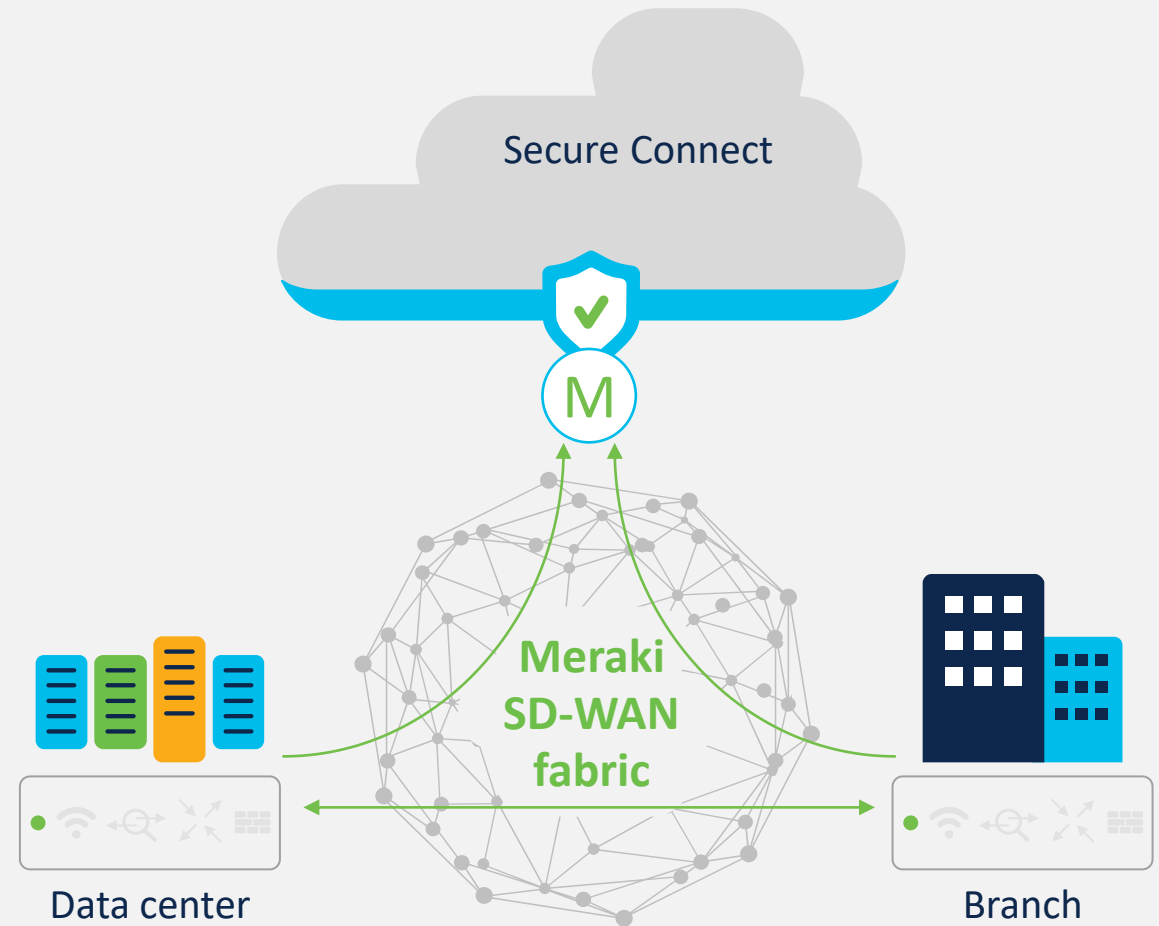
Secure Connect Use Cases



Meraki Site Interconnect

Easy setup to connect Meraki branches to Secure Connect

- Meraki® SD-WAN direct connection to Secure Connect fabric with Auto VPN for resiliency and intelligent path selection
- Advanced security capabilities for branch sites
- Private applications accessible by remote users within the SD-WAN fabric
- Quickly add sites or change regions from Secure Connect



