Meraki TechClub

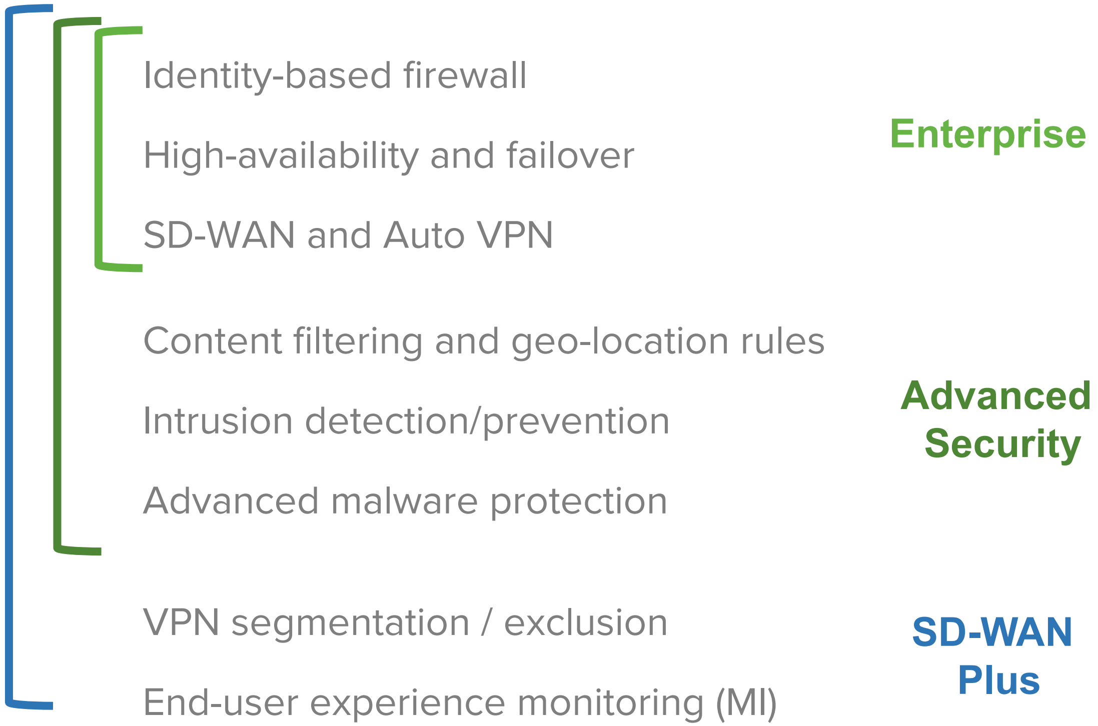
MX update
SASE / SIGRAKI
Cisco+ Secure Connect
Cloud Monitoring
System Manager

Andrej Jeleník
Cisco Systems Engineer

Cisco Meraki

MX Security & SD-WAN

FEATURED HIGHLIGHTS



- Identity-based firewall
- High-availability and failover
- SD-WAN and Auto VPN

Enterprise

- Content filtering and geo-location rules
- Intrusion detection/prevention
- Advanced malware protection

Advanced Security

- VPN segmentation / exclusion
- End-user experience monitoring (MI)

SD-WAN Plus

NGFW, unified threat management and SD-WAN solution with advanced user experience analytics

Various models scaling from teleworker and small branch to campus and datacenter

Meraki Security & SD-WAN Portfolio

Secure SD-WAN

Small Branch

MX64

250Mbps

MX67/68

600Mbps

MX75

1Gbps

Medium Branch

MX85

1Gbps

MX95

2Gbps

MX105

3Gbps

Large Branch

MX250

4Gbps

MX450

6Gbps

Virtualized Headends

vMX

vMX-S

200Mbps

vMX

vMX-M

500Mbps

vMX

vMX-L

1Gbps

Wireless WAN

MG21/E

300Mbps

MG41/E

1.2Gbps

Teleworker

Z3/C

100Mbps

MX67 and MX68 Families w/ New Performance Improvements

MX67

MX68

MX67C

FIREWALL THROUGHPUT

450 → **600 Mbps**

VPN THROUGHPUT

200 → **300 Mbps**

MX68CW

MX67W

MX68W

Benefits of Cellular, Now Integrated

Connect Remote Sites

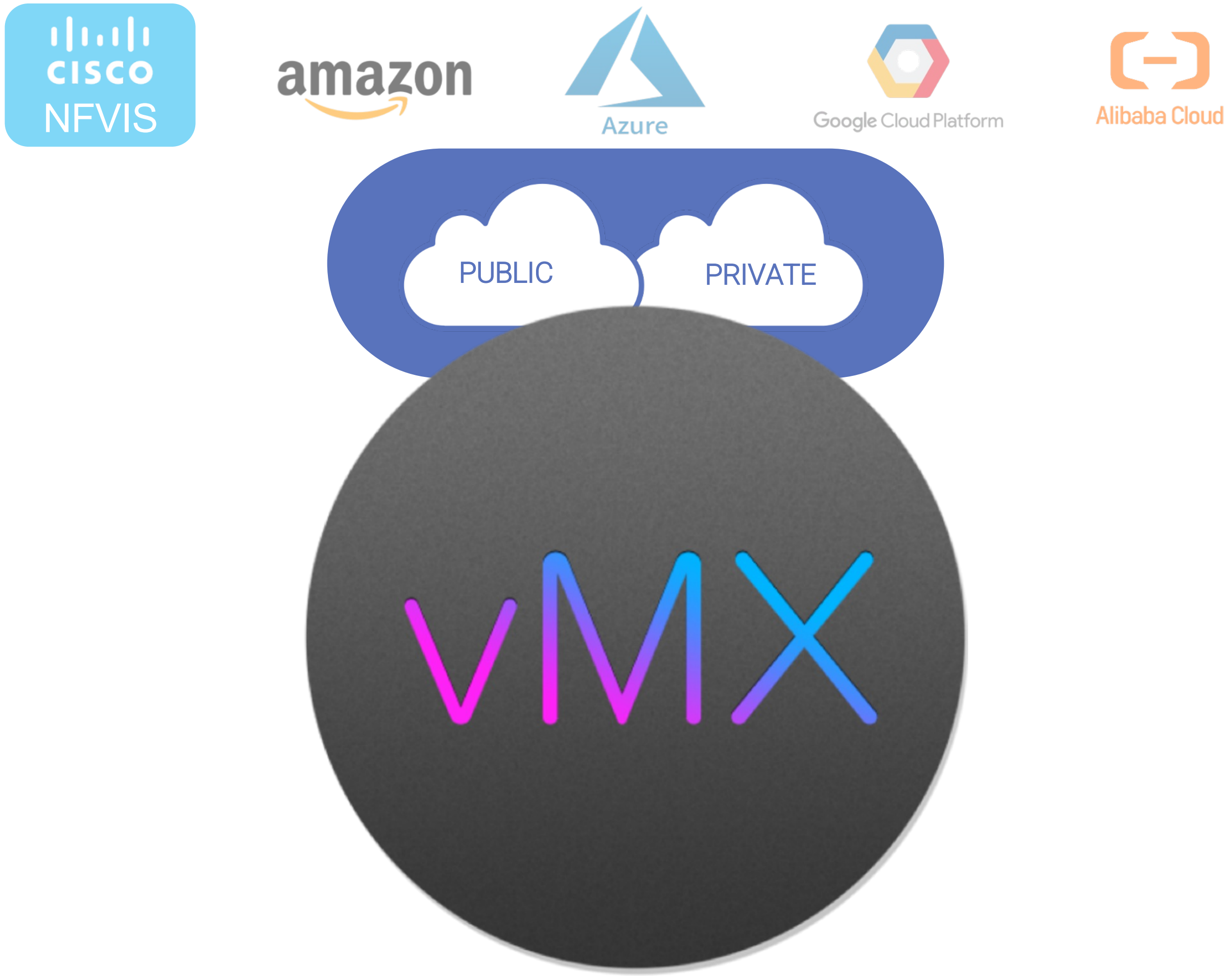
Limit downtime

SIM & LTE MODEM INTEGRATED

Meraki simple

multi-cloud connectivity

Three-click secure SD-WAN connectivity to private and public clouds



Licensing that fits the business’ needs

Enterprise

Essential SD-WAN features

Secure connectivity & basic security

All I need is AutoVPN and a firewall

Advanced Security

All enterprise features plus:

Fully featured
unified threat management

I connect to the internet,
so I need UTM security as well

Secure SD-WAN Plus

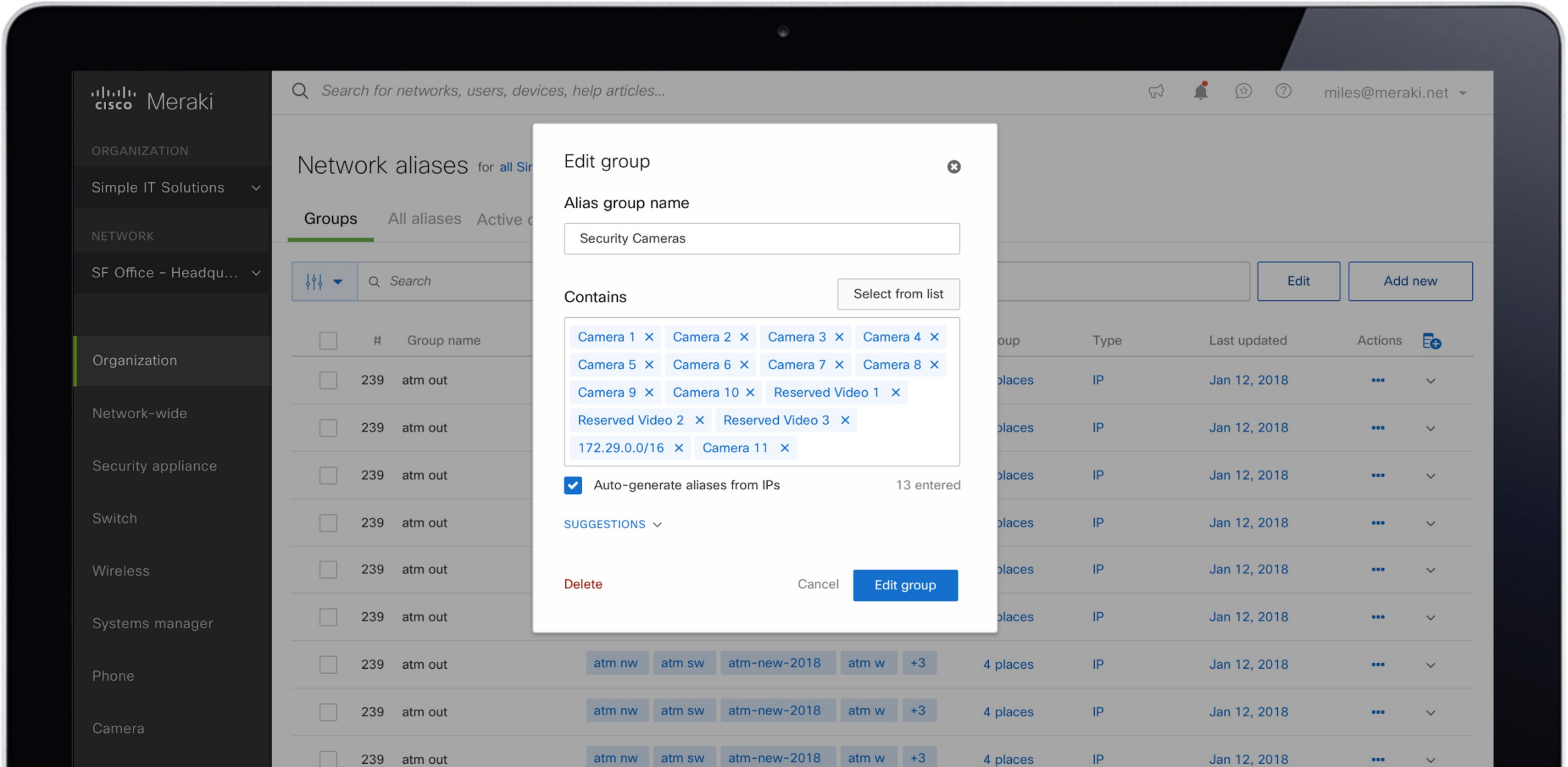
All advanced security features plus:

Advanced analytics with ML
Smart SaaS optimization
Segmentation

My business relies on apps served
from SaaS/IaaS/DC

Enhanced Firewall Rules on MX

Consolidate firewall rules using org-wide logical groups and objects * GA FY21Q1



Meraki

Search for networks, users, devices, help articles...

miles@meraki.net

ORGANIZATION

Simple IT Solutions

NETWORK

SF Office – Headqu...

- Organization
- Network-wide
- Security appliance
- Switch
- Wireless
- Systems manager
- Phone
- Camera

Network aliases for all Si

Groups | All aliases | Active

Search

Edit | Add new

	#	Group name		oup	Type	Last updated	Actions
□	239	atm out		places	IP	Jan 12, 2018	•••
□	239	atm out		places	IP	Jan 12, 2018	•••
□	239	atm out		places	IP	Jan 12, 2018	•••
□	239	atm out		places	IP	Jan 12, 2018	•••
□	239	atm out		places	IP	Jan 12, 2018	•••
□	239	atm out		places	IP	Jan 12, 2018	•••
□	239	atm out	atm nw, atm sw, atm-new-2018, atm w, +3	4 places	IP	Jan 12, 2018	•••
□	239	atm out	atm nw, atm sw, atm-new-2018, atm w, +3	4 places	IP	Jan 12, 2018	•••
□	239	atm out	atm nw, atm sw, atm-new-2018, atm w, +3	4 places	IP	Jan 12, 2018	•••

Edit group

Alias group name: Security Cameras

Contains — Select from list

Camera 1 ×, Camera 2 ×, Camera 3 ×, Camera 4 ×, Camera 5 ×, Camera 6 ×, Camera 7 ×, Camera 8 ×, Camera 9 ×, Camera 10 ×, Reserved Video 1 ×, Reserved Video 2 ×, Reserved Video 3 ×, 172.29.0.0/16 ×, Camera 11 ×

☑ Auto-generate aliases from IPs — 13 entered

SUGGESTIONS

Delete | Cancel | Edit group

MX Network Objects

Compatibility

- **Network Object/Group Compatibility**
  - Network Objects can contain:
    - IP Address, IP Subnet (CIDR), FQDN or Wildcard FQDN.
  - Network Groups can contain:
    - one or more Network Objects.

- **Firewall Compatibility**
  - Network Objects/Groups can be applied to:
    - Individual & Template Networks: Layer 3 Inbound, Layer 3 Outbound and Failover Cellular Firewall Rules
    - Organization-wide Site to Site VPN Outbound Firewall Rules

MX Firmware 16

Latest stable release

NBAR2

AnyConnect

SD-WAN Over LTE

Smart Path Steering for DIA

IDS Snort 3.0

vMX on GCP

MX 17

Stable release candidate

CORE

- IPv6 MVP on MX

ANALYTICS

- NBAR2 Expansion

WAN INTELLIGENCE

- SD-Internet Top 10

SECURITY

- Inline Snort
- Brighter Skies
- Adaptive Policy

NBAR2 - Powerful App Recognition Engine !

From 200 up to 1500+ applications

Classifying all clients traffic by using NBAR engine

Part of MX-16

- Enhanced application visibility
- Aligned with full Meraki platform
- Replacing existing TA engine
- KB Link

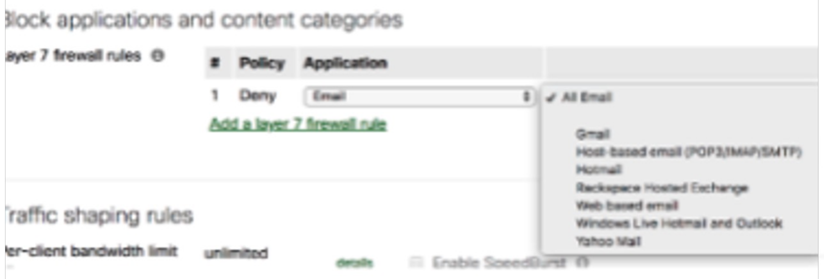
License :

ENT SEC SDW

Platform Supported :

All MX, Teleworker

Without NBAR



Block applications and content categories

Layer 7 firewall rules

#	Policy	Application
1	Deny	Email

Add a layer 7 firewall rule

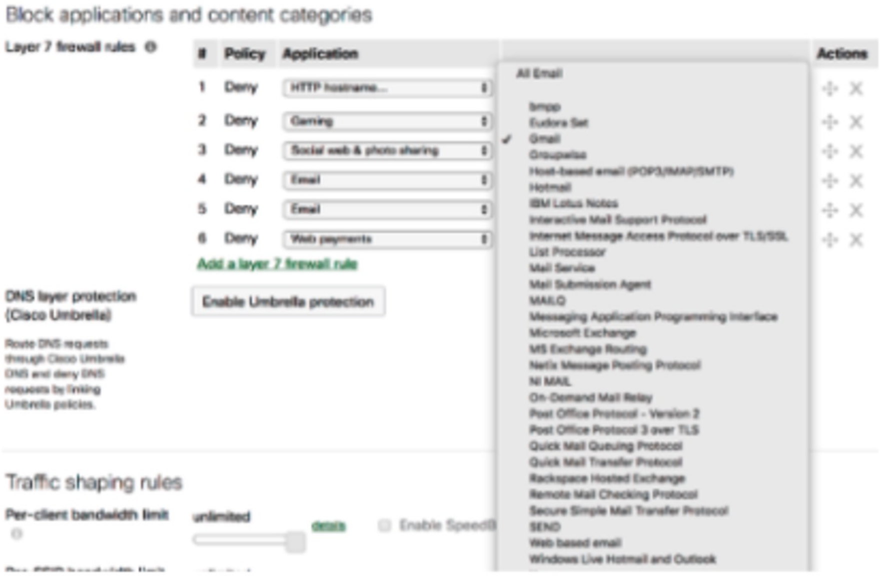
✓ All Email

Gmail
Host-based email (POP3/IMAP/SMTP)
Hotmail
Rackspace Hosted Exchange
Web based email
Windows Live Hotmail and Outlook
Yahoo Mail

Traffic shaping rules

Per-client bandwidth limit unlimited details □ Enable SpeedBurst

With NBAR



Block applications and content categories

Layer 7 firewall rules

#	Policy	Application	Actions
1	Deny	HTTP hostname...	✥ ✕
2	Deny	Gaming	✥ ✕
3	Deny	Social web & photo sharing	✥ ✕
4	Deny	Email	✥ ✕
5	Deny	Email	✥ ✕
6	Deny	Web payments	✥ ✕

Add a layer 7 firewall rule

All Email

bmpp
Eudora Set
✓ Gmail
Groupwise
Host-based email (POP3/IMAP/SMTP)
Hotmail
IBM Lotus Notes
Interactive Mail Support Protocol
Internet Message Access Protocol over TLS/SSL
List Processor
Mail Service
Mail Submission Agent
MAILO
Messaging Application Programming Interface
Microsoft Exchange
MS Exchange Routing
Netix Message Posting Protocol
NI MAIL
On-Demand Mail Relay
Post Office Protocol - Version 2
Post Office Protocol 3 over TLS
Quick Mail Queuing Protocol
Quick Mail Transfer Protocol
Rackspace Hosted Exchange
Remote Mail Checking Protocol
Secure Simple Mail Transfer Protocol
SEND
Web based email
Windows Live Hotmail and Outlook

DNS layer protection (Cisco Umbrella)

Enable Umbrella protection

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

Traffic shaping rules

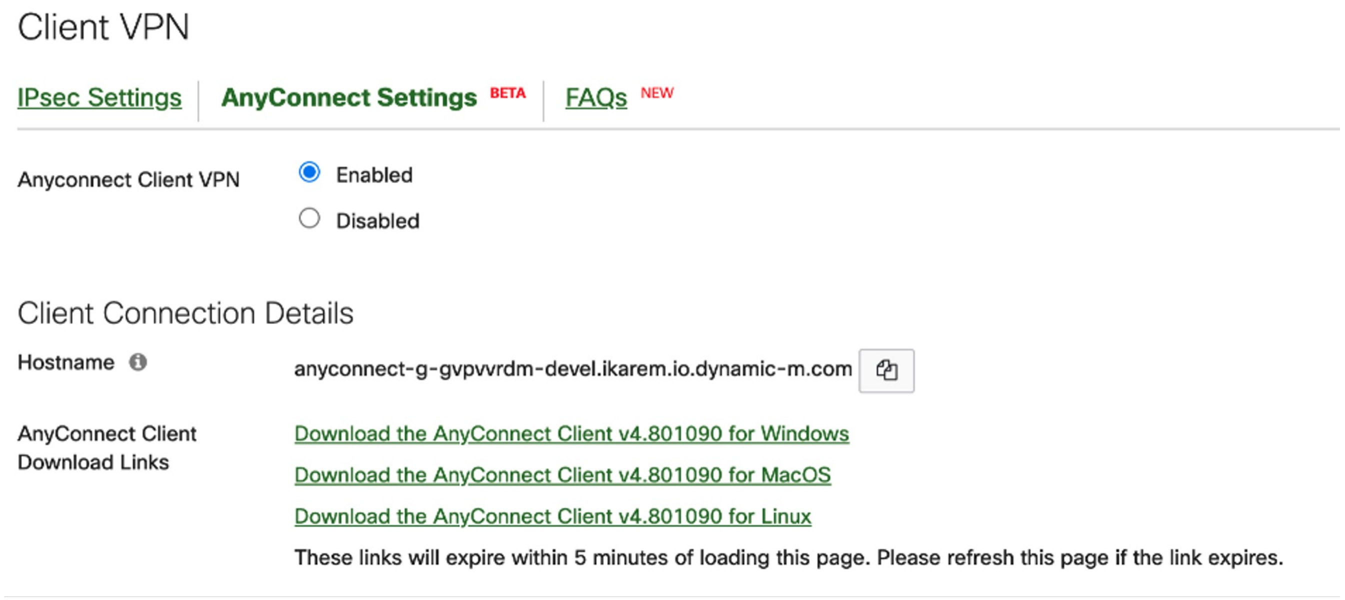
Per-client bandwidth limit unlimited details □ Enable SpeedB

AnyConnect - Client VPN

Remote access simplified with the Cisco AnyConnect Client

Benefits

- Mainstream VPN Client Support
- TLS VPN support
- Per user policy with RADIUS Filter-ID
- Certificate based authentication
- Split tunneling support
- Easy Client deployment and configuration with MDM
- Automatic public certificate enrollment and renewal with Meraki DDNS hostname



Client VPN

IPsec Settings | AnyConnect Settings BETA | FAQs NEW

Anyconnect Client VPN ● Enabled ○ Disabled

Client Connection Details

Hostname: anyconnect-g-gvpvvrdm-devel.ikarem.io.dynamic-m.com

AnyConnect Client Download Links:

Download the AnyConnect Client v4.801090 for Windows

Download the AnyConnect Client v4.801090 for MacOS

Download the AnyConnect Client v4.801090 for Linux

These links will expire within 5 minutes of loading this page. Please refresh this page if the link expires.