Meraki SD-WAN Features

Capabilities

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

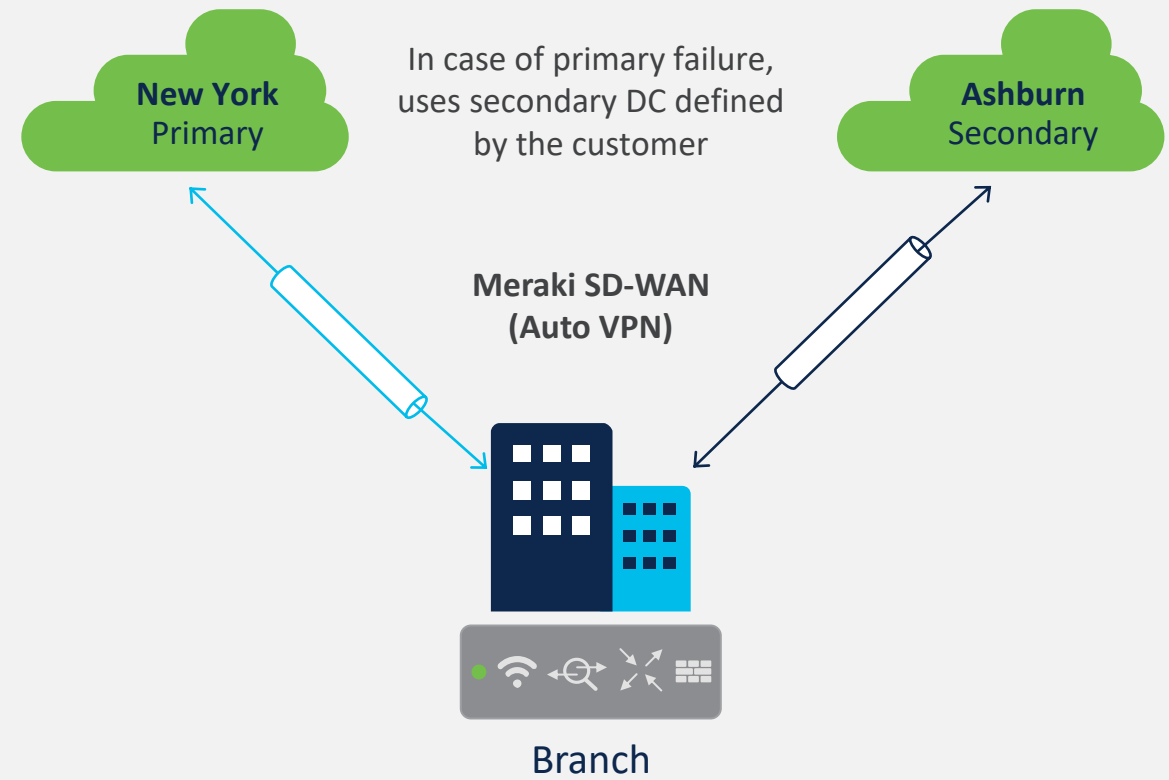
High availability

- 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

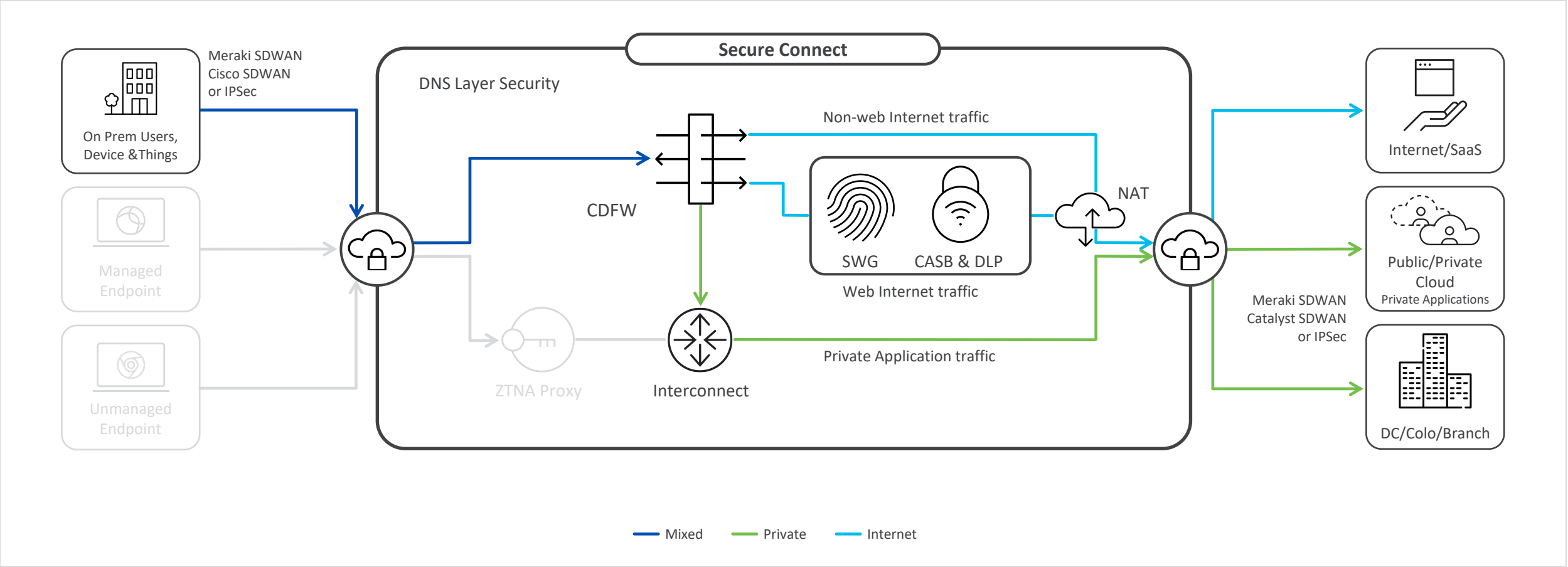


Secure Branch Traffic

Site Interconnect

SIA

SPA



Meraki SD-WAN Onboarding – Assign Region

- Quick add (1) of existing Meraki branches
- Select Branches (2) and assign to Region or Cloud Hub (3 and 4)

Assign region to onboard network

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

Unassigned 1 **Assigned** 0

den

1 Item selected [Clear all](#) [Cancel](#) **3 Assign to Region or Cloud Hub**

<input checked="" type="checkbox"/>	Networks & Templates	VPN	Type	Address
2 <input checked="" type="checkbox"/>	DEN-booth-site-108	Off	MX100-HW	

Assign site directly to these regions
Internet & Private App Access

US West
Los Angeles/Palo Alto

US Northeast
New York/Ashburn

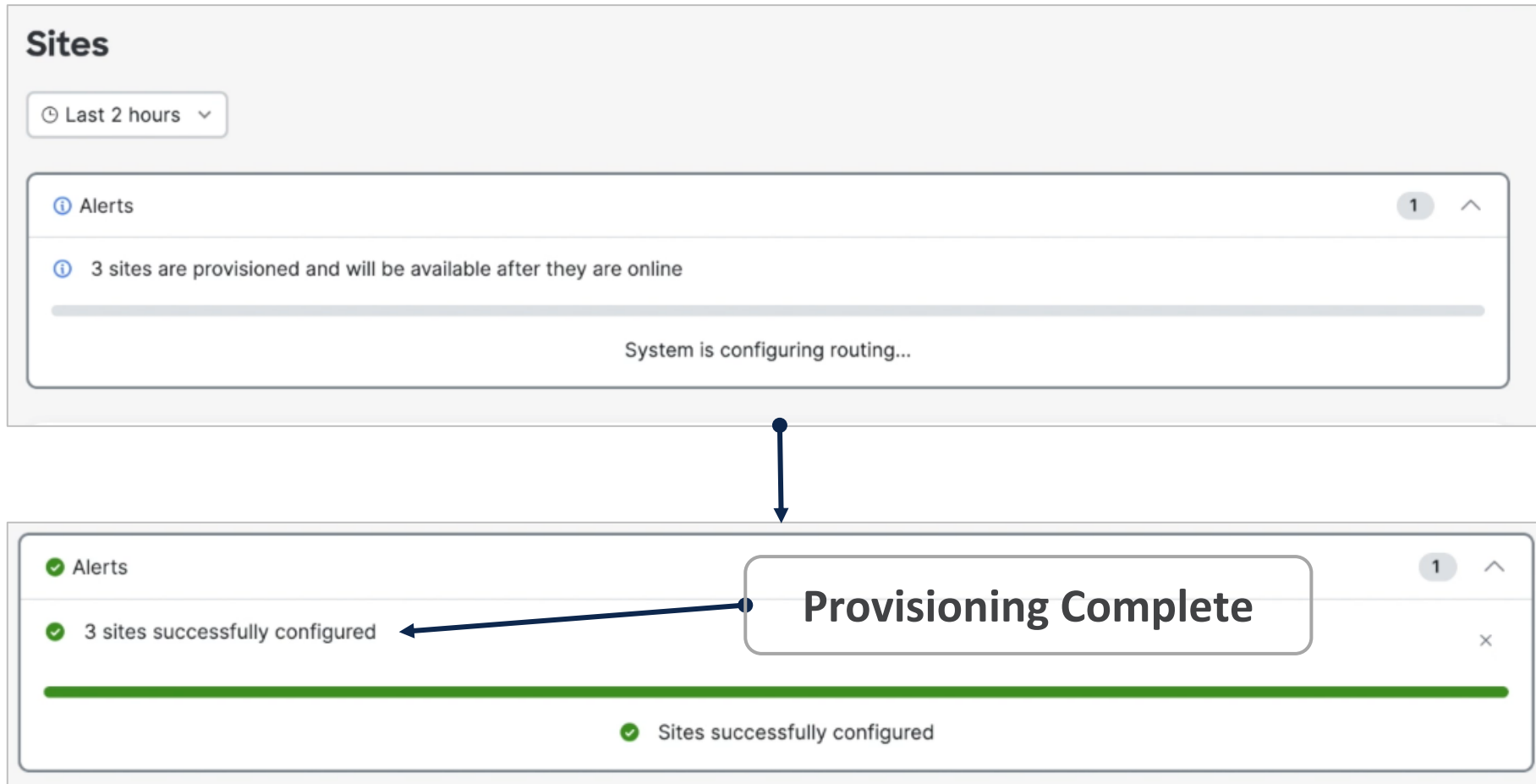
Assign site to Cloud Hub in these regions
Internet Access Only
Up to 24 Cloud Hubs can be deployed.