Smart Path Steering for DIA

Enhance SaaS QoE with Direct Internet Access optimization

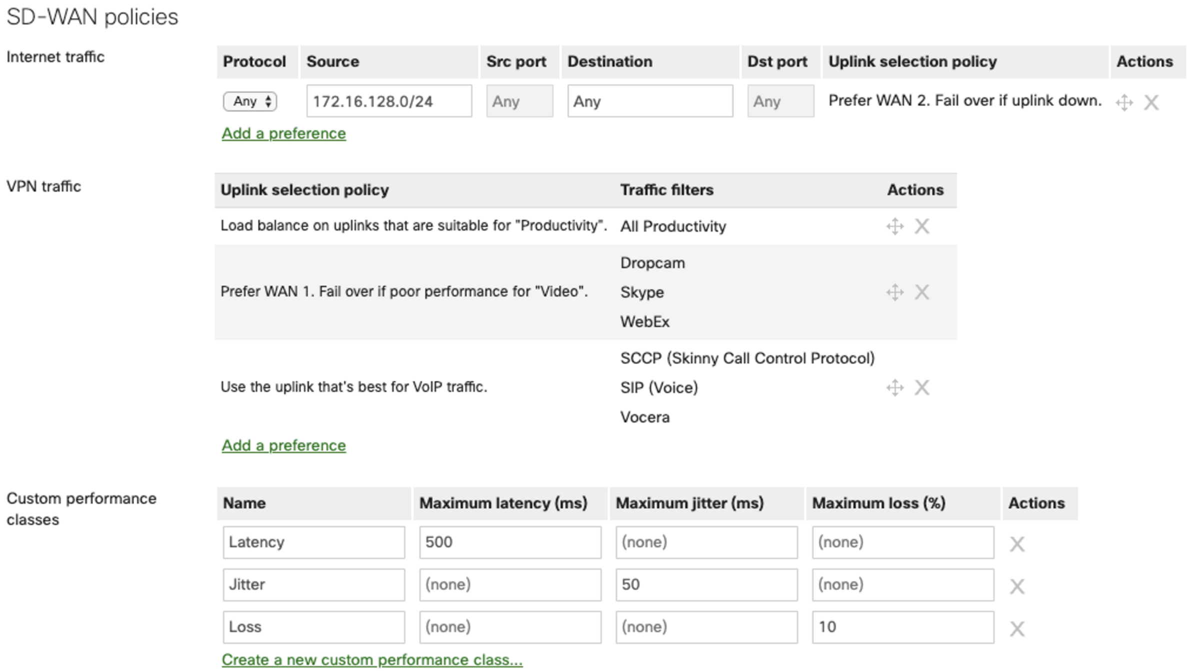
- Empowers customers to handle Internet brownouts
- Customers can now apply the SD-WAN performance classes to L3/L4 traffic that's Internet-bound
- Performance is evaluated based on the uplink's performance

License :

SDW

Platform Supported :

All MX



SD-WAN policies

Internet traffic

Protocol	Source	Src port	Destination	Dst port	Uplink selection policy	Actions
Any	172.16.128.0/24	Any	Any	Any	Prefer WAN 2. Fail over if uplink down.	✥ ✕

Add a preference

VPN traffic

Uplink selection policy	Traffic filters	Actions
Load balance on uplinks that are suitable for "Productivity".	All Productivity	✥ ✕
Prefer WAN 1. Fail over if poor performance for "Video".	Dropcam Skype WebEx	✥ ✕
Use the uplink that's best for VoIP traffic.	SCCP (Skinny Call Control Protocol) SIP (Voice) Vocera	✥ ✕

Add a preference

Custom performance classes

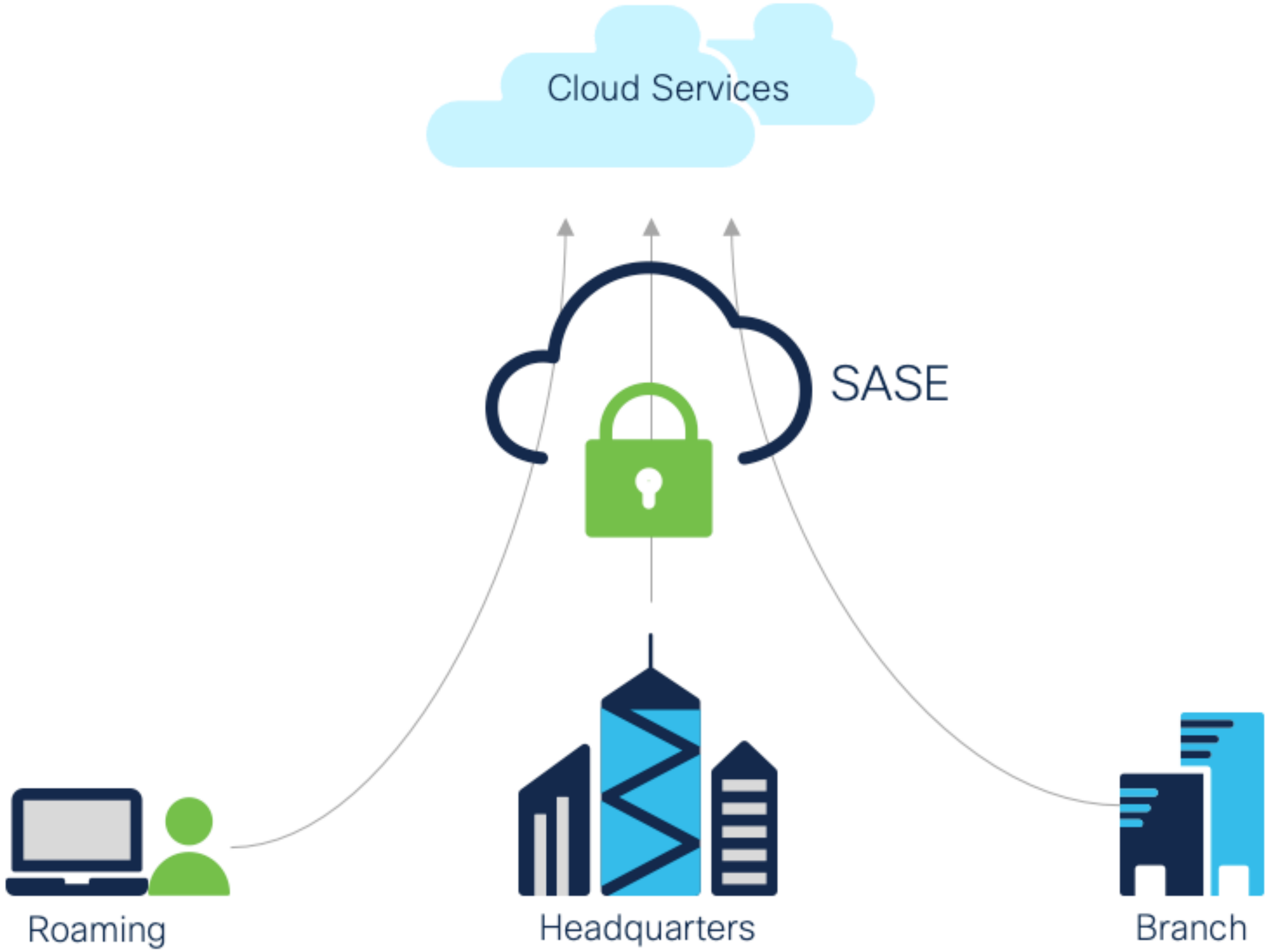
Name	Maximum latency (ms)	Maximum jitter (ms)	Maximum loss (%)	Actions
Latency	500	(none)	(none)	✕
Jitter	(none)	50	(none)	✕
Loss	(none)	(none)	10	✕

Create a new custom performance class...

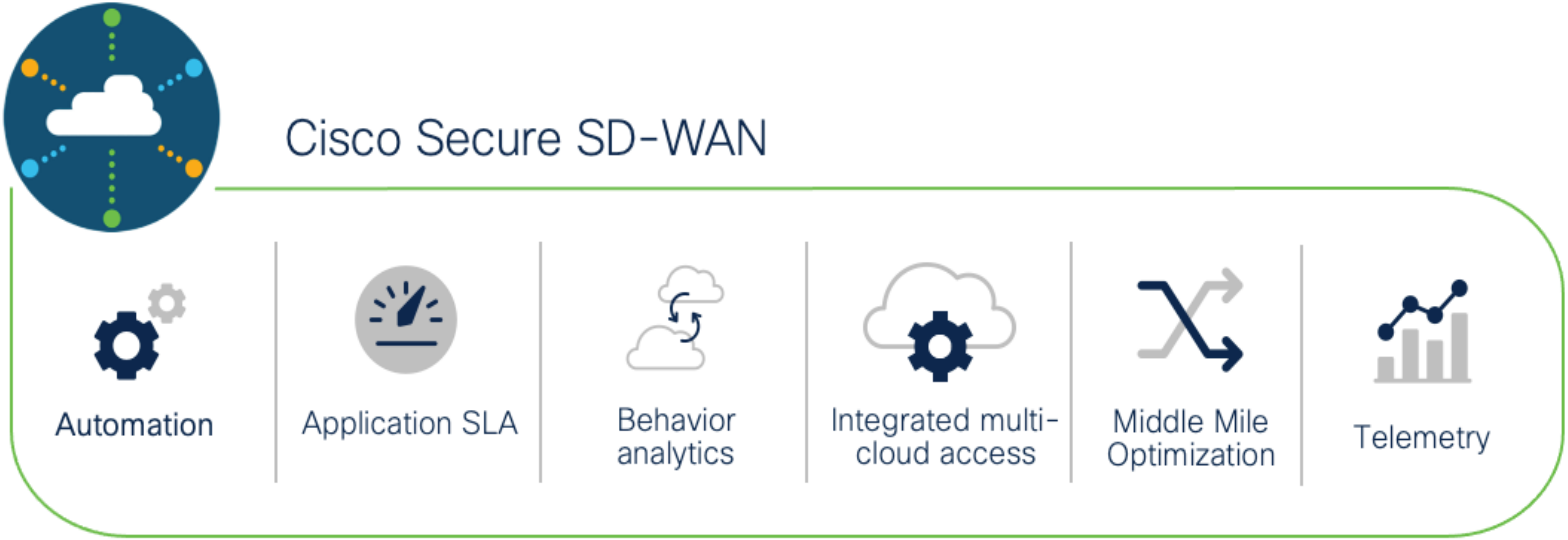
IPv6 on MX17

- MX 17.5+ firmware is required for IPv6 functionality on MX Security & SD-WAN Platforms.
- This is part of Meraki's ongoing, cross-product initiative to support IPv6.
- Supported models: Z3, Z3C, MX64, MX64W, MX65, MX65W, MX67, MX67W, MX67C, MX68, MX68W, MX68CW, MX75, MX84, MX85, MX95, MX100, MX105, MX250, MX450.
- See this link for a list of updated Meraki products that support IPv6 and to what degree.

Secure Access Service Edge (SASE)



Meraki SD-WAN



Cisco Secure SD-WAN

Automation

Application SLA

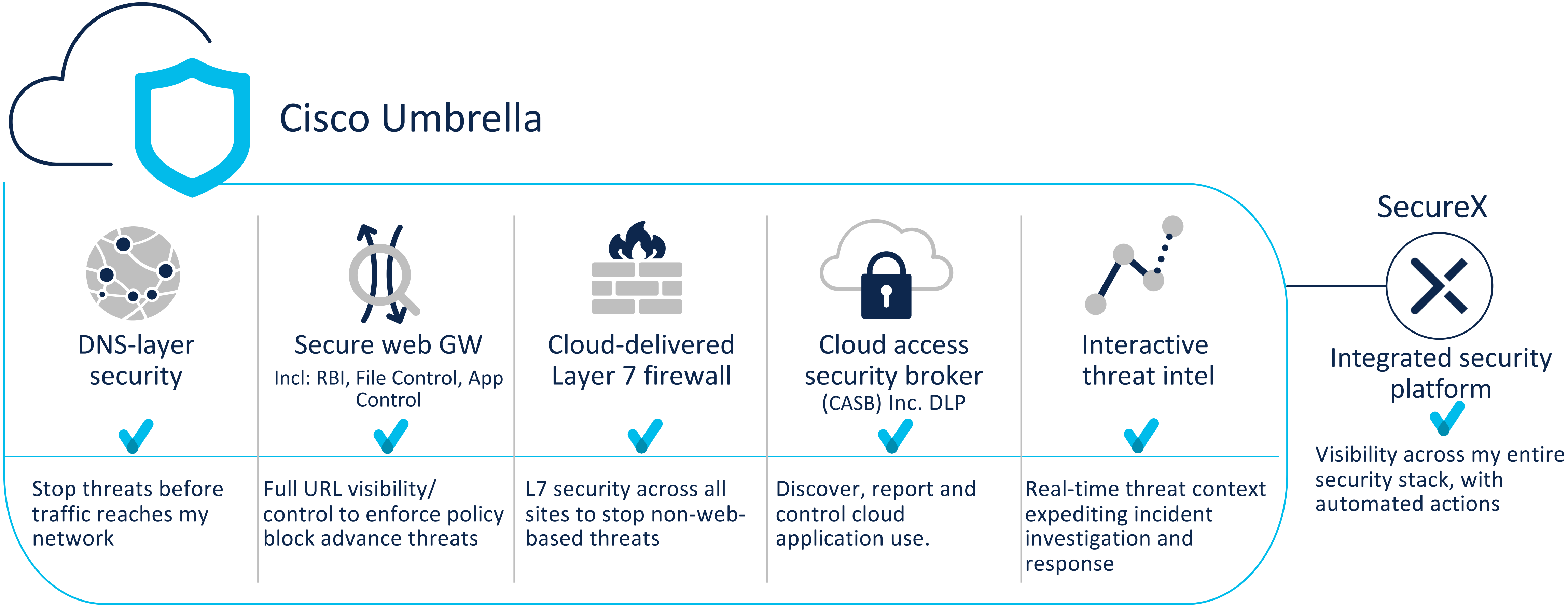
Behavior analytics

Integrated multi-cloud access

Middle Mile Optimization

Telemetry

SASE cloud security capabilities / SIG



Cisco Umbrella

DNS-layer security

✓

Stop threats before traffic reaches my network

Secure web GW

Incl: RBI, File Control, App Control

✓

Full URL visibility/ control to enforce policy block advance threats

Cloud-delivered Layer 7 firewall

✓

L7 security across all sites to stop non-web-based threats

Cloud access security broker (CASB) Inc. DLP

✓

Discover, report and control cloud application use.