[Configure Cloud Hubs](#)

hub
Rio de Janeiro/Sao Paulo

[Back](#) [Finish and Save](#)

Meraki SD-WAN – Review Real-Time Provisioning



Firewall Rule

Cloud Firewall

Create firewall policy rules to control network traffic based on IP, port, and protocol. Rules are evaluated from the top down. [Firewall policy documentation](#)

Cloud IPS settings

Rules

Search

Filters 10 results

#

Rule name

Status

Action

Protocol

1

RAVPN-Finance-allow-app-NAP-108
Private app and network

Enabled

Allow

N/A

Finance Group

2

Branch-Finance-allow-to-app-NAP-108
Private app and network

Enabled

Allow

N/A

10.100.0.0/13 10.200.0.0/13

+ Add rule

Internet traffic rule

Private application and network rule

Create FW Rules
anew or leverage
Policy Import.

Identity Source to Internet or
Private Applications as the
Destination

Rule description

Rule name: RAVPN-Finance-allow-app-NAP-108, Priority: 1, Description:

Rule intent

Source: Finance Group (dcloud.local\Finance Group) (7), Action: Allow, Destination: web-108

Rule schedule and logging

Rule starts: Immediately, Rule ends: Never, Logging: Enabled

Rule status

Enable or disable the rule. [Enable]

Cancel

Delete rule

Apply Changes

Policy Import from MX into Secure Connect

- On-premise policy rules are reviewed, selected, and added to Secure Connect
- Reduce transition time to cloud fabric
- Identify and review duplicate and unused rules

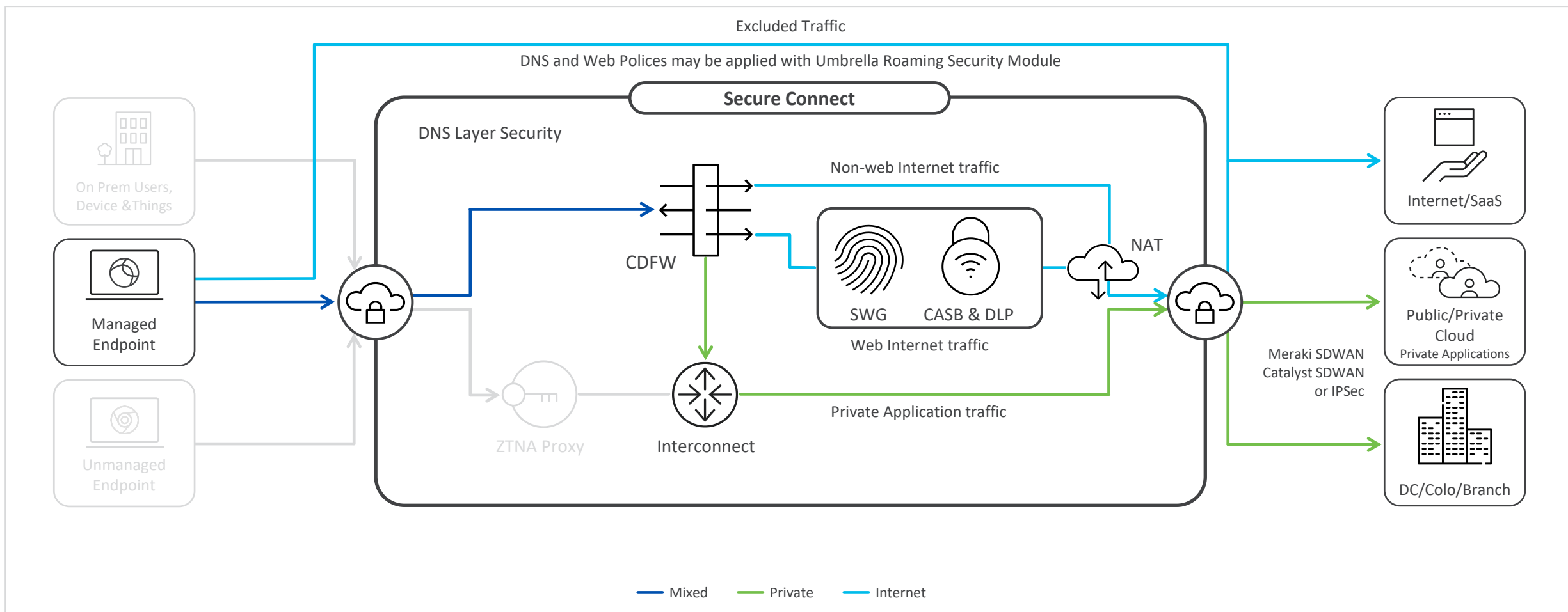
The screenshot displays the Meraki Secure Connect web interface. The main heading is 'Policy Import from MX Client VPN', with a subtext: 'Select the network and associated rules to import with Secure Connect. View [Documentation](#) for details.' The workflow consists of four steps: 1. Select Networks (active), 2. Select Firewall Rules, 3. Fix Duplicate Rules, and 4. Summary.

Under the 'Select Networks' step, there is a search bar and a filter dropdown showing '6 results'. Below this, a table lists available networks with checkboxes for selection. Two networks, 'SFO - 2' and 'SFO - 3', are currently selected.

	Network	Model	Device Name	Public IP Address	Location	No. of Rules
<input type="checkbox"/>	ATL - 12	MX60	Austin	192.168.1.1	Austin	50
<input type="checkbox"/>	NYC - 7	MX67W	New York	192.168.1.10	New York	45
<input type="checkbox"/>	NYC - 8	MX68	New York2	192.168.1.5	New York Main	125
<input checked="" type="checkbox"/>	SFO - 2	MX250	San Francisco2	192.168.1.7	San Francisco Meraki	20
<input checked="" type="checkbox"/>	SFO - 3	MX450	San Francisco3	192.168.1.30	San Francisco	25
<input type="checkbox"/>	SJC - 1	MX450	San Jose1	192.168.1.9	San Jose Main	55

At the bottom, there are 'Cancel' and 'Save and Next Step: Select Rules' buttons.

RAVPNN Client with Traffic Steering



RAVPN Cloud Head-End Setup and Review


Define Regions to Provision Head-Ends and save will then Generate FQDN

Assign Private Subnet Ranges for Clients

Specify DNS servers and domain

Get Started Secure Client

Configure regions
In each selected region, enable at least 2 data center locations to route traffic through.

 Ensure there are no overlapping IP pools across locations.

☐ Asia Pacific & Oceania

0 enabled locations

▼

☐ Europe

0 enabled locations

▼

☐ North America

0 enabled locations

▼

DNS Servers ⓘ
Add the IP addresses of your organization's private DNS servers.

DNS server IP address 1 *

IP address

DNS server IP address 2 (optional)

IP address

Default domain * ⓘ

e.g. "domain.com"