Interactive threat intel

✓

Real-time threat context expediting incident investigation and response

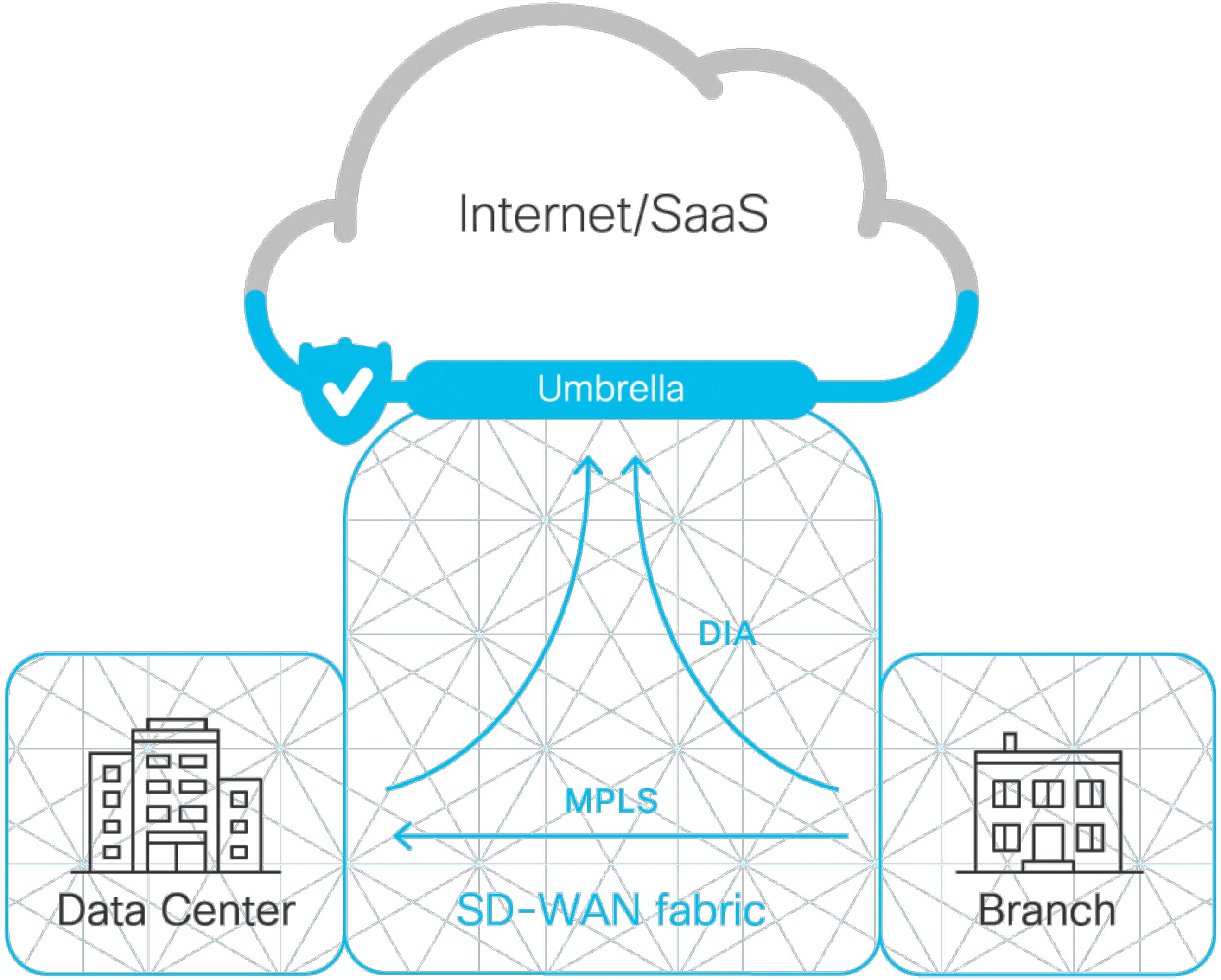
SecureX

Integrated security platform

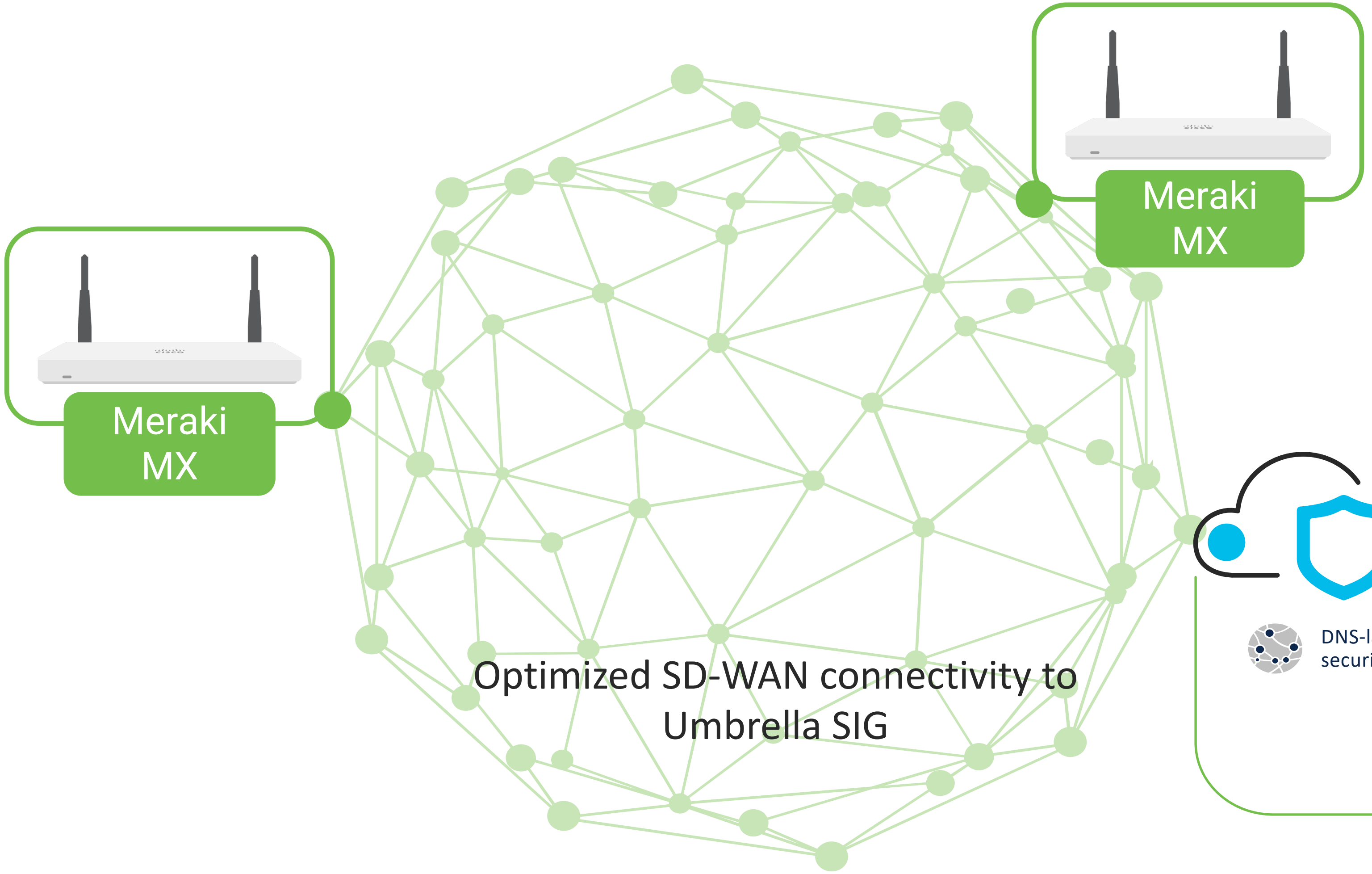
✓

Visibility across my entire security stack, with automated actions

Meraki / Umbrella SIG Integration



Best-in-Class & Seamless SASE Security / SIGRAKI



Optimized SD-WAN connectivity to Umbrella SIG

Simple and Fast Deployment

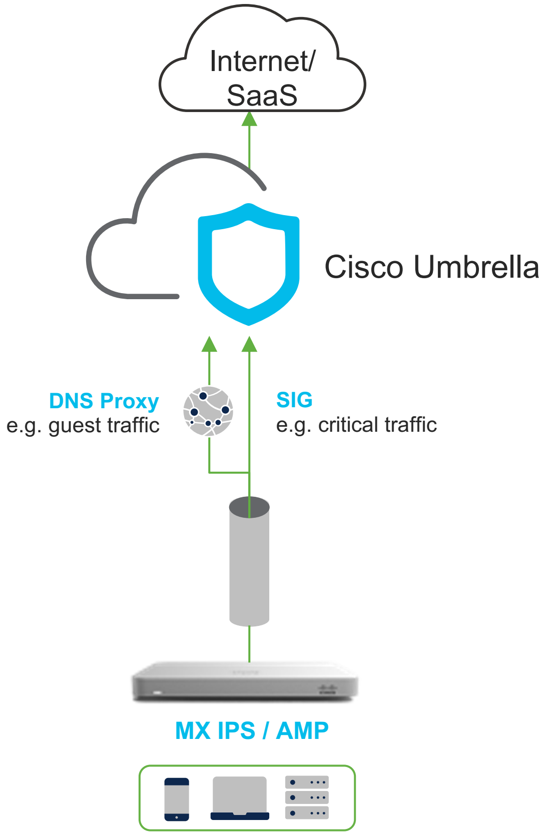
- Users can create an Auto VPN tunnel in just three clicks
- Umbrella policies can be automatically applied
- New sites inherit default policies

Cisco Umbrella

- DNS-layer security
- Secure web gateway
- Cloud-delivered firewall
- Cloud access security broker (CASB)
- Data loss prevention
- Remote browser Isolation
- Interactive threat intel

Meraki MX and Umbrella **Integration Options**

Phase 1
Meraki dashboard and user interface
simplify tunnel creation



Internet/
SaaS

Cisco Umbrella

DNS Proxy
e.g. guest traffic

SIG
e.g. critical traffic

MX IPS / AMP

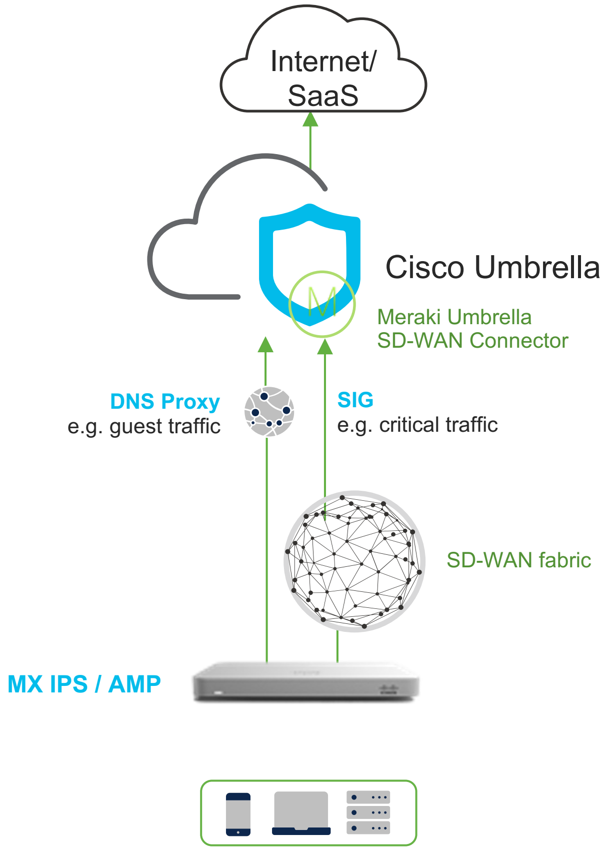
IPsec Tunnel Connectivity

Choose per site

SASE your way

Competitive Differentiator

Phase 2
Auto VPN extends Meraki's SD-WAN fabric
into the Umbrella cloud



Internet/
SaaS

Cisco Umbrella

Meraki Umbrella
SD-WAN Connector

DNS Proxy
e.g. guest traffic

SIG
e.g. critical traffic

SD-WAN fabric

MX IPS / AMP

SD-WAN Fabric Integration

Cisco+ Secure Connect Now

Radically simple, unified SASE turnkey solution

Simple

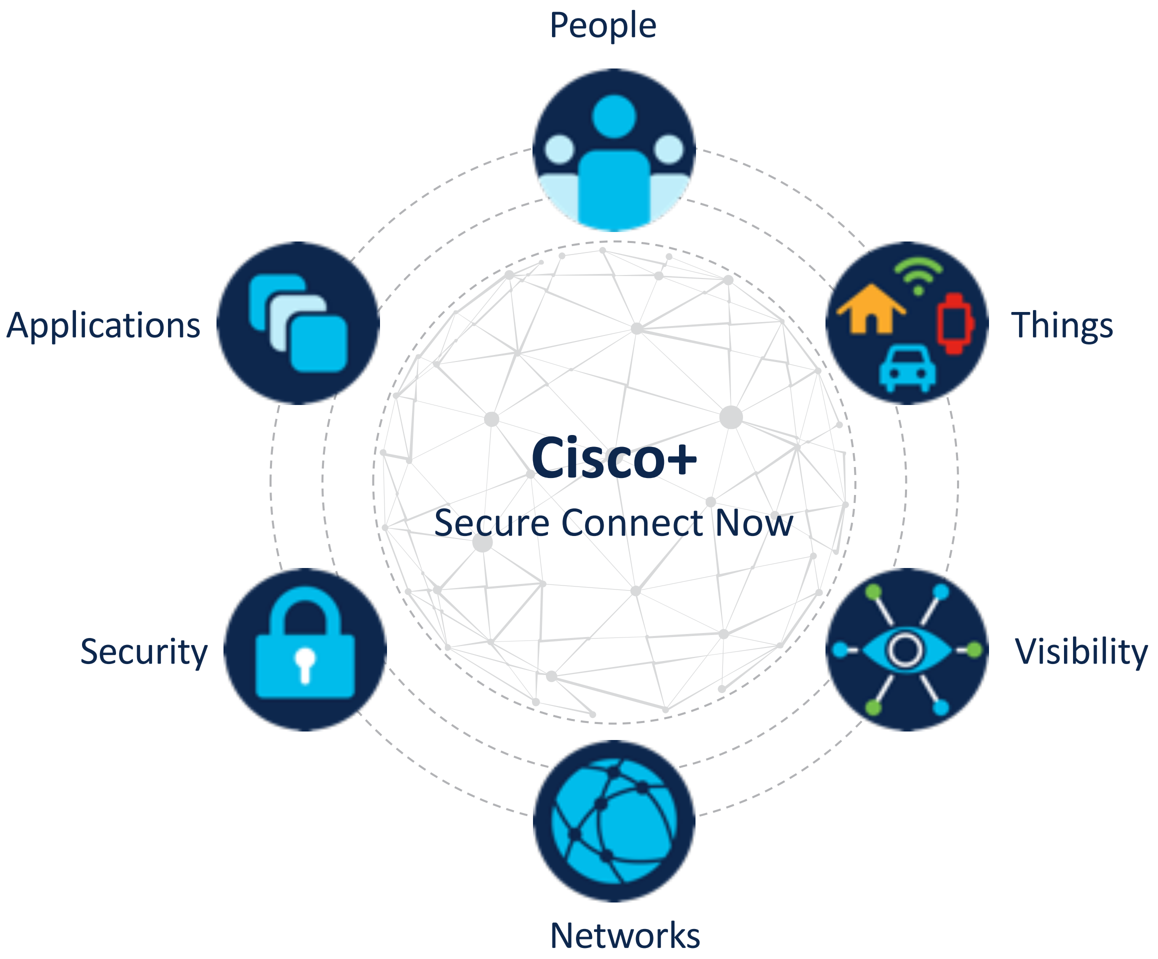
Increase business agility through an easy to consume and use as-a-service subscription that is cost-effective

Secure

Protect across every point of service - user, device, application - enforcing security closest to threats

Intelligent

Deliver actionable insights end-to-end, to predict, understand, and remediate the application experience



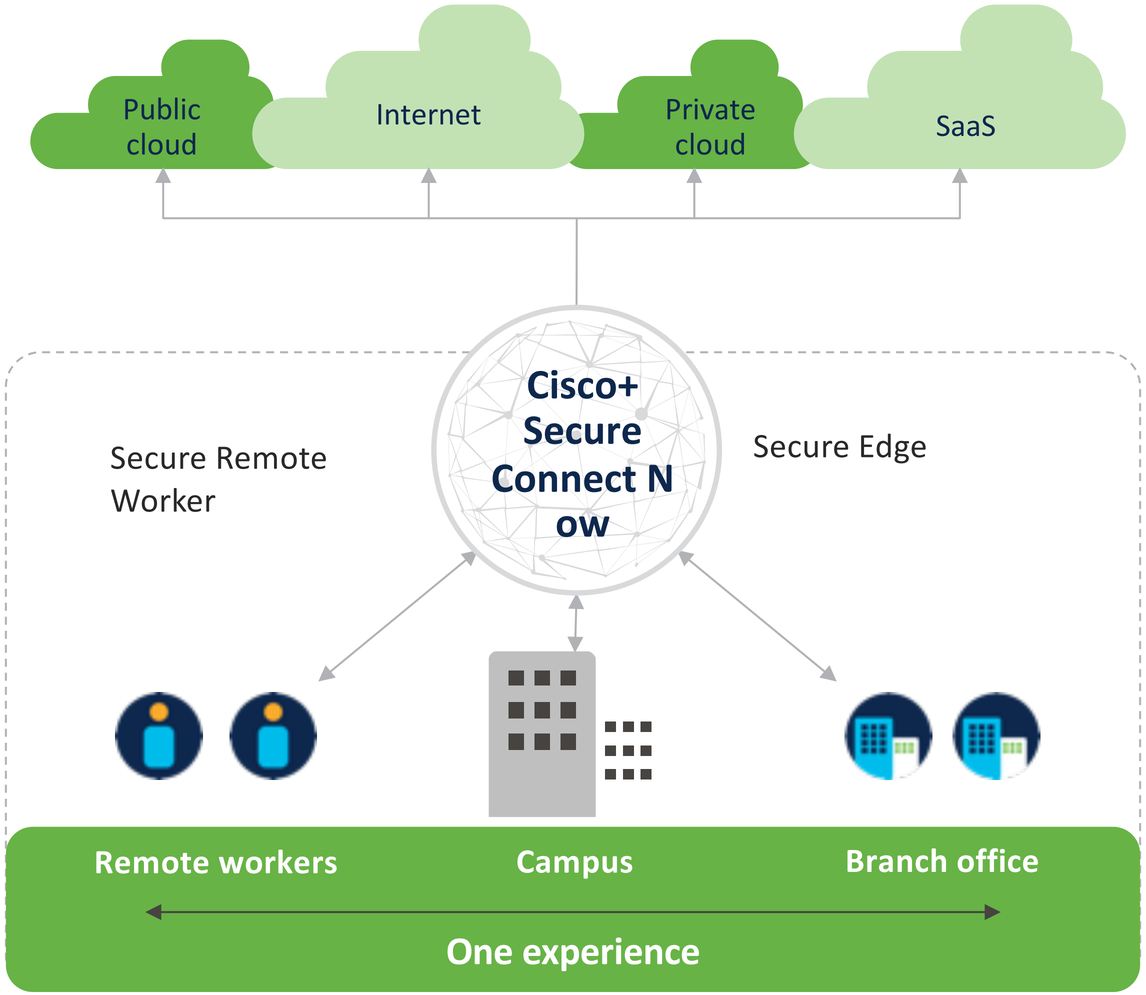
Built for Speed and Simplicity

Major SASE use cases

Secure internet access
Provide users with safe access to the internet and cloud applications from any location and block malicious activity
and threats

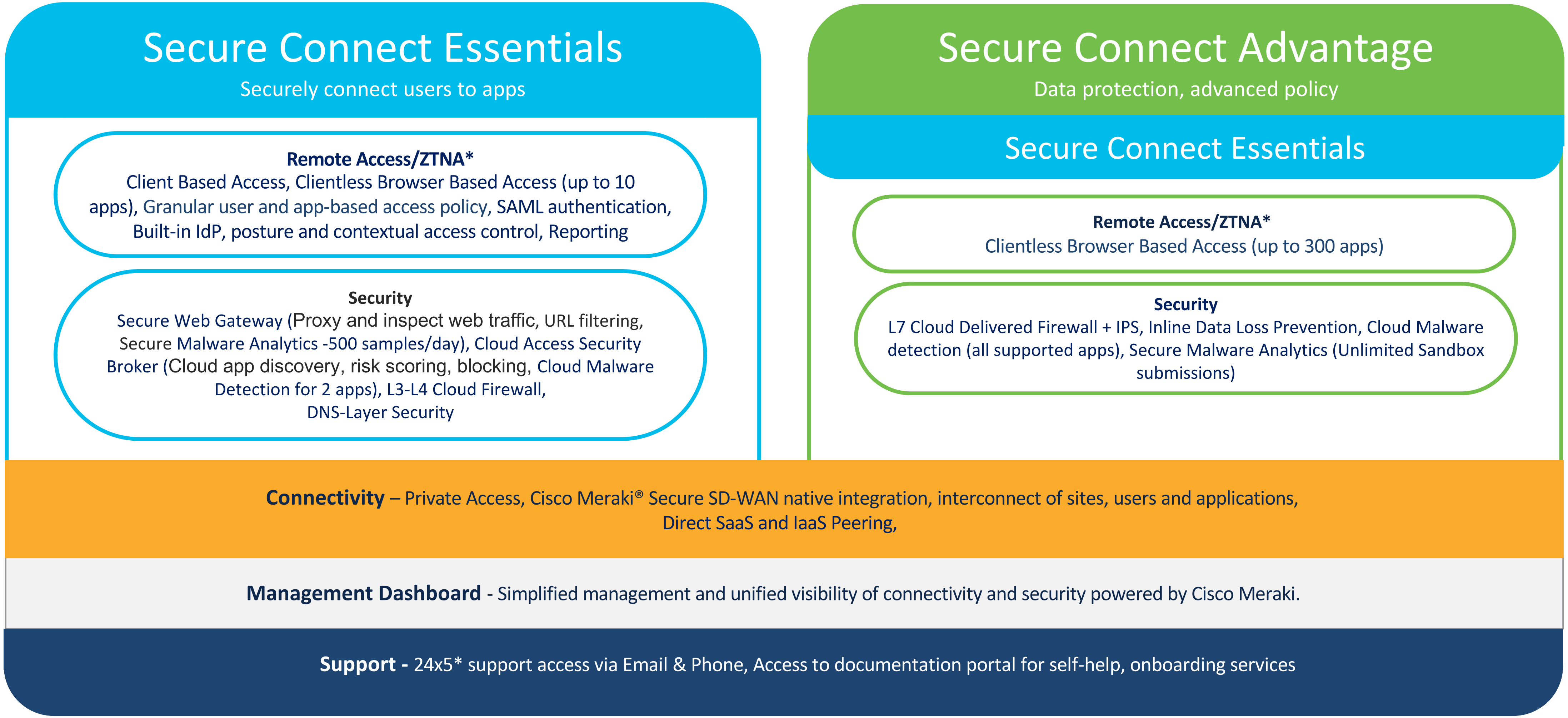
Secure private access
Deliver secure connections to company assets in private data centers or in the private cloud.

Interconnect
Dramatically simplify architecture and configuration by inherently interconnecting anything you connect to the SASE Fabric



Cisco+ Secure Connect

Subscription Tier Capabilities



Secure Connect Essentials

Securely connect users to apps

Remote Access/ZTNA*
Client Based Access, Clientless Browser Based Access (up to 10 apps), Granular user and app-based access policy, SAML authentication, Built-in IdP, posture and contextual access control, Reporting

Security
Secure Web Gateway (Proxy and inspect web traffic, URL filtering, Secure Malware Analytics -500 samples/day), Cloud Access Security Broker (Cloud app discovery, risk scoring, blocking, Cloud Malware Detection for 2 apps), L3-L4 Cloud Firewall, DNS-Layer Security

Secure Connect Advantage

Data protection, advanced policy

Secure Connect Essentials

Remote Access/ZTNA*
Clientless Browser Based Access (up to 300 apps)

Security
L7 Cloud Delivered Firewall + IPS, Inline Data Loss Prevention, Cloud Malware detection (all supported apps), Secure Malware Analytics (Unlimited Sandbox submissions)

Connectivity – Private Access, Cisco Meraki® Secure SD-WAN native integration, interconnect of sites, users and applications, Direct SaaS and IaaS Peering,

Management Dashboard - Simplified management and unified visibility of connectivity and security powered by Cisco Meraki.

Support - 24x5* support access via Email & Phone, Access to documentation portal for self-help, onboarding services

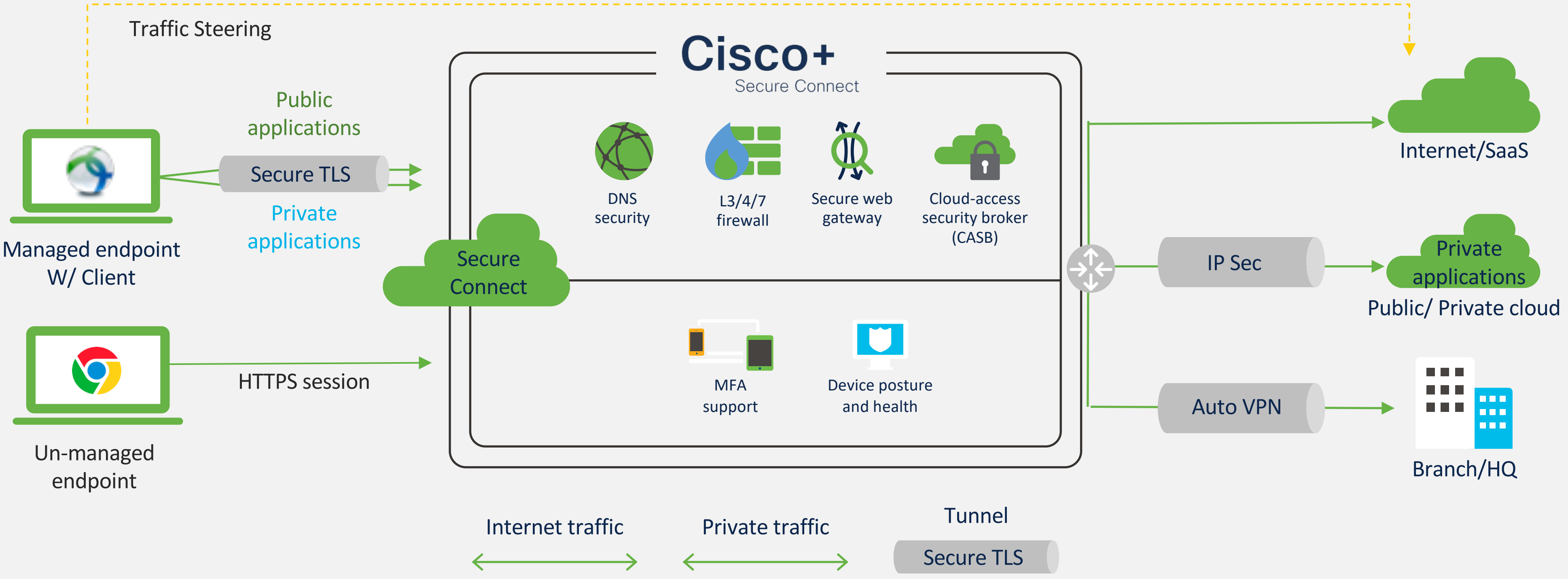
Note: Check Cisco+ Secure Connect Offer Description HERE for user terms
*Part of July 2022 release.

Cisco+ Secure Connect Now

Secure Remote Worker

Core elements

- Internet/SaaS
  - Cloud security (SIG)
- Meraki® IdP (identity provider)
- Private access
  - Client and clientless access
  - Device posture
  - SAML MFA
  - Access control

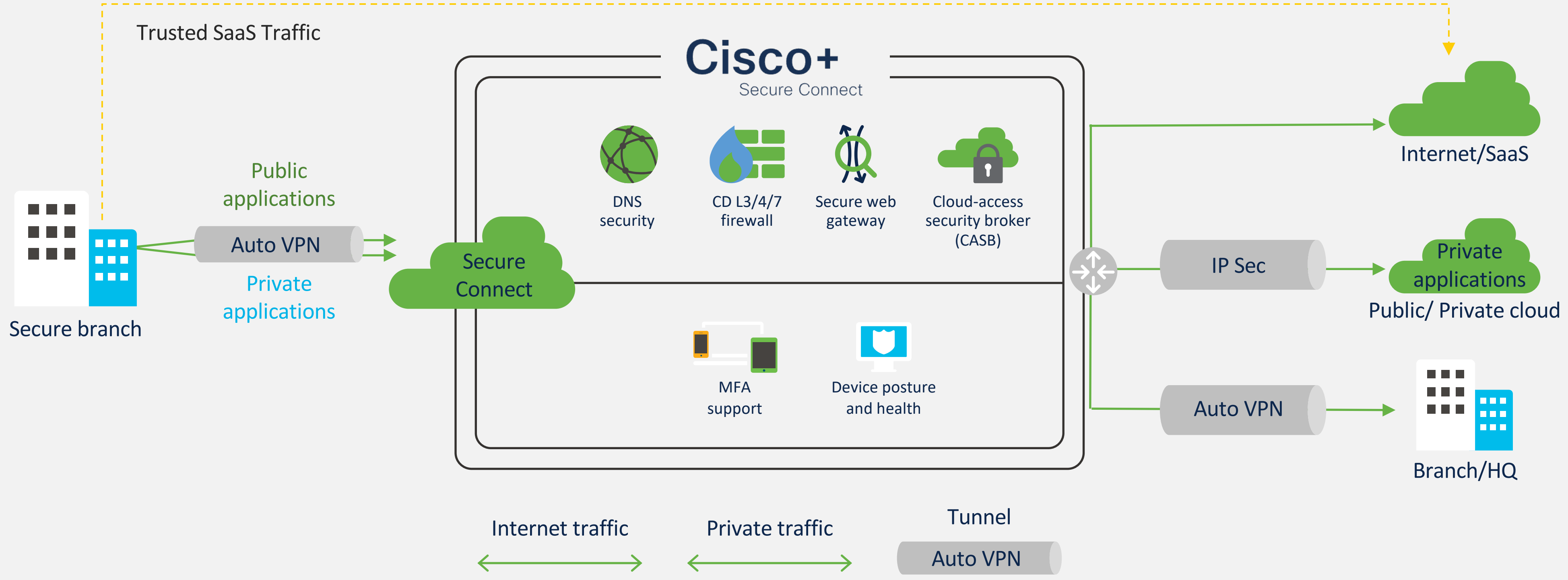


Cisco+ Secure Connect Now

Secure Branch Connectivity

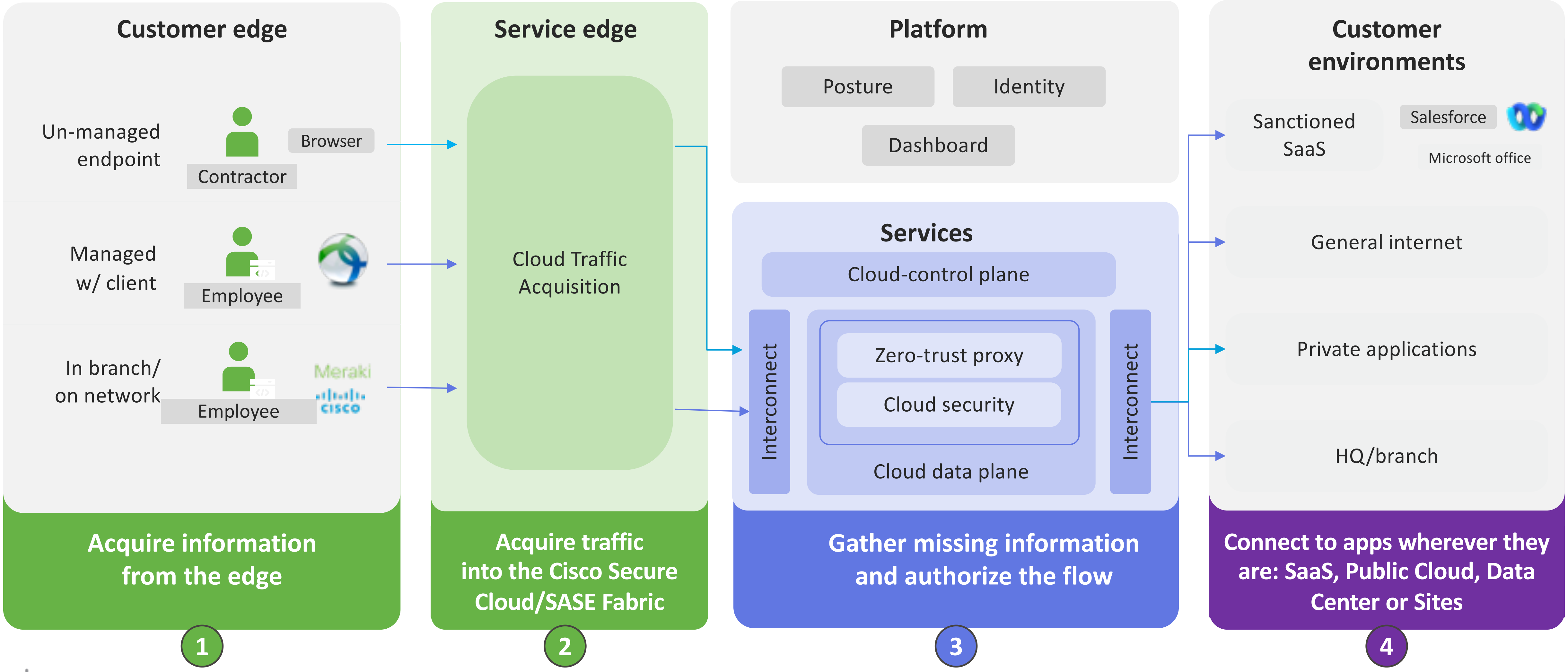
Core elements

- Internet/SaaS
  - Cloud security (SIG)
- Private application access
- Branch to Branch through Secure Connect fabric



Cisco+ Secure Connect Now

High-level architecture



Customer edge

Un-managed endpoint

Contractor

Browser

Managed w/ client

Employee

In branch/ on network

Employee

Meraki

cisco

Acquire information from the edge

1

Service edge

Cloud Traffic Acquisition

Acquire traffic into the Cisco Secure Cloud/SASE Fabric

2

Platform

Posture

Identity

Dashboard

Services

Cloud-control plane

Interconnect

Zero-trust proxy

Cloud security

Cloud data plane

Interconnect

Gather missing information and authorize the flow

3

Customer environments

Sanctioned SaaS

Salesforce

Microsoft office

General internet

Private applications

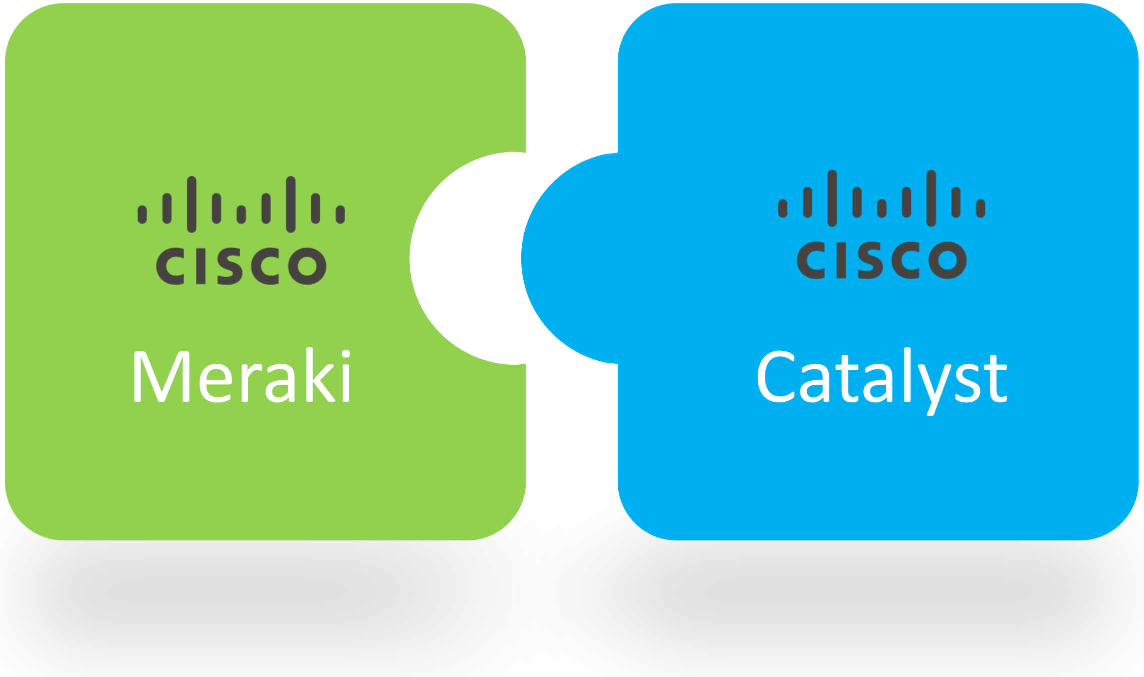
HQ/branch

Connect to apps wherever they are: SaaS, Public Cloud, Data Center or Sites

4

Cloud Monitoring for Catalyst Access

#1 in cloud managed networks



Meraki

Catalyst

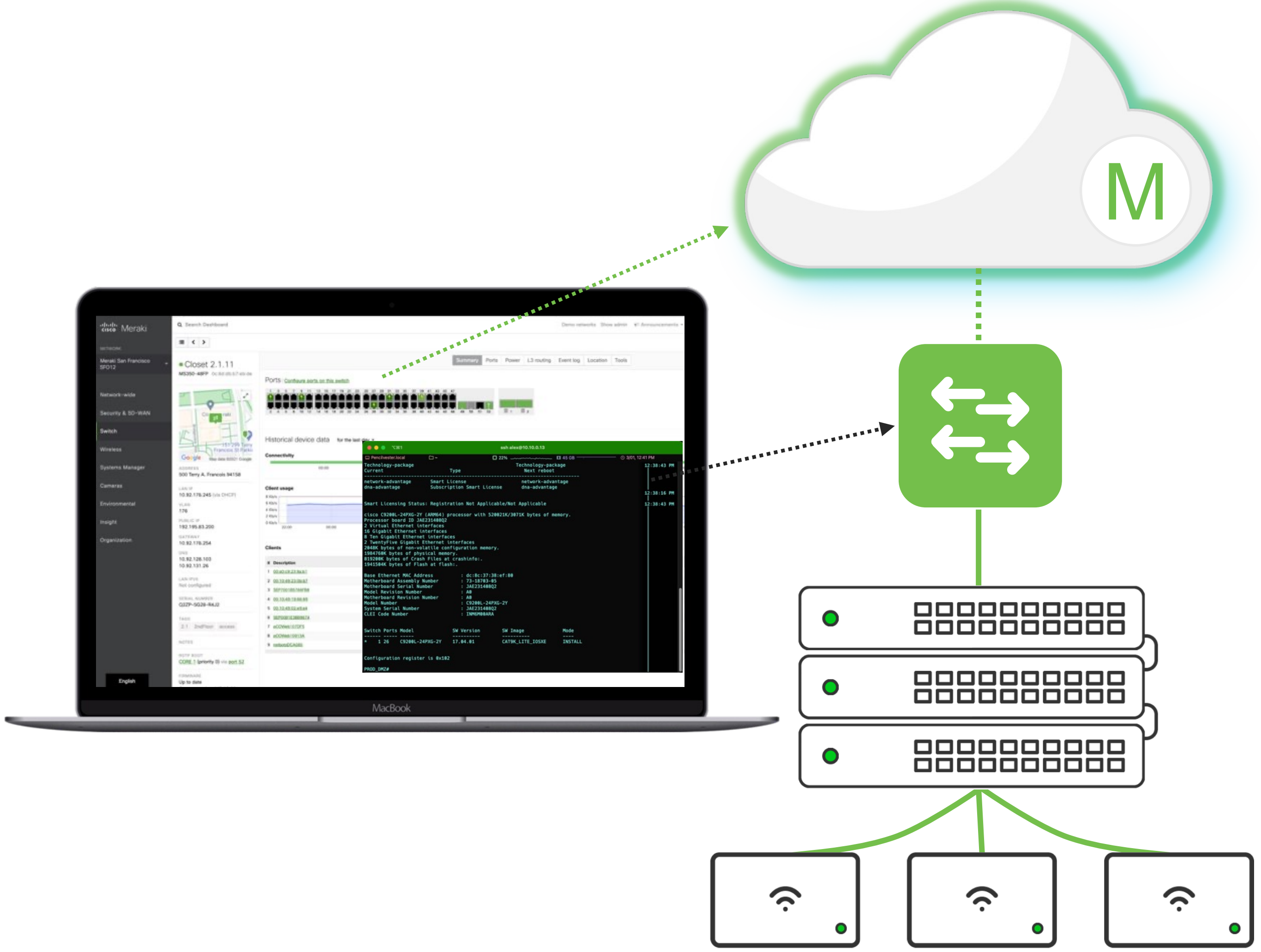
#1 in networking

Cloud Monitoring for Catalyst

Unified view of Cisco network infrastructure

Device health and troubleshooting

Network client and traffic information



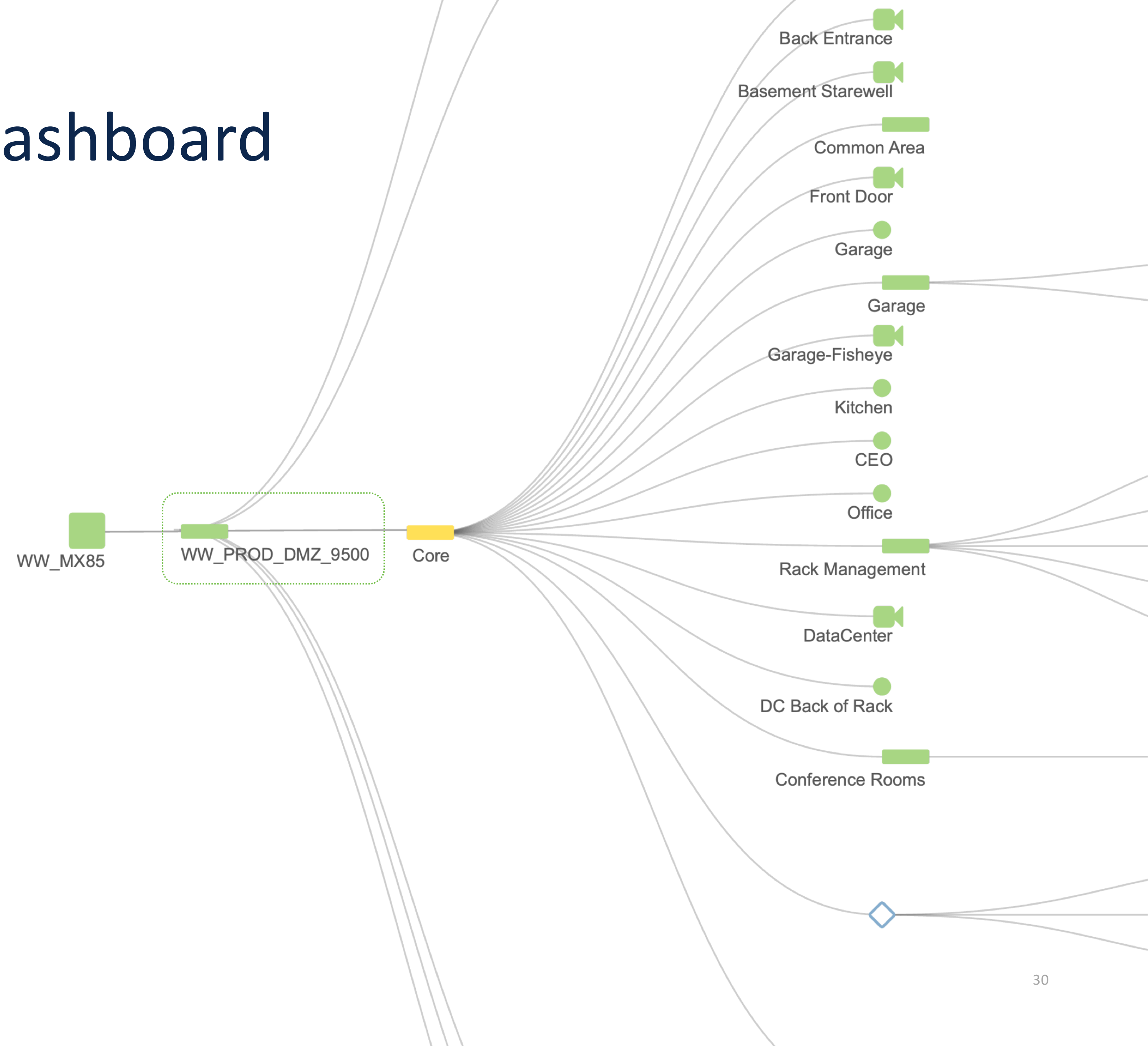
```
Technology-package                           Technology-package
Current                  Type                Next reboot
--------------------------------------------------------------------
network-advantage        Smart License       network-advantage
dna-advantage            Subscription Smart License  dna-advantage


Smart Licensing Status: Registration Not Applicable/Not Applicable

cisco C9200L-24PXG-2Y (ARM64) processor with 520021K/3071K bytes of memory.
Processor board ID JAE23140BQ2
2 Virtual Ethernet interfaces
16 Gigabit Ethernet interfaces
8 Ten Gigabit Ethernet interfaces
2 TwentyFive Gigabit Ethernet interfaces
2048K bytes of non-volatile configuration memory.
1984760K bytes of physical memory.
819200K bytes of Crash Files at crashinfo:.
1941504K bytes of Flash at flash:.

Base Ethernet MAC Address          : dc:8c:37:38:ef:80
Motherboard Assembly Number        : 73-18703-05
Motherboard Serial Number          : JAE23140BQ2
Model Revision Number              : A0
Motherboard Revision Number        : A0
Model Number                       : C9200L-24PXG-2Y
System Serial Number               : JAE23140BQ2
CLEI Code Number                   : INM6M00ARA


Switch Ports Model              SW Version        SW Image              Mode
------ ----- -----              ----------        ----------            ----
*    1 26    C9200L-24PXG-2Y    17.04.01          CAT9K_LITE_IOSXE      INSTALL


Configuration register is 0x102

PROD_DMZ#
```