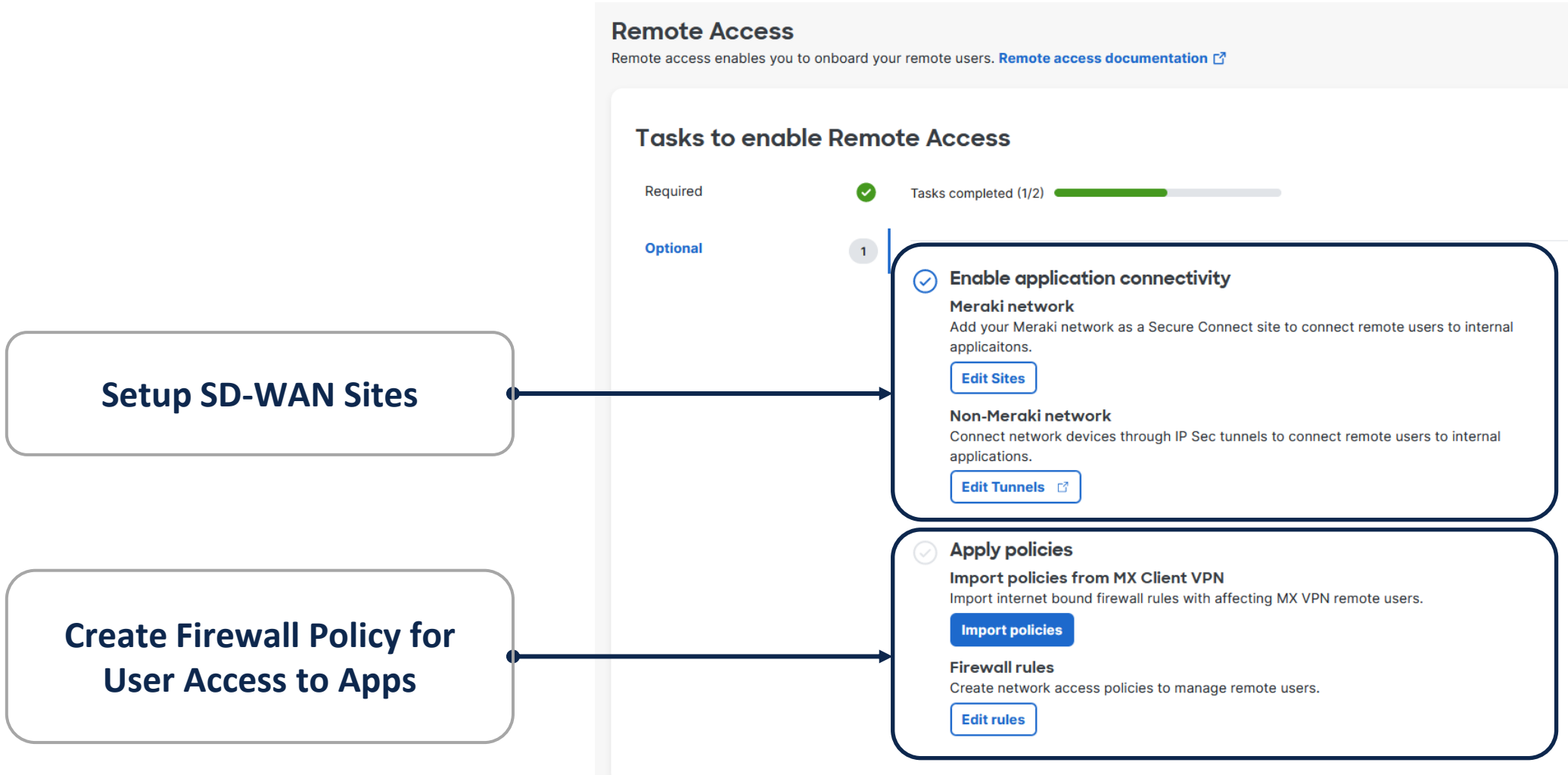
Additional DNS Names (optional) ⓘ

Add up to 25 DNS names separated by commas.

Proceed to configure Secure Client and traffic steering
After saving, options to configure Secure Client and traffic steering will be available in the next view.

Save

Remote Access Setup



Traffic Steering Option under Remote Access

Enable to Configure Options for Traffic Steering

Define how to Steer: Outside or Inside the Tunnel

I.e., list RDP Client IP range(s) to exclude from RAVPN tunnel on your RDP server

Regions DNS Secure Client **Traffic Steering**

Send all traffic through the tunnel? ⓘ

☐ Yes, send all traffic ☒ Customize traffic steering

Local area network (LAN) access ⓘ

☒ Enable LAN access for remote users

How to send all remote users' traffic ⓘ

☒ Send all traffic except traffic going to these destinations

☐ Only send traffic going to these destinations

Do not tunnel to these destinations

Traffic to these destinations will be steered outside the tunnel as exceptions.

Preview

Remote user Tunnel Private apps Internet Destination exceptions LAN access

Add destination

☐ **Destinations** ⓘ

☐ 88.188.0.0/16

Exceptions (optional) ⓘ

Enter an IPV4, subnet CIDR, or domain

DNS resolution ⓘ

Standard DNS (Default)

Save

Enhanced Posture Endpoint Compliance

Client-based posture enforces:

- Certificate
- OS Versions
- Anti-malware Software
- Firewall
- Disk Encryption

Endpoint Posture
Configure requirements for endpoint devices to connect to a network