One Network, One Dashboard

Consolidated Device Inventory

Centralized monitoring of IOS and Meraki devices

Unified topology view

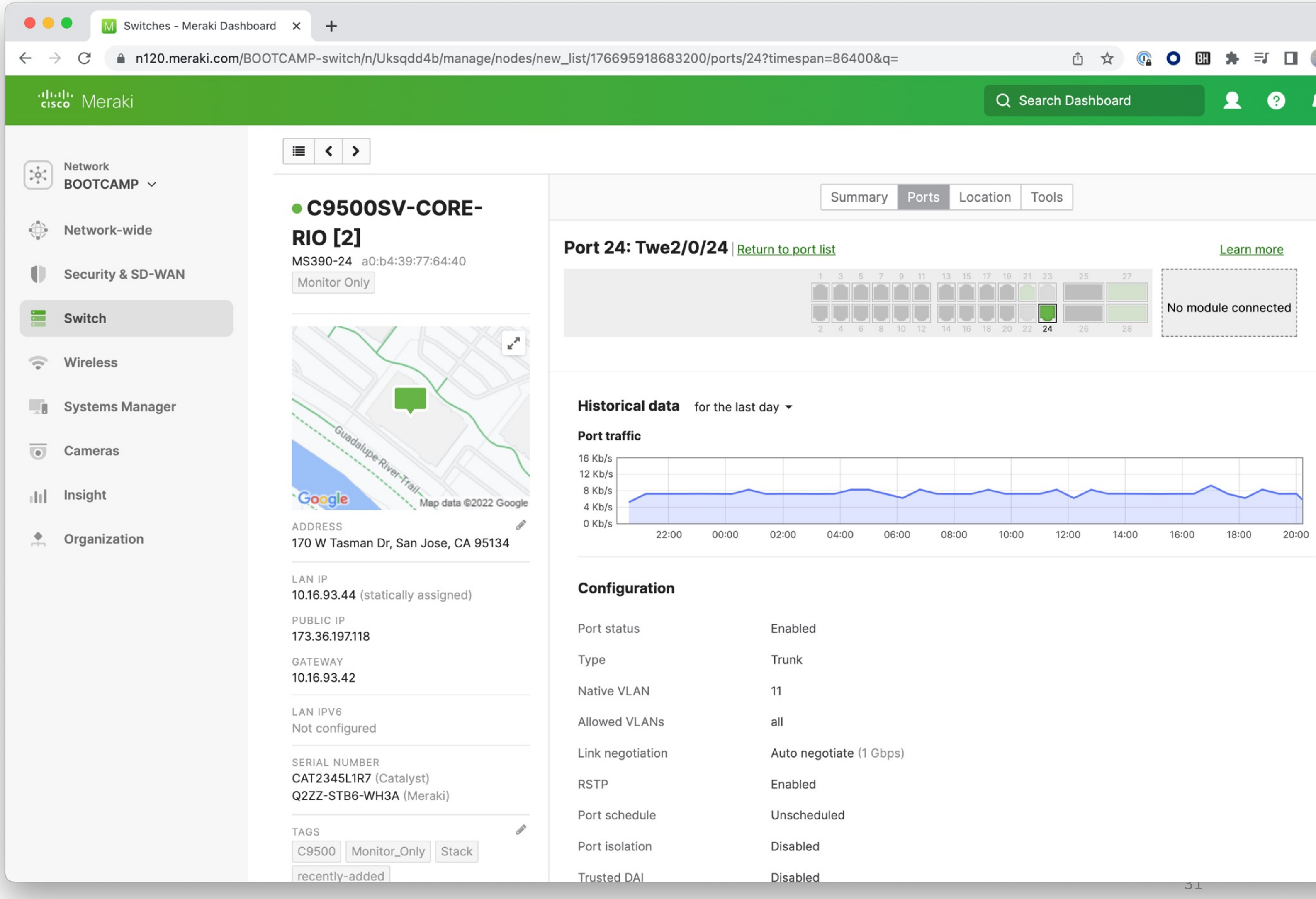


Keep Your Network Healthy

In-Dashboard alerts for switch or port issues

Port-level packet and error counters

Remote troubleshooting and diagnostics tools



C9500SV-CORE-RIO [2]

MS390-24 a0:b4:39:77:64:40

Monitor Only

ADDRESS
170 W Tasman Dr, San Jose, CA 95134

LAN IP
10.16.93.44 (statically assigned)

PUBLIC IP
173.36.197.118

GATEWAY
10.16.93.42

LAN IPV6
Not configured

SERIAL NUMBER
CAT2345L1R7 (Catalyst)
Q2ZZ-STB6-WH3A (Meraki)

TAGS
C9500 Monitor_Only Stack recently-added

Port 24: Twe2/0/24

Historical data for the last day

Port traffic

Configuration

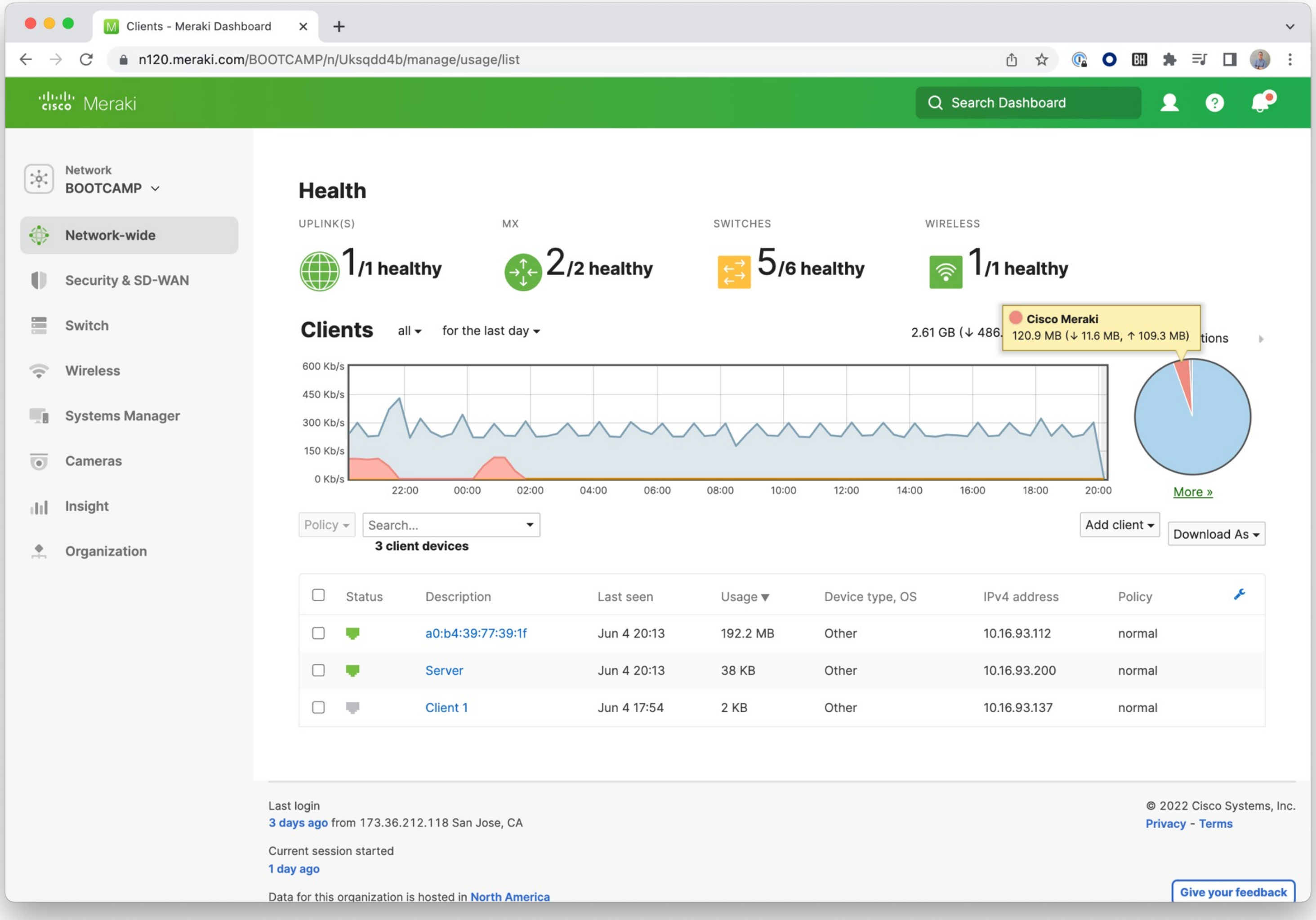
Port status	Enabled
Type	Trunk
Native VLAN	11
Allowed VLANs	all
Link negotiation	Auto negotiate (1 Gbps)
RSTP	Enabled
Port schedule	Unscheduled
Port isolation	Disabled
Trusted DAI	Disabled

Know What’s Happening With Your Users

See connected devices across your network

Detailed network usage and traffic statistics

Application visibility into network traffic



Health

UPLINK(S) 1/1 healthy

MX 2/2 healthy

SWITCHES 5/6 healthy

WIRELESS 1/1 healthy

Clients all for the last day

2.61 GB (↓ 486. … tions

Cisco Meraki
120.9 MB (↓ 11.6 MB, ↑ 109.3 MB)

3 client devices

☐	Status	Description	Last seen	Usage ▾	Device type, OS	IPv4 address	Policy
☐	🟩	a0:b4:39:77:39:1f	Jun 4 20:13	192.2 MB	Other	10.16.93.112	normal
☐	🟩	Server	Jun 4 20:13	38 KB	Other	10.16.93.200	normal
☐	▨	Client 1	Jun 4 17:54	2 KB	Other	10.16.93.137	normal

Last login
3 days ago from 173.36.212.118 San Jose, CA

Current session started
1 day ago

Data for this organization is hosted in North America

© 2022 Cisco Systems, Inc.
Privacy - Terms

Give your feedback

Cloud Monitoring Capabilities

Centralized view of the entire network

Visibility of Cisco devices whether Meraki or Catalyst switches from one Dashboard

Real time switch and port health

Monitor Catalyst connectivity and health from the Dashboard

Remote monitoring

Powerful live troubleshooting tools for identifying and correcting issues, even from thousands of miles away

App visibility

Make it easy to understand how valuable network resources are being used. *(DNA Advantage License required for full feature set)*

Network topology

Monitor devices and their connections in a unified dynamically generated topology diagram

Supported Platforms and Software

Models

Catalyst
9200/L
9300/L/X
9500

Firmware

IOS-XE 17.3+

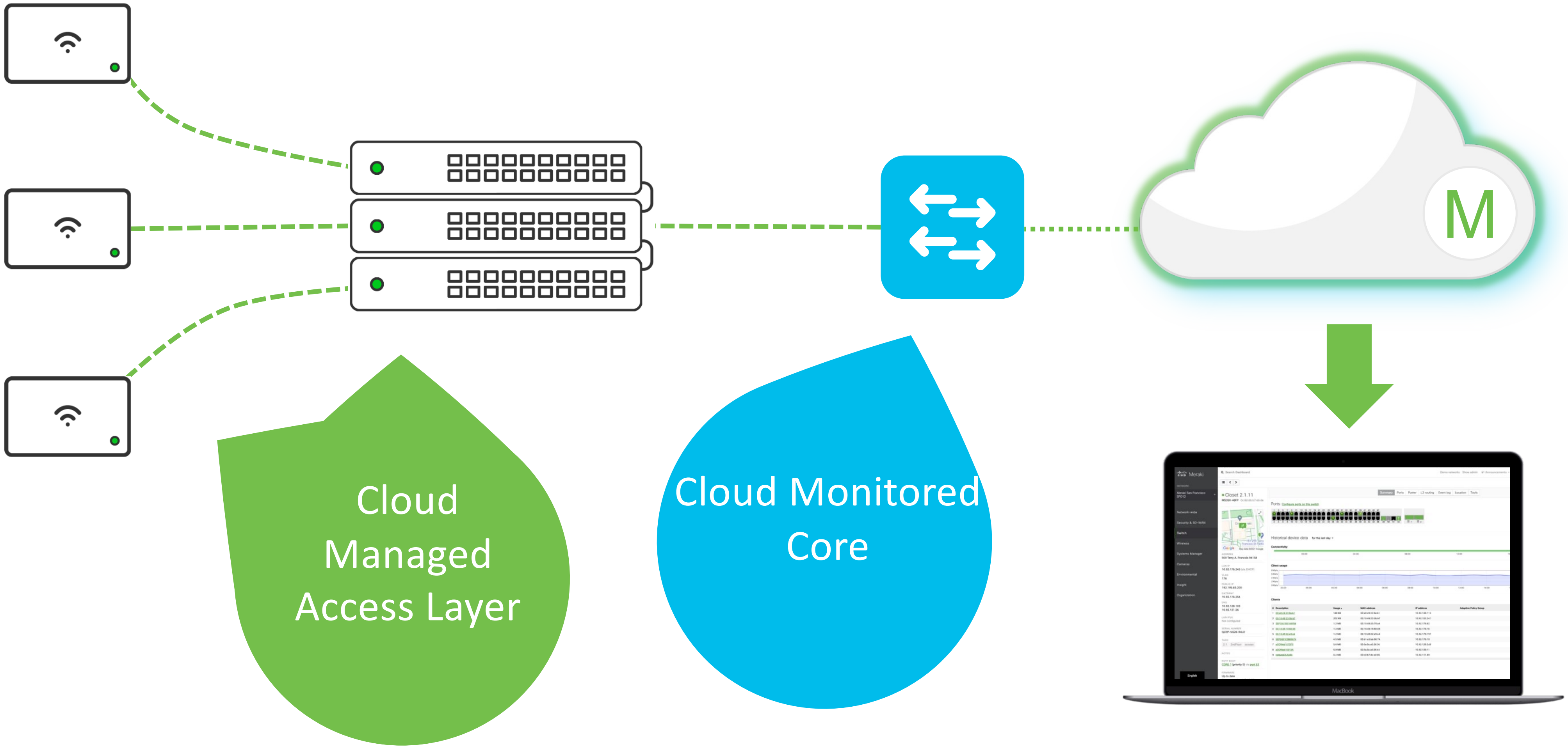
Licensing

DNA Advantage
DNA Essentials*

* DNA Essentials will not provide application or usage data

Architecture Use Cases

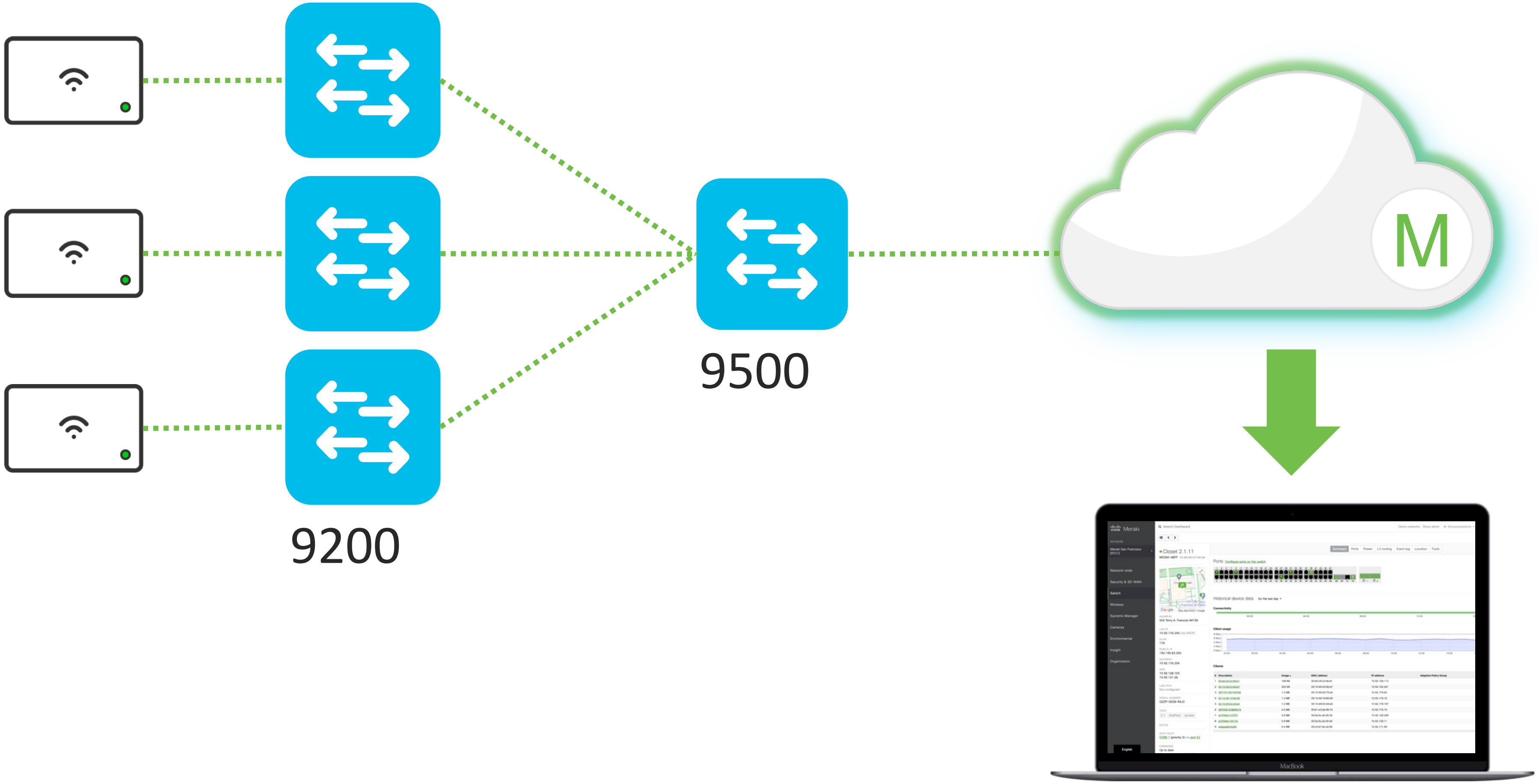
Tiered Architecture



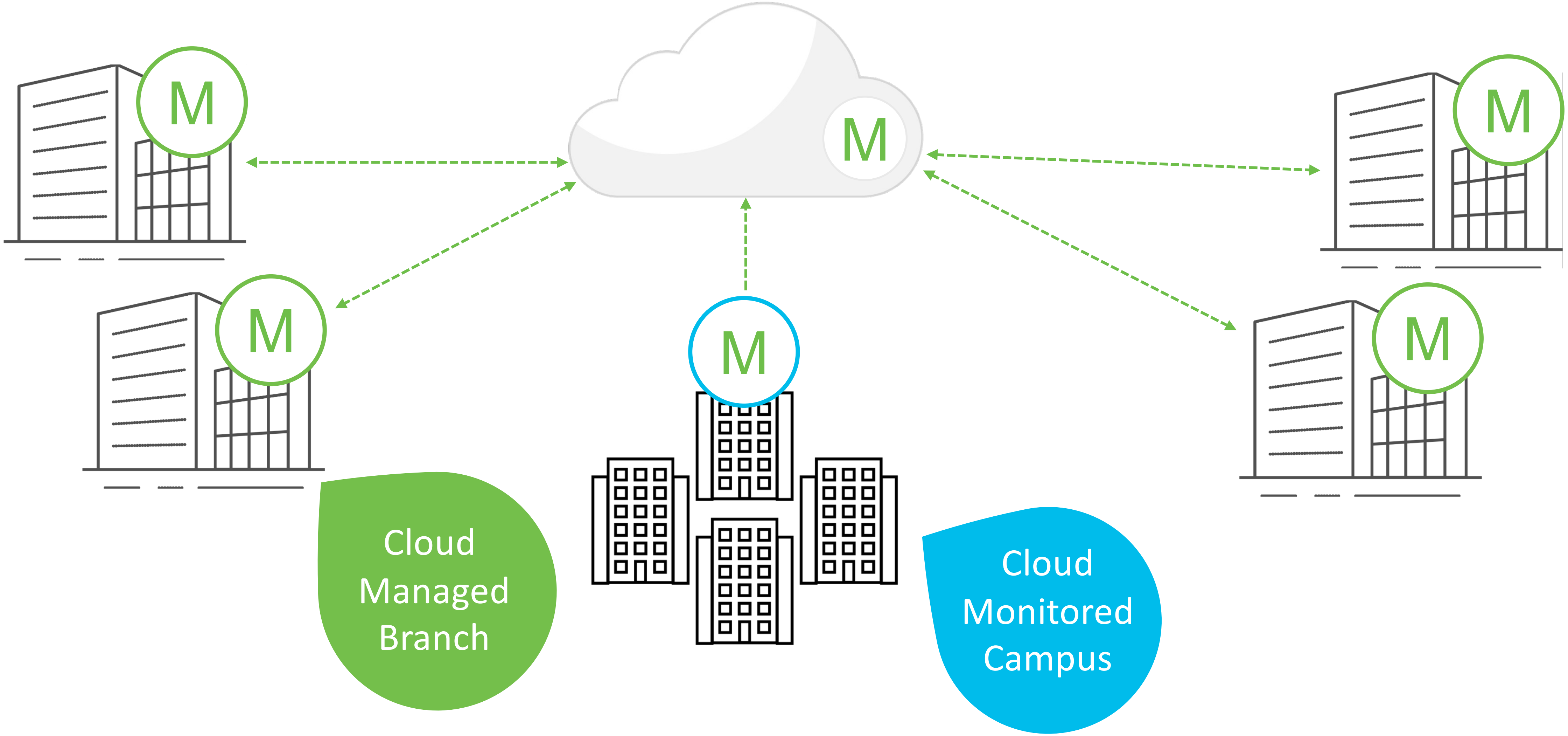
Cloud Managed Access Layer

Cloud Monitored Core

Centralized Monitoring of Catalyst Networks



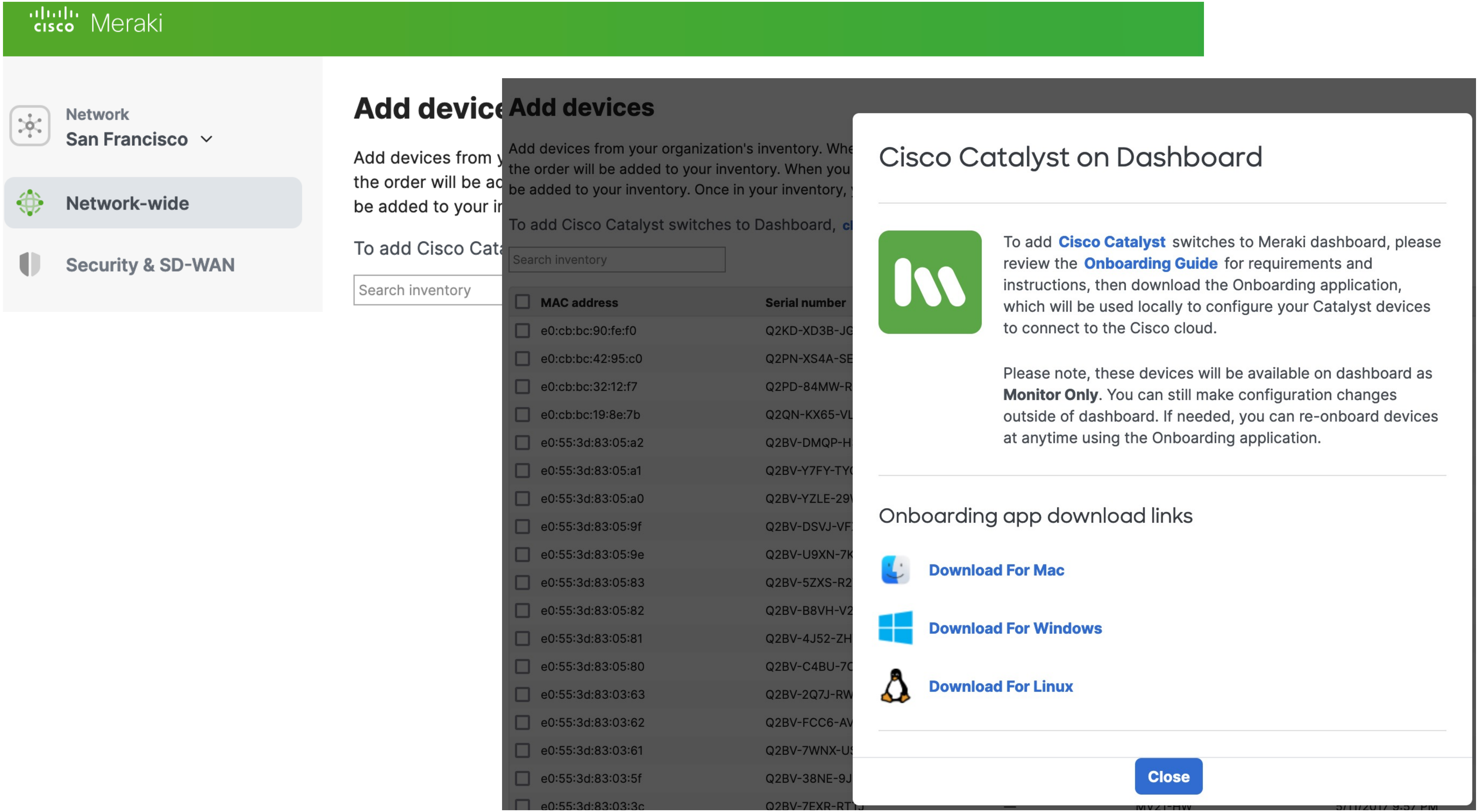
Catalyst Campus with Meraki Branches



Cloud Managed Branch

Cloud Monitored Campus

Onboarding Your Devices



Add device

Add devices from y
the order will be ac
be added to your in

To add Cisco Cata

Search inventory

Add devices

Add devices from your organization's inventory. Whe
the order will be added to your inventory. When you
be added to your inventory. Once in your inventory, y

To add Cisco Catalyst switches to Dashboard, cl

Search inventory

□	MAC address	Serial number
□	e0:cb:bc:90:fe:f0	Q2KD-XD3B-JG
□	e0:cb:bc:42:95:c0	Q2PN-XS4A-SE
□	e0:cb:bc:32:12:f7	Q2PD-84MW-R
□	e0:cb:bc:19:8e:7b	Q2QN-KX65-VL
□	e0:55:3d:83:05:a2	Q2BV-DMQP-H
□	e0:55:3d:83:05:a1	Q2BV-Y7FY-TY
□	e0:55:3d:83:05:a0	Q2BV-YZLE-29
□	e0:55:3d:83:05:9f	Q2BV-DSVJ-VF
□	e0:55:3d:83:05:9e	Q2BV-U9XN-7K
□	e0:55:3d:83:05:83	Q2BV-5ZXS-R2
□	e0:55:3d:83:05:82	Q2BV-B8VH-V2
□	e0:55:3d:83:05:81	Q2BV-4J52-ZH
□	e0:55:3d:83:05:80	Q2BV-C4BU-7C
□	e0:55:3d:83:03:63	Q2BV-2Q7J-RW
□	e0:55:3d:83:03:62	Q2BV-FCC6-AV
□	e0:55:3d:83:03:61	Q2BV-7WNX-U
□	e0:55:3d:83:03:5f	Q2BV-38NE-9J
□	e0:55:3d:83:03:3c	Q2BV-7EXR-RT

Cisco Catalyst on Dashboard

To add **Cisco Catalyst** switches to Meraki dashboard, please review the **Onboarding Guide** for requirements and instructions, then download the Onboarding application, which will be used locally to configure your Catalyst devices to connect to the Cisco cloud.

Please note, these devices will be available on dashboard as **Monitor Only**. You can still make configuration changes outside of dashboard. If needed, you can re-onboard devices at anytime using the Onboarding application.

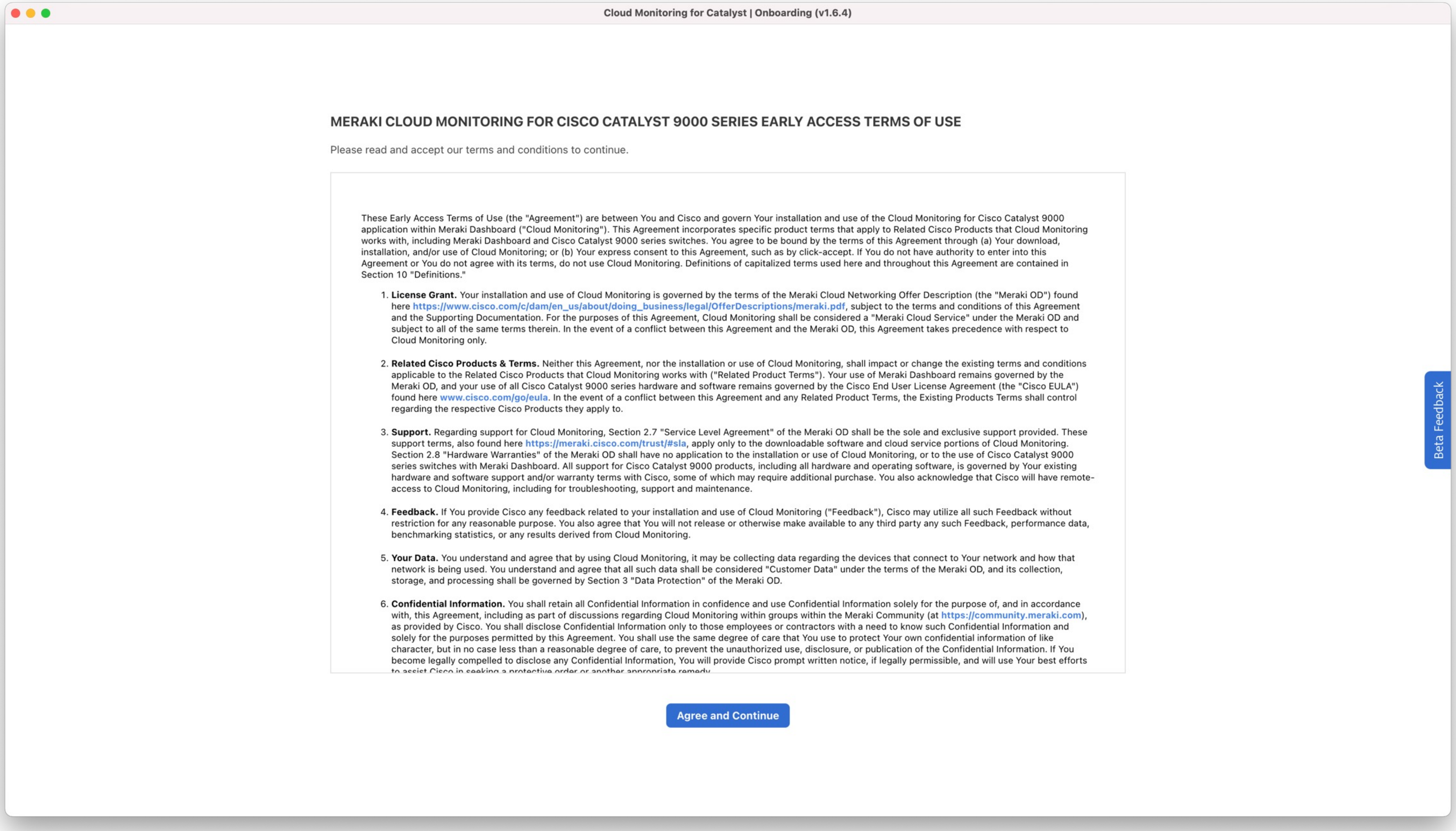
Onboarding app download links

Download For Mac

Download For Windows

Download For Linux

Onboarding Step 0 – Terms and Conditions



MERAKI CLOUD MONITORING FOR CISCO CATALYST 9000 SERIES EARLY ACCESS TERMS OF USE

Please read and accept our terms and conditions to continue.

These Early Access Terms of Use (the "Agreement") are between You and Cisco and govern Your installation and use of the Cloud Monitoring for Cisco Catalyst 9000 application within Meraki Dashboard ("Cloud Monitoring"). This Agreement incorporates specific product terms that apply to Related Cisco Products that Cloud Monitoring works with, including Meraki Dashboard and Cisco Catalyst 9000 series switches. You agree to be bound by the terms of this Agreement through (a) Your download, installation, and/or use of Cloud Monitoring; or (b) Your express consent to this Agreement, such as by click-accept. If You do not have authority to enter into this Agreement or You do not agree with its terms, do not use Cloud Monitoring. Definitions of capitalized terms used here and throughout this Agreement are contained in Section 10 "Definitions."

1. **License Grant.** Your installation and use of Cloud Monitoring is governed by the terms of the Meraki Cloud Networking Offer Description (the "Meraki OD") found here https://www.cisco.com/c/dam/en_us/about/doing_business/legal/OfferDescriptions/meraki.pdf, subject to the terms and conditions of this Agreement and the Supporting Documentation. For the purposes of this Agreement, Cloud Monitoring shall be considered a "Meraki Cloud Service" under the Meraki OD and subject to all of the same terms therein. In the event of a conflict between this Agreement and the Meraki OD, this Agreement takes precedence with respect to Cloud Monitoring only.

2. **Related Cisco Products & Terms.** Neither this Agreement, nor the installation or use of Cloud Monitoring, shall impact or change the existing terms and conditions applicable to the Related Cisco Products that Cloud Monitoring works with ("Related Product Terms"). Your use of Meraki Dashboard remains governed by the Meraki OD, and your use of all Cisco Catalyst 9000 series hardware and software remains governed by the Cisco End User License Agreement (the "Cisco EULA") found here www.cisco.com/go/eula. In the event of a conflict between this Agreement and any Related Product Terms, the Existing Products Terms shall control regarding the respective Cisco Products they apply to.

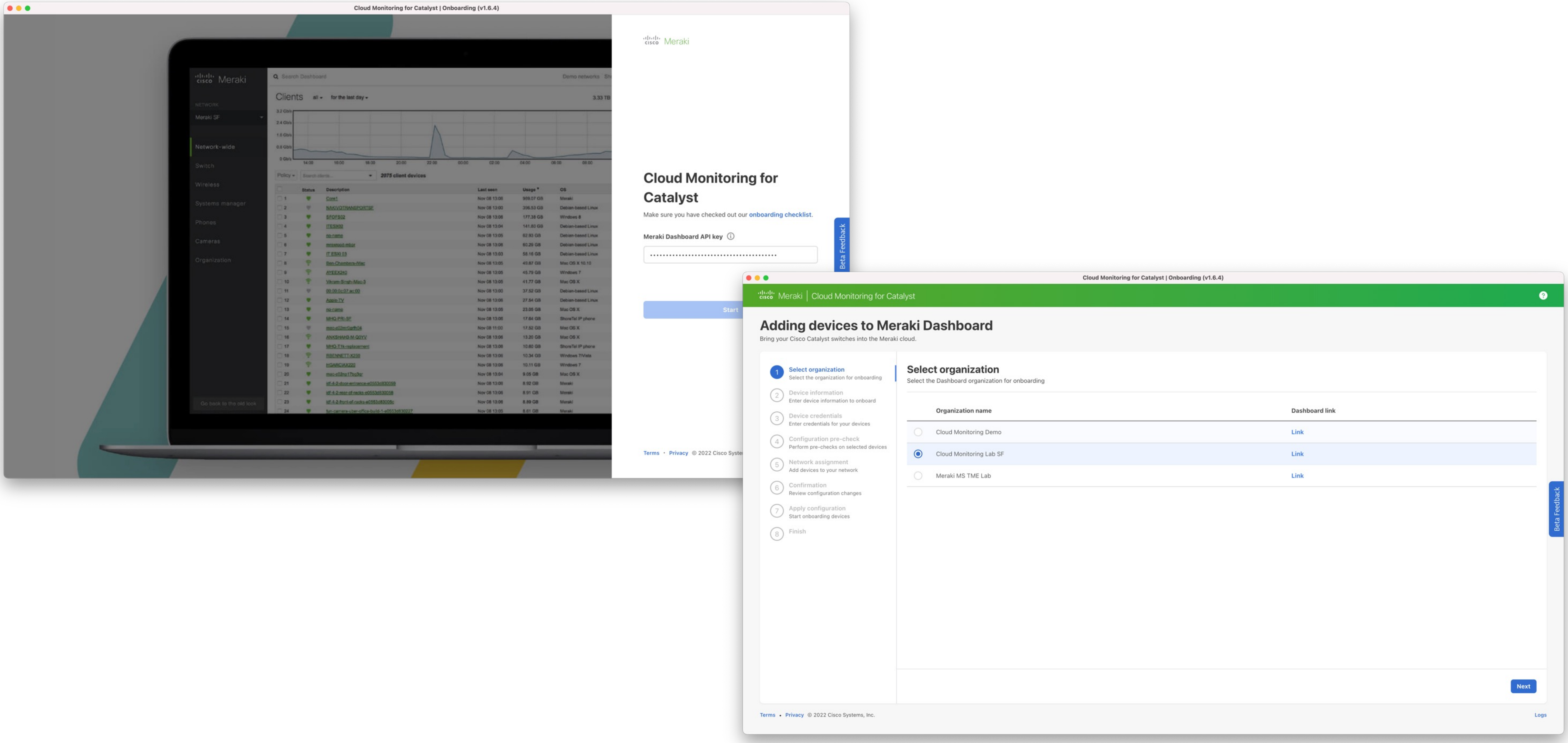
3. **Support.** Regarding support for Cloud Monitoring, Section 2.7 "Service Level Agreement" of the Meraki OD shall be the sole and exclusive support provided. These support terms, also found here https://meraki.cisco.com/trust/#sla, apply only to the downloadable software and cloud service portions of Cloud Monitoring. Section 2.8 "Hardware Warranties" of the Meraki OD shall have no application to the installation or use of Cloud Monitoring, or to the use of Cisco Catalyst 9000 series switches with Meraki Dashboard. All support for Cisco Catalyst 9000 products, including all hardware and operating software, is governed by Your existing hardware and software support and/or warranty terms with Cisco, some of which may require additional purchase. You also acknowledge that Cisco will have remote-access to Cloud Monitoring, including for troubleshooting, support and maintenance.

4. **Feedback.** If You provide Cisco any feedback related to your installation and use of Cloud Monitoring ("Feedback"), Cisco may utilize all such Feedback without restriction for any reasonable purpose. You also agree that You will not release or otherwise make available to any third party any such Feedback, performance data, benchmarking statistics, or any results derived from Cloud Monitoring.

5. **Your Data.** You understand and agree that by using Cloud Monitoring, it may be collecting data regarding the devices that connect to Your network and how that network is being used. You understand and agree that all such data shall be considered "Customer Data" under the terms of the Meraki OD, and its collection, storage, and processing shall be governed by Section 3 "Data Protection" of the Meraki OD.

6. **Confidential Information.** You shall retain all Confidential Information in confidence and use Confidential Information solely for the purpose of, and in accordance with, this Agreement, including as part of discussions regarding Cloud Monitoring within groups within the Meraki Community (at https://community.meraki.com), as provided by Cisco. You shall disclose Confidential Information only to those employees or contractors with a need to know such Confidential Information and solely for the purposes permitted by this Agreement. You shall use the same degree of care that You use to protect Your own confidential information of like character, but in no case less than a reasonable degree of care, to prevent the unauthorized use, disclosure, or publication of the Confidential Information. If You become legally compelled to disclose any Confidential Information, You will provide Cisco prompt written notice, if legally permissible, and will use Your best efforts to assist Cisco in seeking a protective order or another appropriate remedy.

Onboarding Step 1 – API Key & Org Selection



Cloud Monitoring for Catalyst | Onboarding (v1.6.4)

Cloud Monitoring for Catalyst

Make sure you have checked out our onboarding checklist.

Meraki Dashboard API key: ··

Terms · Privacy © 2022 Cisco Syste

Cloud Monitoring for Catalyst | Onboarding (v1.6.4)

Adding devices to Meraki Dashboard

Bring your Cisco Catalyst switches into the Meraki cloud.

1. Select organization – Select the organization for onboarding
2. Device information – Enter device information to onboard
3. Device credentials – Enter credentials for your devices
4. Configuration pre-check – Perform pre-checks on selected devices
5. Network assignment – Add devices to your network
6. Confirmation – Review configuration changes
7. Apply configuration – Start onboarding devices
8. Finish

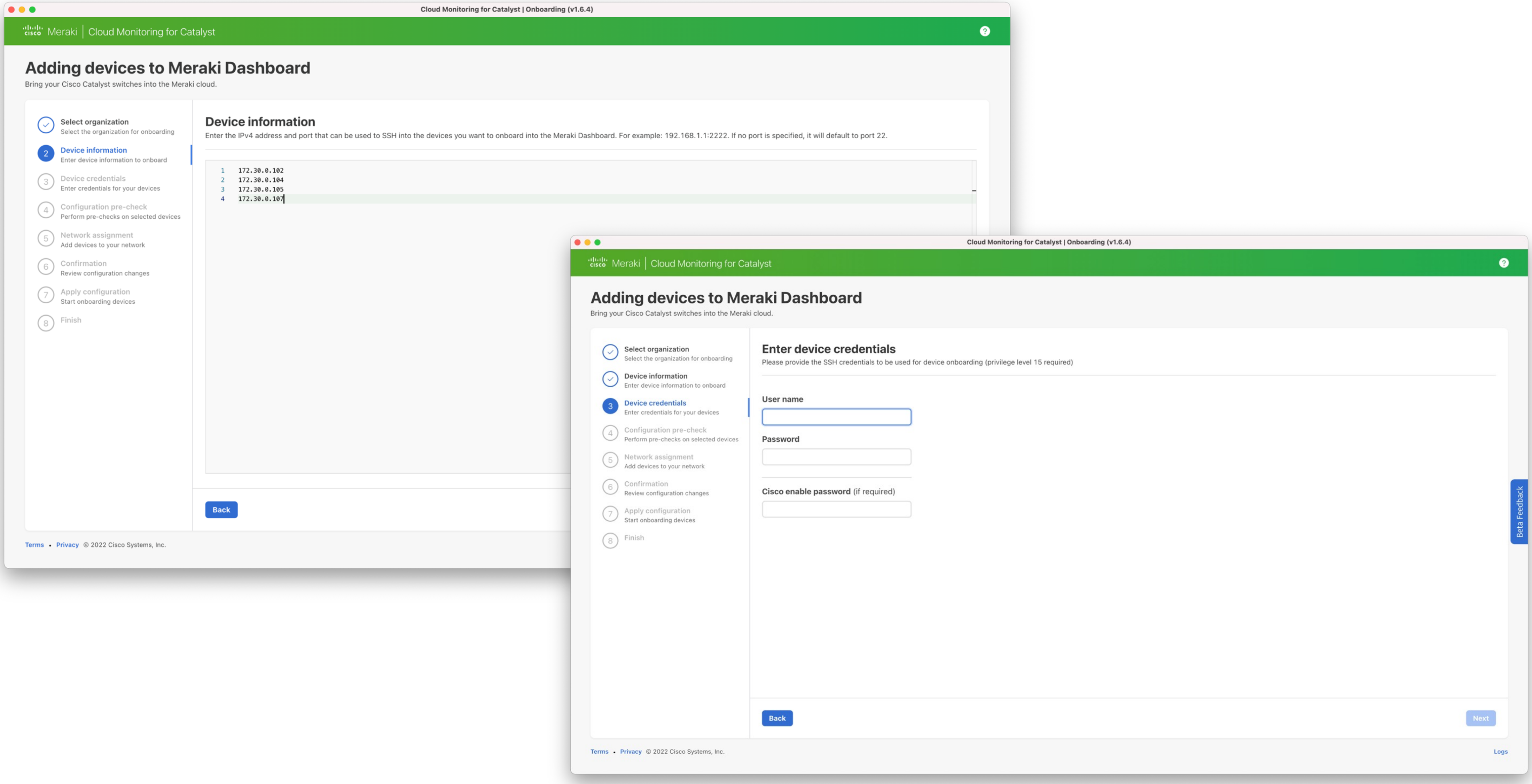
Select organization

Select the Dashboard organization for onboarding

	Organization name	Dashboard link
○	Cloud Monitoring Demo	Link
●	Cloud Monitoring Lab SF	Link
○	Meraki MS TME Lab	Link

Terms · Privacy © 2022 Cisco Systems, Inc.