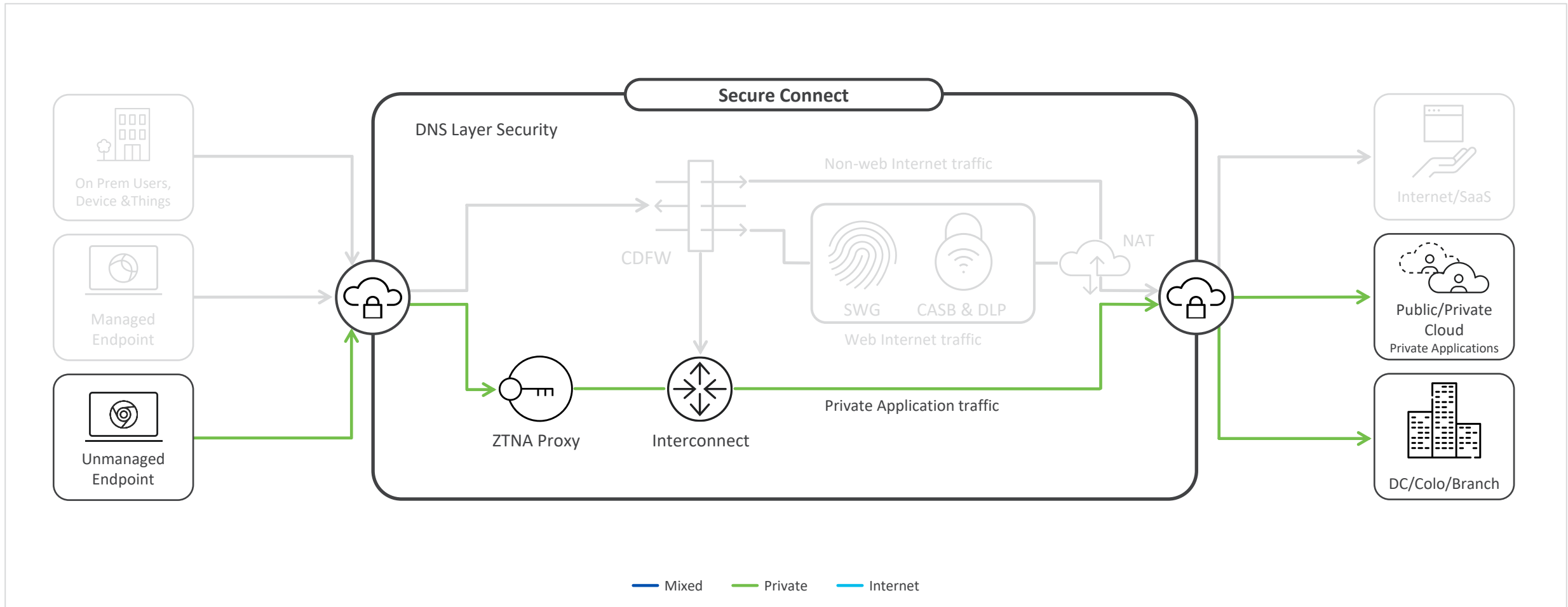
Browser-based access

Client-based access

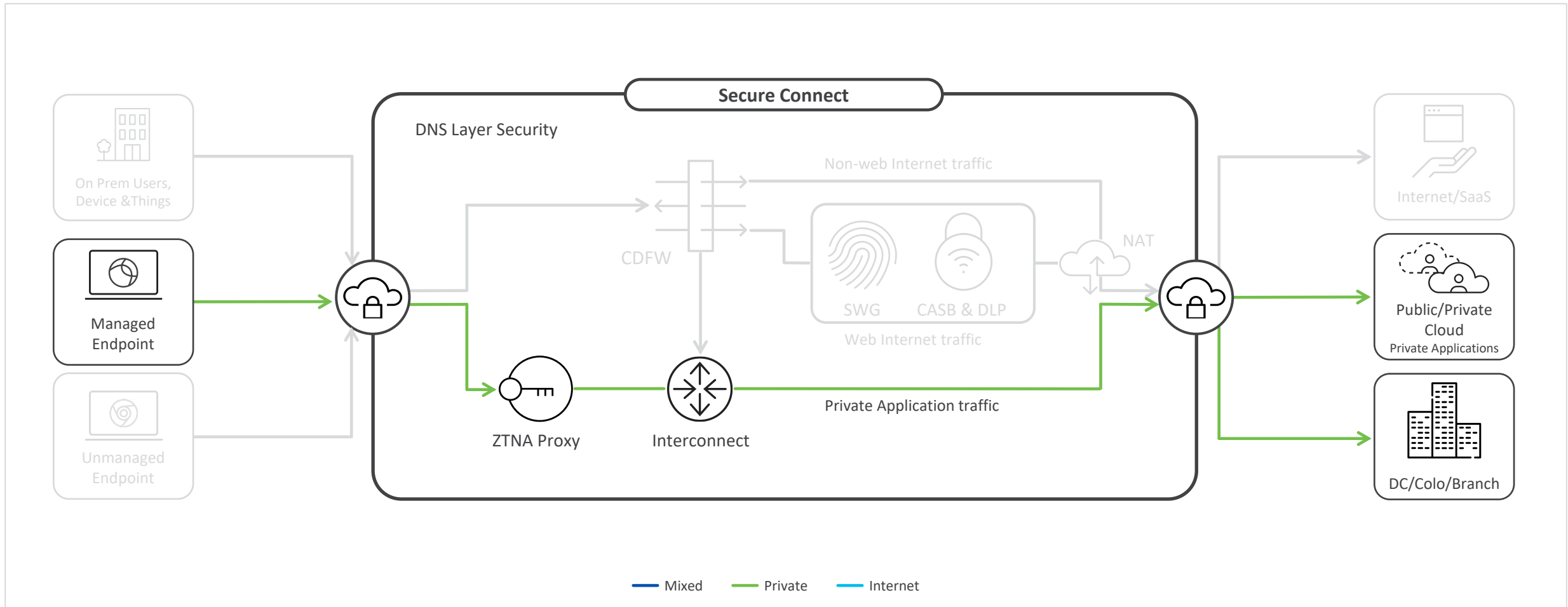
Client-based access
Requirements for endpoints connecting to Cisco Secure Client.
[Documentation on client-based access](#)

<div>Certificate</div> <div>None</div>	<div>Operating Systems</div> <div>10.0.22000, 10.0.22621, 10.0.22631, Latest</div>	<div>Anti-Malware</div> <div>AVG Anti-Virus</div>	<div>Firewall</div> <div>No firewall required</div>	<div>Disk Encryption</div> <div>No disk-encryption required</div>
--	--	---	---	---

Zero Trust Access – Browser-based



Zero Trust Access – Client-based



Define Private Apps behind MX Branches

- Define IP addresses or ranges
- Select protocol and enter ports or port ranges
- App connector in roadmap

← Applications

Add Application

Define access methods for your private application and assign it to a group. Private applications and groups can be referenced as destinations in cloud firewall and zero trust access policies. [Private application documentation](#)

General info

Application name

Private App 2

+ Add description

Network address

Specify one or more network addresses to route traffic to this application.

Network address

Application address ⓘ	Protocol	Port/port range
192.16.0.0-192.16.0.48	TCP	49154
	UDP	40
	TCP - HTTP/HTTPS	40

Select VPN Access Methods to Private App

- Enable access to private app for VPN tunnel user
- VPNaaS in Secure Connect
- Secure Client VPN module

☒

VPN

When enabled, allowed users and devices can access this private application on configured addresses via the client VPN, Cisco Secure Client.

VPN configurations

	Network address	Protocol-port pairs
<input checked="" type="checkbox"/>	192.16.0.0/12	TCP, 20 UDP, 40 TCP, HTTP/HTTPS, 40
<input checked="" type="checkbox"/>	1.1.1.1	TCP, 20

Select ZTA Access Methods to Private App

- Secure Client ZTA module
- Client-less Browser access

Zero trust access

Allow endpoints to connect to this resource from outside your network without requiring a VPN connection.

☒ **Client-based**

When enabled, allowed users and devices can access this private application on configured addresses via client-based endpoint posture validation.

Client-based configurations

Network address	Protocol-port pairs
<input checked="" type="checkbox"/> 192.16.0.0/12	TCP, 20 UDP, 40 HTTPS, 40
<input checked="" type="checkbox"/> 1.1.1.1	TCP, 20

☒ **Browser-based**

When enabled, allowed users and devices can access this private application on configured addresses via browser-based endpoint posture validation.

Browser-based configurations

☒ 192.16.0.0/12

Protocol: Server name indication: External URL:

Validated application certificate

☒ Enable

Endpoint Posture for Zero Trust Access

- Create two types of access type posture
- Show associated rules

Endpoint Posture

Configure requirements for endpoint devices to connect to a network.

Zero trust accessVPN access

Profiles

Create profiles for client-based or browser-based access. Enable profiles by associating them to [zero trust access policies](#). [Zero trust access endpoint posture profile documentation](#)

Access type ▾

 X results

+ Add profile

Profile name	Access type	Requirements	Associated rules ⓘ
New profile 1	Client-based	Operating system Firewall Endpoint security agent System password Disk encryption	Rule 1 Rule 2 Rule 3 Rule 4 Rule 9 +3
Temp access	Browser-based	Operating system Browser Location	Rule 1 Rule 2 Rule 3
New profile 2	Client-based	Operating system Firewall Endpoint security agent System password Disk encryption	Rule 1

Endpoint Posture for Remote Access VPN

- Define a profile to enforce for Remote Workers

← Endpoint Posture Summary

Remote Access VPN Endpoint Posture

Configure requirements for endpoint devices to connect to a network.

Certificate

Operating Systems

Anti-Malware

Firewall

Disk Encryption

Operating Systems

Require specific operating systems for endpoints to connect to the network.

Require the following operating system(s):

Windows × Mac OS X ×

Grace period for latest version ⓘ

Users must upgrade to the required version within: 2 weeks

Windows

Zero Trust Access - Policies

Zero Trust Access Policies

Create rules to control and secure access to applications. [Zero trust policies documentation](#)

✓ New rule added
Manager access

Rules

+ Add rule

Q Search

Filters 123 results

#	Name	Action	Users & Groups	Apps & Groups	Posture ⓘ	Hits
1	Manager access <div>✓ Enabled</div>	✓ Allow	Managers	<div>AWS App name 2</div> <div>Asana Designer apps</div> <div>Show 3 more</div> <div>2 ZTNA methods ⓘ</div>	<div>Managers</div> <div>Remote worker</div>	No Data ...
2	HR access <div>✓ Enabled</div>	✓ Allow	HR	<div>HR apps</div> <div>Client-based access</div>	HR	No Data ...
3	Sales access <div>✓ Enabled</div>	✓ Allow	Sales	<div>Sales apps</div> <div>Browser-based access</div>	Sales	No Data ...
4	Sales access <div>✓ Enabled</div>	✓ Allow	Sales	<div>Sales apps</div> <div>Client-based access</div>	<div>Sales</div> <div>Contractors</div>	No Data ...
5	Engineer access <div>⊖ Disabled</div>	✓ Allow	Engineers	<div>Engineer apps</div> <div>2 ZTNA methods ⓘ</div>	<div>Engineers</div> <div>Remote worker</div>	No Data ...
ⓘ	Default rule <div>✓ Enabled</div>	⊘ Deny	All	All	None	No Data ...

Create ZTA rules using Users/Groups, defined private apps and posture profiles

Positioning SSE and SASE*

Outcome:

Leverage the power of the Meraki platform to unify and simplify networking and security

Select best-of-breed SD-WAN and SSE to be integrated tightly but managed separately

Architecture:

Meraki MX

Catalyst SD-WAN

3rd Party SD-WAN

Offer:

Cisco Secure Connect

Cisco Secure Access

Cisco Secure Access

“If you don’t innovate fast, disrupt your industry, disrupt yourself, you’ll be left behind”

John Chambers

Q&A

PROSSIMI APPUNTAMENTI

CI VEDIAMO A MAGGIO CON I NUOVI APPUNTAMENTI

STAY TUNED!

<https://events.tdsynnex.it/cyber-unit-missione-protezione/>

TEAM CISCO: it.cisco@tdsynnex.com

SPEAKER: federico.frosini@tdsynnex.com,

giacomoalberto.casati@tdsynnex.com, andrea.pezzoni@tdsynnex.com