Onboarding Step 2&3 – Device IP and Credentials



Cloud Monitoring for Catalyst | Onboarding (v1.6.4)
Meraki | Cloud Monitoring for Catalyst

Adding devices to Meraki Dashboard

Bring your Cisco Catalyst switches into the Meraki cloud.

Select organization
Select the organization for onboarding
2 Device information
Enter device information to onboard
3 Device credentials
Enter credentials for your devices
4 Configuration pre-check
Perform pre-checks on selected devices
5 Network assignment
Add devices to your network
6 Confirmation
Review configuration changes
7 Apply configuration
Start onboarding devices
8 Finish

Device information

Enter the IPv4 address and port that can be used to SSH into the devices you want to onboard into the Meraki Dashboard. For example: 192.168.1.1:2222. If no port is specified, it will default to port 22.

```
172.30.0.102
172.30.0.104
172.30.0.105
172.30.0.107
```

Back
Terms • Privacy © 2022 Cisco Systems, Inc.
Cloud Monitoring for Catalyst | Onboarding (v1.6.4)
Meraki | Cloud Monitoring for Catalyst

Adding devices to Meraki Dashboard

Bring your Cisco Catalyst switches into the Meraki cloud.

Select organization
Select the organization for onboarding
Device information
Enter device information to onboard
3 Device credentials
Enter credentials for your devices
4 Configuration pre-check
Perform pre-checks on selected devices
5 Network assignment
Add devices to your network
6 Confirmation
Review configuration changes
7 Apply configuration
Start onboarding devices
8 Finish

Enter device credentials

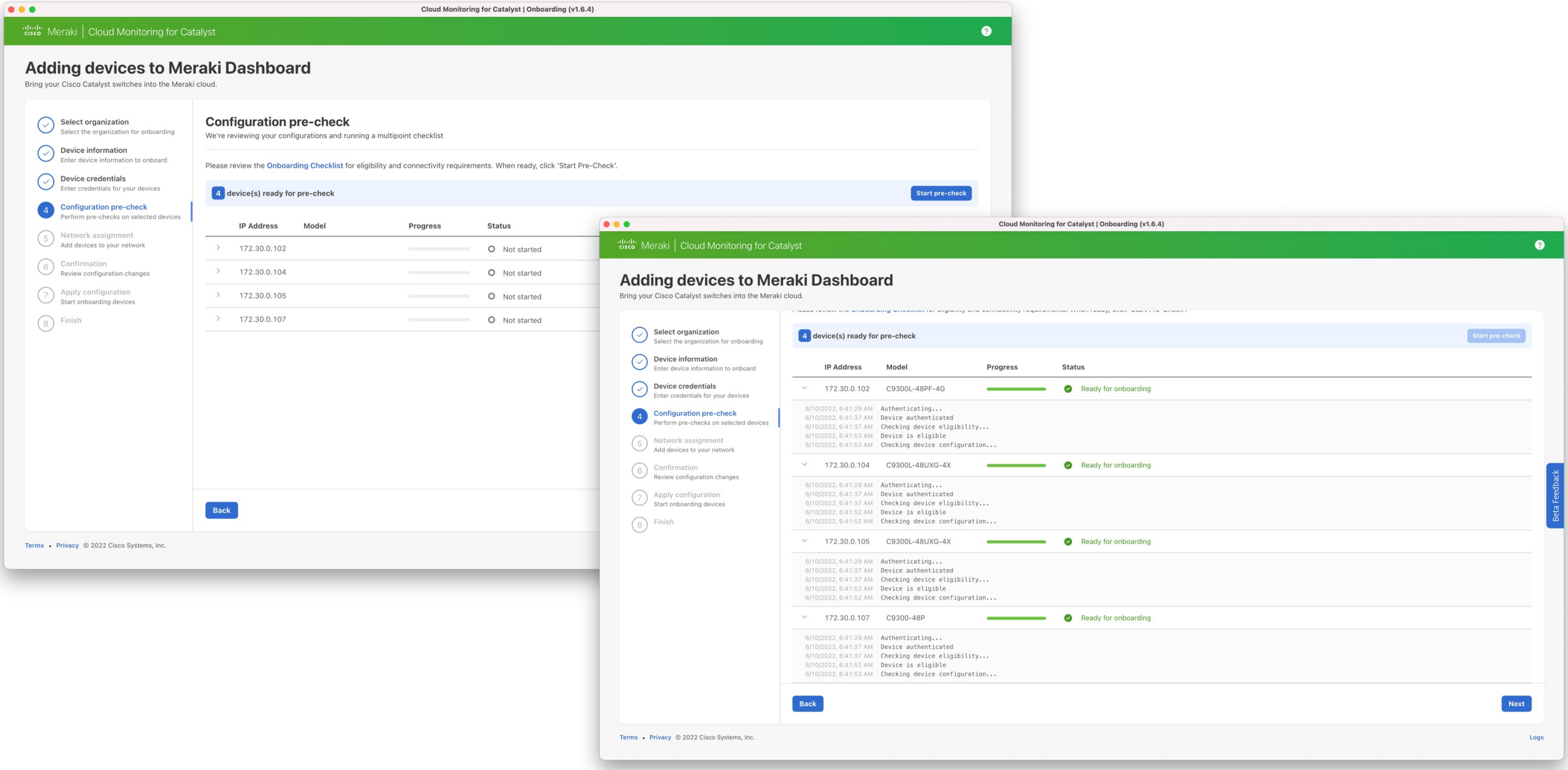
Please provide the SSH credentials to be used for device onboarding (privilege level 15 required)

User name

Password

Cisco enable password (if required)

Onboarding Step 4 – Device Pre-Checks



Cloud Monitoring for Catalyst | Onboarding (v1.6.4)
Meraki | Cloud Monitoring for Catalyst

Adding devices to Meraki Dashboard

Bring your Cisco Catalyst switches into the Meraki cloud.

Select organization
Select the organization for onboarding
Device information
Enter device information to onboard
Device credentials
Enter credentials for your devices
4 Configuration pre-check
Perform pre-checks on selected devices
5 Network assignment
Add devices to your network
6 Confirmation
Review configuration changes
7 Apply configuration
Start onboarding devices
8 Finish

Configuration pre-check

We're reviewing your configurations and running a multipoint checklist

Please review the Onboarding Checklist for eligibility and connectivity requirements. When ready, click 'Start Pre-Check'.

4 device(s) ready for pre-check

IP Address	Model	Progress	Status
172.30.0.102			○ Not started
172.30.0.104			○ Not started
172.30.0.105			○ Not started
172.30.0.107			○ Not started

Terms • Privacy © 2022 Cisco Systems, Inc.

Cloud Monitoring for Catalyst | Onboarding (v1.6.4)
Meraki | Cloud Monitoring for Catalyst

Adding devices to Meraki Dashboard

Bring your Cisco Catalyst switches into the Meraki cloud.

Select organization
Select the organization for onboarding
Device information
Enter device information to onboard
Device credentials
Enter credentials for your devices
4 Configuration pre-check
Perform pre-checks on selected devices
5 Network assignment
Add devices to your network
6 Confirmation
Review configuration changes
7 Apply configuration
Start onboarding devices
8 Finish

4 device(s) ready for pre-check

IP Address	Model	Progress	Status
172.30.0.102	C9300L-48PF-4G		✓ Ready for onboarding

```
6/10/2022, 6:41:29 AM  Authenticating...
6/10/2022, 6:41:37 AM  Device authenticated
6/10/2022, 6:41:37 AM  Checking device eligibility...
6/10/2022, 6:41:53 AM  Device is eligible
6/10/2022, 6:41:53 AM  Checking device configuration...
```

IP Address	Model	Progress	Status
172.30.0.104	C9300L-48UXG-4X		✓ Ready for onboarding

```
6/10/2022, 6:41:29 AM  Authenticating...
6/10/2022, 6:41:37 AM  Device authenticated
6/10/2022, 6:41:37 AM  Checking device eligibility...
6/10/2022, 6:41:52 AM  Device is eligible
6/10/2022, 6:41:52 AM  Checking device configuration...
```

IP Address	Model	Progress	Status
172.30.0.105	C9300L-48UXG-4X		✓ Ready for onboarding

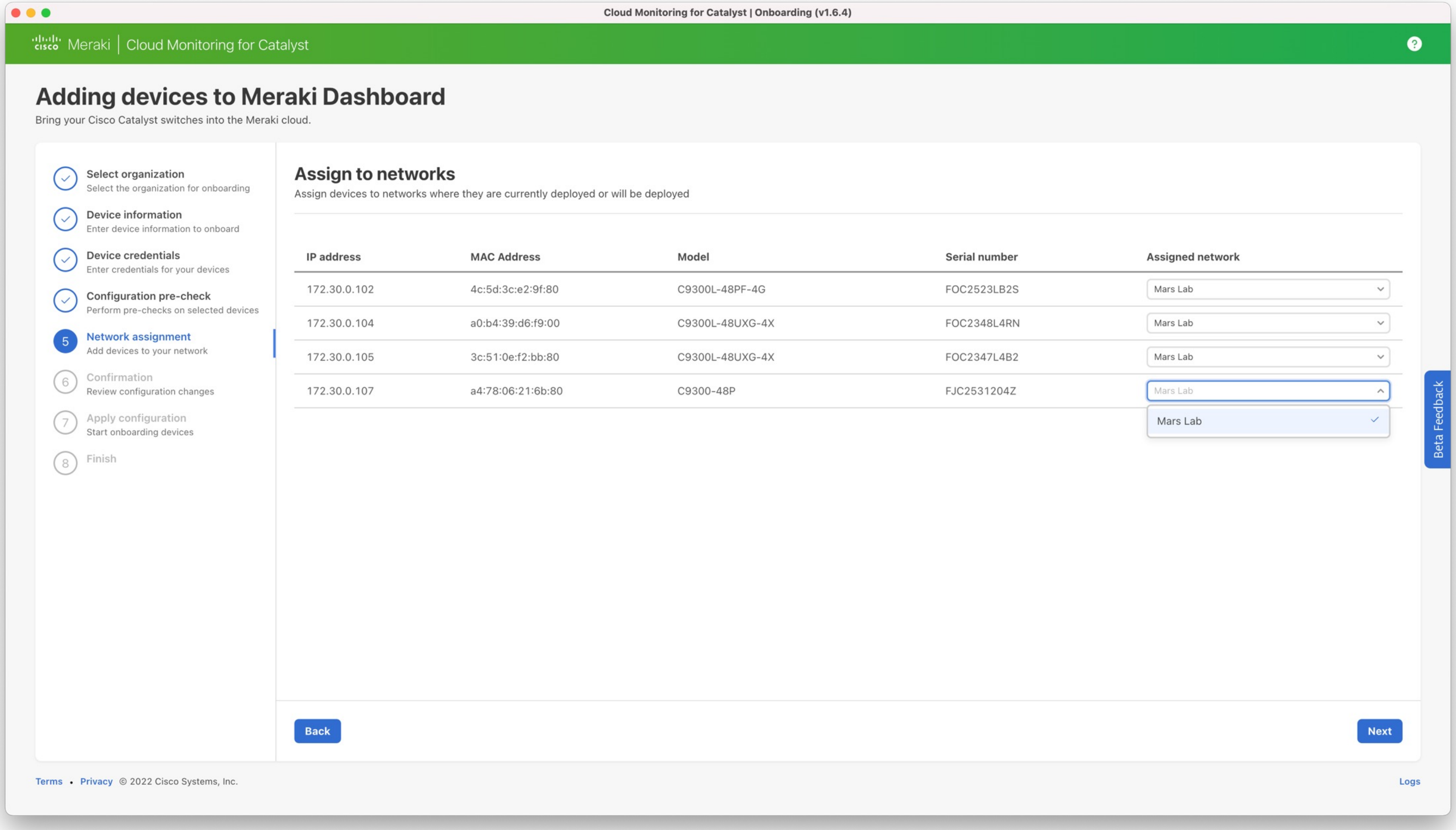
```
6/10/2022, 6:41:29 AM  Authenticating...
6/10/2022, 6:41:37 AM  Device authenticated
6/10/2022, 6:41:37 AM  Checking device eligibility...
6/10/2022, 6:41:52 AM  Device is eligible
6/10/2022, 6:41:52 AM  Checking device configuration...
```

IP Address	Model	Progress	Status
172.30.0.107	C9300-48P		✓ Ready for onboarding

```
6/10/2022, 6:41:29 AM  Authenticating...
6/10/2022, 6:41:37 AM  Device authenticated
6/10/2022, 6:41:37 AM  Checking device eligibility...
6/10/2022, 6:41:52 AM  Device is eligible
6/10/2022, 6:41:52 AM  Checking device configuration...
```

Terms • Privacy © 2022 Cisco Systems, Inc.

Onboarding Step 5 – Network Selection



Cloud Monitoring for Catalyst | Onboarding (v1.6.4)

Adding devices to Meraki Dashboard

Bring your Cisco Catalyst switches into the Meraki cloud.

- ✓ **Select organization** Select the organization for onboarding
- ✓ **Device information** Enter device information to onboard
- ✓ **Device credentials** Enter credentials for your devices
- ✓ **Configuration pre-check** Perform pre-checks on selected devices
- 5 **Network assignment** Add devices to your network
- 6 Confirmation Review configuration changes
- 7 Apply configuration Start onboarding devices
- 8 Finish

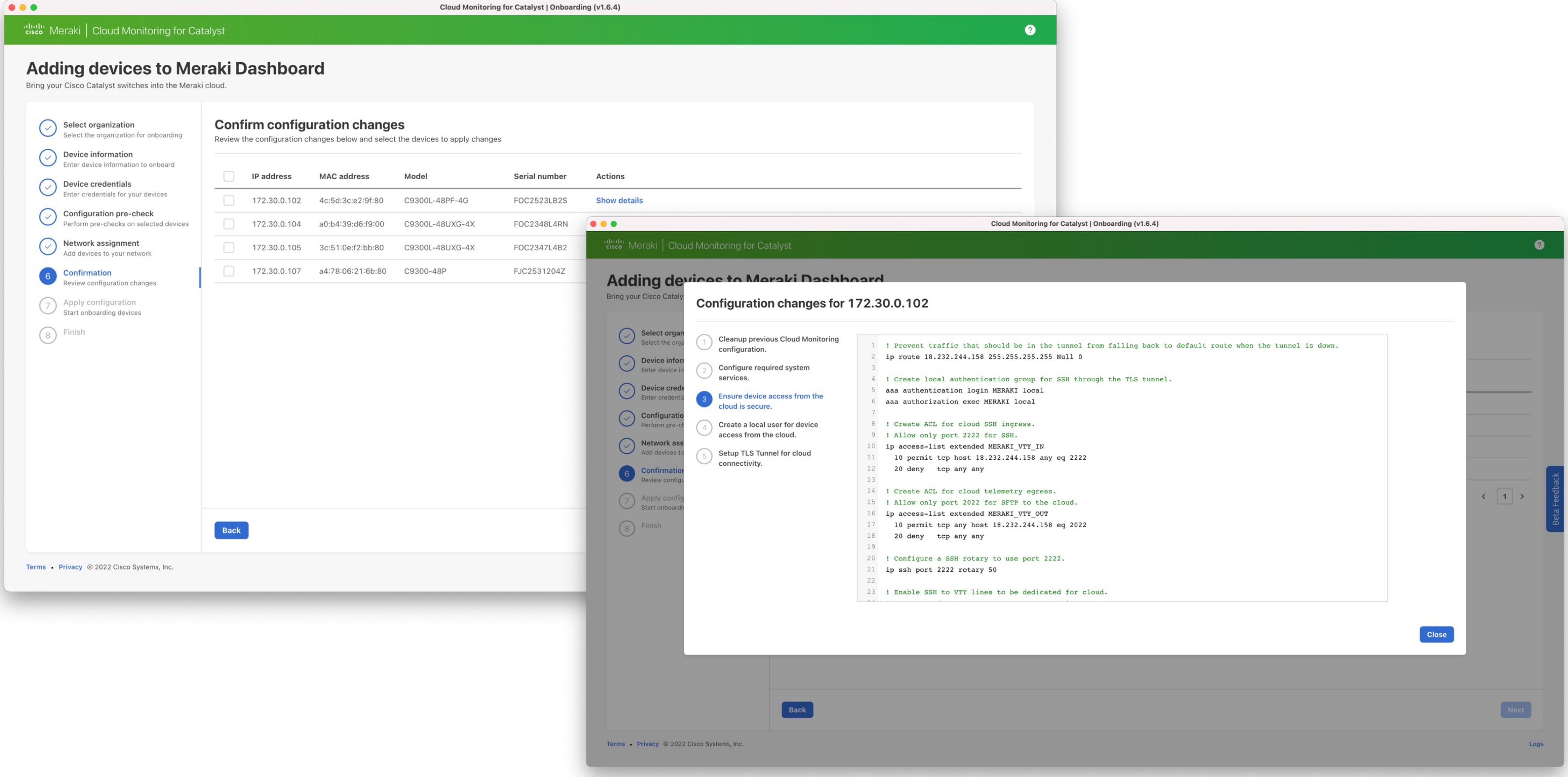
Assign to networks

Assign devices to networks where they are currently deployed or will be deployed

IP address	MAC Address	Model	Serial number	Assigned network
172.30.0.102	4c:5d:3c:e2:9f:80	C9300L-48PF-4G	FOC2523LB2S	Mars Lab
172.30.0.104	a0:b4:39:d6:f9:00	C9300L-48UXG-4X	FOC2348L4RN	Mars Lab
172.30.0.105	3c:51:0e:f2:bb:80	C9300L-48UXG-4X	FOC2347L4B2	Mars Lab
172.30.0.107	a4:78:06:21:6b:80	C9300-48P	FJC2531204Z	Mars Lab

Terms • Privacy © 2022 Cisco Systems, Inc.

Onboarding Step 6 – Preview Config



Cloud Monitoring for Catalyst | Onboarding (v1.6.4)

Adding devices to Meraki Dashboard

Bring your Cisco Catalyst switches into the Meraki cloud.

1. Select organization – Select the organization for onboarding
2. Device information – Enter device information to onboard
3. Device credentials – Enter credentials for your devices
4. Configuration pre-check – Perform pre-checks on selected devices
5. Network assignment – Add devices to your network
6. Confirmation – Review configuration changes
7. Apply configuration – Start onboarding devices
8. Finish

Confirm configuration changes

Review the configuration changes below and select the devices to apply changes

☐	IP address	MAC address	Model	Serial number	Actions
☐	172.30.0.102	4c:5d:3c:e2:9f:80	C9300L-48PF-4G	FOC2523LB2S	Show details
☐	172.30.0.104	a0:b4:39:d6:f9:00	C9300L-48UXG-4X	FOC2348L4RN	
☐	172.30.0.105	3c:51:0e:f2:bb:80	C9300L-48UXG-4X	FOC2347L4B2	
☐	172.30.0.107	a4:78:06:21:6b:80	C9300-48P	FJC2531204Z	

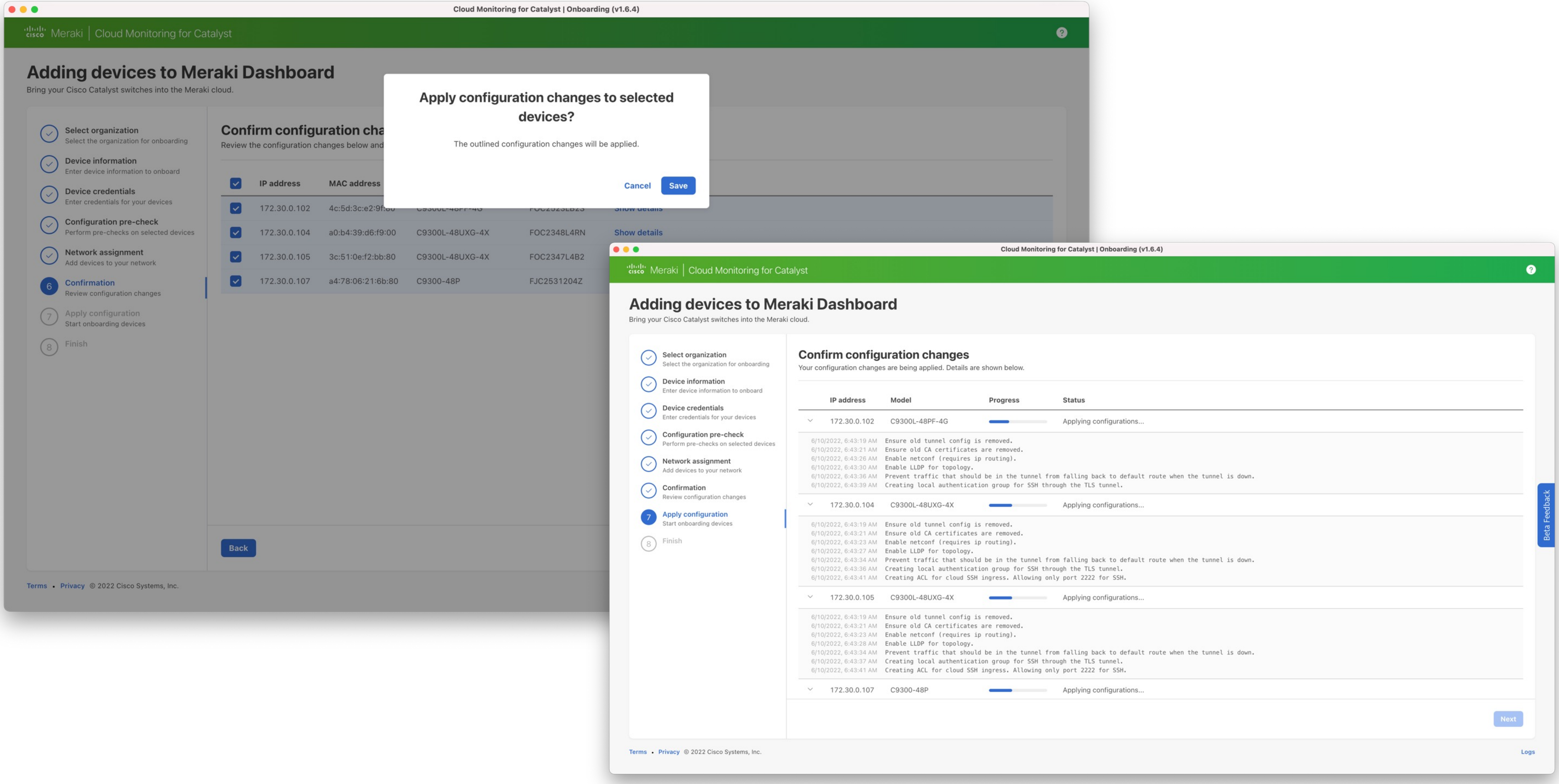
Terms • Privacy © 2022 Cisco Systems, Inc.

Configuration changes for 172.30.0.102

1. Cleanup previous Cloud Monitoring configuration.
2. Configure required system services.
3. Ensure device access from the cloud is secure.
4. Create a local user for device access from the cloud.
5. Setup TLS Tunnel for cloud connectivity.

```
! Prevent traffic that should be in the tunnel from falling back to default route when the tunnel is down.
ip route 18.232.244.158 255.255.255.255 Null 0

! Create local authentication group for SSH through the TLS tunnel.
aaa authentication login MERAKI local
aaa authorization exec MERAKI local

! Create ACL for cloud SSH ingress.
! Allow only port 2222 for SSH.
ip access-list extended MERAKI_VTY_IN
  10 permit tcp host 18.232.244.158 any eq 2222
  20 deny   tcp any any

! Create ACL for cloud telemetry egress.
! Allow only port 2022 for SFTP to the cloud.
ip access-list extended MERAKI_VTY_OUT
  10 permit tcp any host 18.232.244.158 eq 2022
  20 deny   tcp any any

! Configure a SSH rotary to use port 2222.
ip ssh port 2222 rotary 50

! Enable SSH to VTY lines to be dedicated for cloud.
```

Onboarding Step 7 – Apply Configuration


Cloud Monitoring for Catalyst | Onboarding (v1.6.4)
Meraki | Cloud Monitoring for Catalyst

Adding devices to Meraki Dashboard

Bring your Cisco Catalyst switches into the Meraki cloud.

Select organization
Select the organization for onboarding
Device information
Enter device information to onboard
Device credentials
Enter credentials for your devices
Configuration pre-check
Perform pre-checks on selected devices
Network assignment
Add devices to your network
6 Confirmation
Review configuration changes
7 Apply configuration
Start onboarding devices
8 Finish

Confirm configuration cha

Review the configuration changes below and

☑	IP address	MAC address			
☑	172.30.0.102	4c:5d:3c:e2:9f:80	C9300L-48PF-4G	FOC2323LBZ3	Show details
☑	172.30.0.104	a0:b4:39:d6:f9:00	C9300L-48UXG-4X	FOC2348L4RN	Show details
☑	172.30.0.105	3c:51:0e:f2:bb:80	C9300L-48UXG-4X	FOC2347L4B2	
☑	172.30.0.107	a4:78:06:21:6b:80	C9300-48P	FJC2531204Z	

Apply configuration changes to selected devices?

The outlined configuration changes will be applied.

Cloud Monitoring for Catalyst | Onboarding (v1.6.4)
Meraki | Cloud Monitoring for Catalyst

Adding devices to Meraki Dashboard

Bring your Cisco Catalyst switches into the Meraki cloud.

Select organization
Select the organization for onboarding
Device information
Enter device information to onboard
Device credentials
Enter credentials for your devices
Configuration pre-check
Perform pre-checks on selected devices
Network assignment
Add devices to your network
Confirmation
Review configuration changes
7 Apply configuration
Start onboarding devices
8 Finish

Confirm configuration changes

Your configuration changes are being applied. Details are shown below.

IP address	Model	Progress	Status
172.30.0.102	C9300L-48PF-4G		Applying configurations...

```
6/10/2022, 6:43:19 AM  Ensure old tunnel config is removed.
6/10/2022, 6:43:21 AM  Ensure old CA certificates are removed.
6/10/2022, 6:43:26 AM  Enable netconf (requires ip routing).
6/10/2022, 6:43:30 AM  Enable LLDP for topology.
6/10/2022, 6:43:36 AM  Prevent traffic that should be in the tunnel from falling back to default route when the tunnel is down.
6/10/2022, 6:43:39 AM  Creating local authentication group for SSH through the TLS tunnel.
```

IP address	Model	Progress	Status
172.30.0.104	C9300L-48UXG-4X		Applying configurations...

```
6/10/2022, 6:43:19 AM  Ensure old tunnel config is removed.
6/10/2022, 6:43:21 AM  Ensure old CA certificates are removed.
6/10/2022, 6:43:23 AM  Enable netconf (requires ip routing).
6/10/2022, 6:43:27 AM  Enable LLDP for topology.
6/10/2022, 6:43:34 AM  Prevent traffic that should be in the tunnel from falling back to default route when the tunnel is down.
6/10/2022, 6:43:36 AM  Creating local authentication group for SSH through the TLS tunnel.
6/10/2022, 6:43:41 AM  Creating ACL for cloud SSH ingress. Allowing only port 2222 for SSH.
```

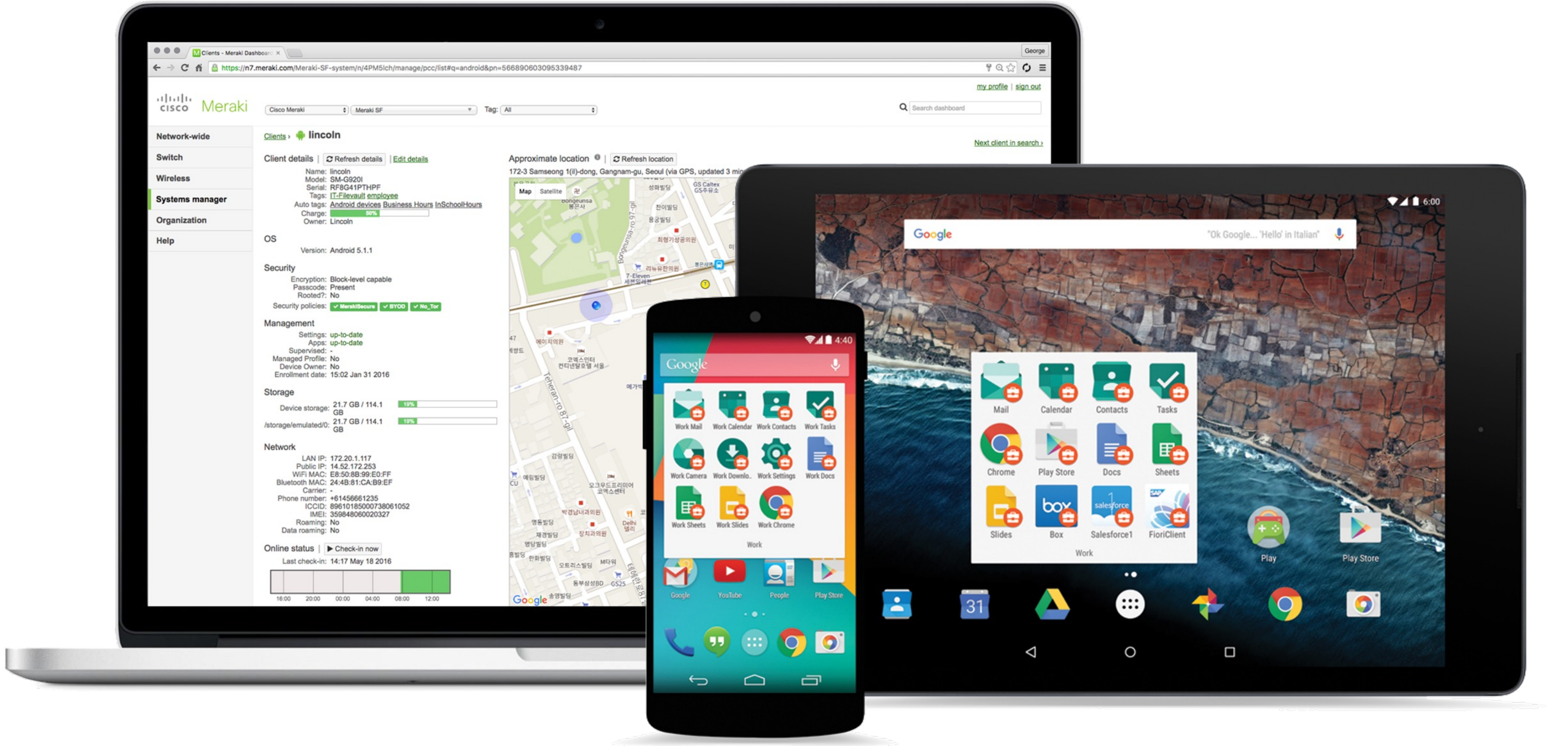
IP address	Model	Progress	Status
172.30.0.105	C9300L-48UXG-4X		Applying configurations...

```
6/10/2022, 6:43:19 AM  Ensure old tunnel config is removed.
6/10/2022, 6:43:21 AM  Ensure old CA certificates are removed.
6/10/2022, 6:43:23 AM  Enable netconf (requires ip routing).
6/10/2022, 6:43:28 AM  Enable LLDP for topology.
6/10/2022, 6:43:34 AM  Prevent traffic that should be in the tunnel from falling back to default route when the tunnel is down.
6/10/2022, 6:43:37 AM  Creating local authentication group for SSH through the TLS tunnel.
6/10/2022, 6:43:41 AM  Creating ACL for cloud SSH ingress. Allowing only port 2222 for SSH.
```

IP address	Model	Progress	Status
172.30.0.107	C9300-48P		Applying configurations...

Cisco Meraki systems manager

Product overview



lincoln

Client details

Name: lincoln
Model: SM-G920I
Serial: RF8G41PTHPF
Tags: IT-Filevault employee
Auto tags: Android devices Business Hours InSchoolHours
Charge: 50%
Owner: Lincoln

OS

Version: Android 5.1.1

Security

Encryption: Block-level capable
Passcode: Present
Rooted?: No
Security policies: ✓ MerakiSecure ✓ BYOD ✓ No_Tor

Management

Settings: up-to-date
Apps: up-to-date
Supervised: -
Managed Profile: No
Device Owner: No
Enrollment date: 15:02 Jan 31 2016

Storage

Device storage: 21.7 GB / 114.1 GB 19%
/storage/emulated/0: 21.7 GB / 114.1 GB 19%

Network

LAN IP: 172.20.1.117
Public IP: 14.52.172.253
WiFi MAC: E8:50:8B:99:E0:FF
Bluetooth MAC: 24:4B:81:CA:B9:EF
Carrier: -
Phone number: +61456661235
ICCID: 89610185000738061052
IMEI: 359848060020327
Roaming: No
Data roaming: No

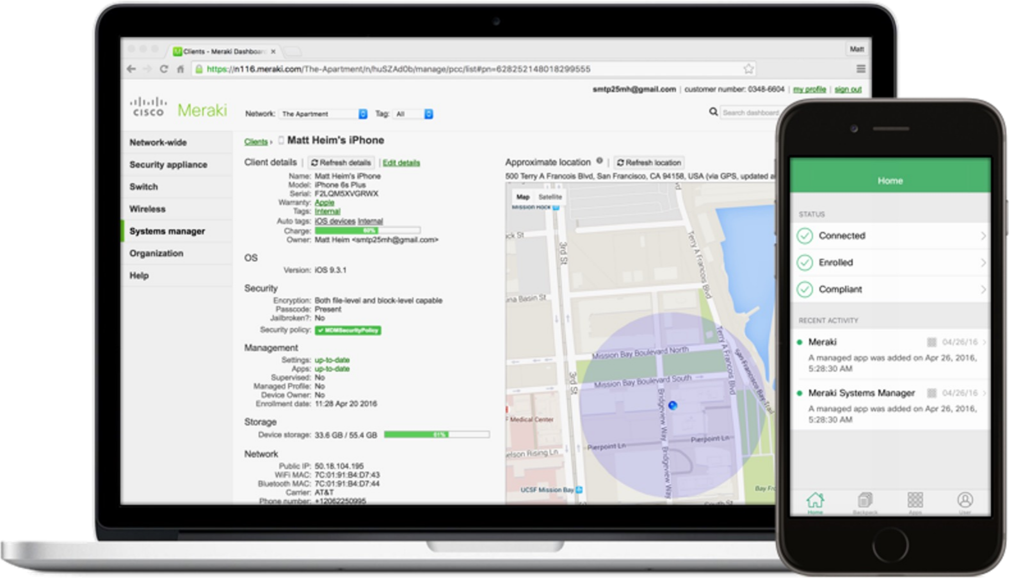
Online status

Last check-in: 14:17 May 18 2016

Approximate location

172-3 Samseong 1(il)-dong, Gangnam-gu, Seoul (via GPS, updated 3 min

Systems Manager Endpoint Management



smtp25mh@gmail.com | customer number: 0348-6604 | my profile | sign out

Clients › Matt Heim's iPhone

Client details

Name: Matt Heim's iPhone
Model: iPhone 6s Plus
Serial: F2LQM5XVGRWX
Warranty: Apple
Tags: Internal
Auto tags: iOS devices Internal
Charge: 60%
Owner: Matt Heim <smtp25mh@gmail.com>

OS

Version: iOS 9.3.1

Security

Encryption: Both file-level and block-level capable
Passcode: Present
Jailbroken?: No
Security policy: ✓ MDMSecurityPolicy

Management

Settings: up-to-date
Apps: up-to-date
Supervised: No
Managed Profile: No
Device Owner: No
Enrollment date: 11:28 Apr 20 2016

Storage

Device storage: 33.6 GB / 55.4 GB 61%

Network

Public IP: 50.18.104.195
WiFi MAC: 7C:01:91:B4:D7:43
Bluetooth MAC: 7C:01:91:B4:D7:44
Carrier: AT&T
Phone number: +12062250995

Approximate location

500 Terry A Francois Blvd, San Francisco, CA 94158, USA (via GPS, updated a

STATUS

✓ Connected
✓ Enrolled
✓ Compliant

RECENT ACTIVITY

● Meraki 04/26/16
A managed app was added on Apr 26, 2016, 5:28:30 AM

● Meraki Systems Manager 04/26/16
A managed app was added on Apr 26, 2016, 5:28:30 AM

FEATURE HIGHLIGHTS

- Device security and location
- Network settings deployment
- Mobile and desktop troubleshooting
- Easy and rapid provisioning
- Backpack file sharing
- Software inventory and app deployment
- MDM-less onboarding with Trusted Access

Multi platform MDM support - macOS, iOS, AppleTV, Windows, Android, & Chrome OS

Cloud-based - no on-site appliances or software, works with any vendor’s network

Deployment Programs

Apple

Device Enrollment Program (DEP) and Apple School Manager (ASM)

“Supervision” for advanced control and automatic enrollment

Android

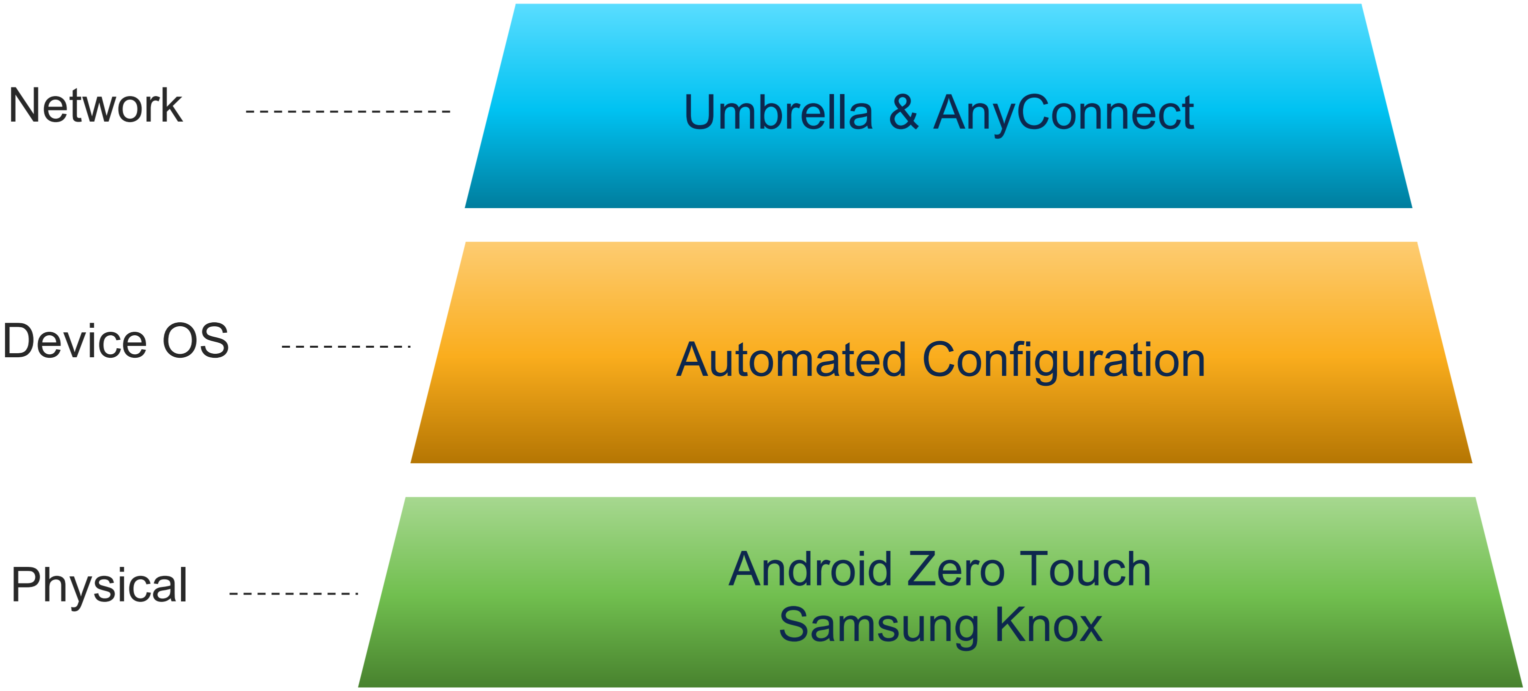
Android Enterprise (Android for Work)

** Android zero-touch enrollment **

Device Owner Mode for advanced control

SM Android Security

Secure in the office or remote



Supported for
Apple iOS too!

Deployment Programs

Volume Purchase Program

Free and paid app management

Silently push apps

Migrate from Apple ID management

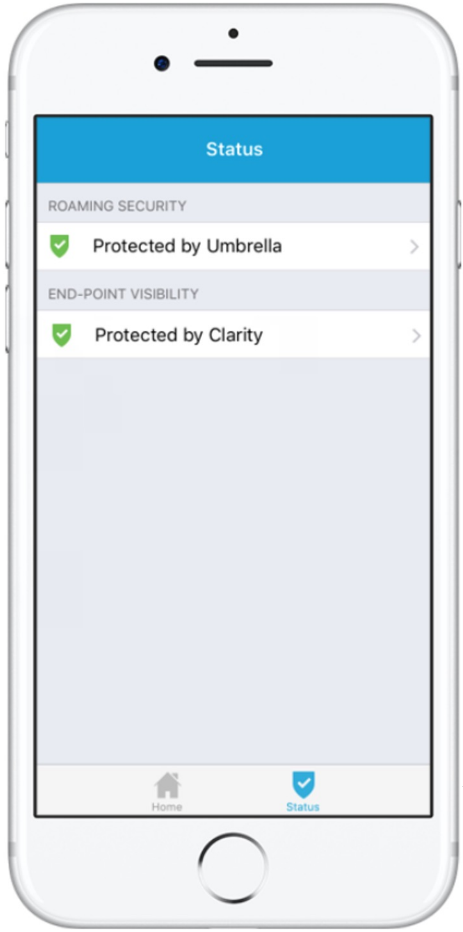
Recover/uninstall managed apps

Playstore Apps for Android Enterprise

Integration with Google for Work Play Store

Push and manage apps in Device Owner mode and BYOD

Cisco Security Connector



Status

ROAMING SECURITY

Protected by Umbrella

END-POINT VISIBILITY

Protected by Clarity

Deployed and managed by Systems Manager

Cisco Umbrella

Your first line of defense against Internet threats protects against phishing attacks.

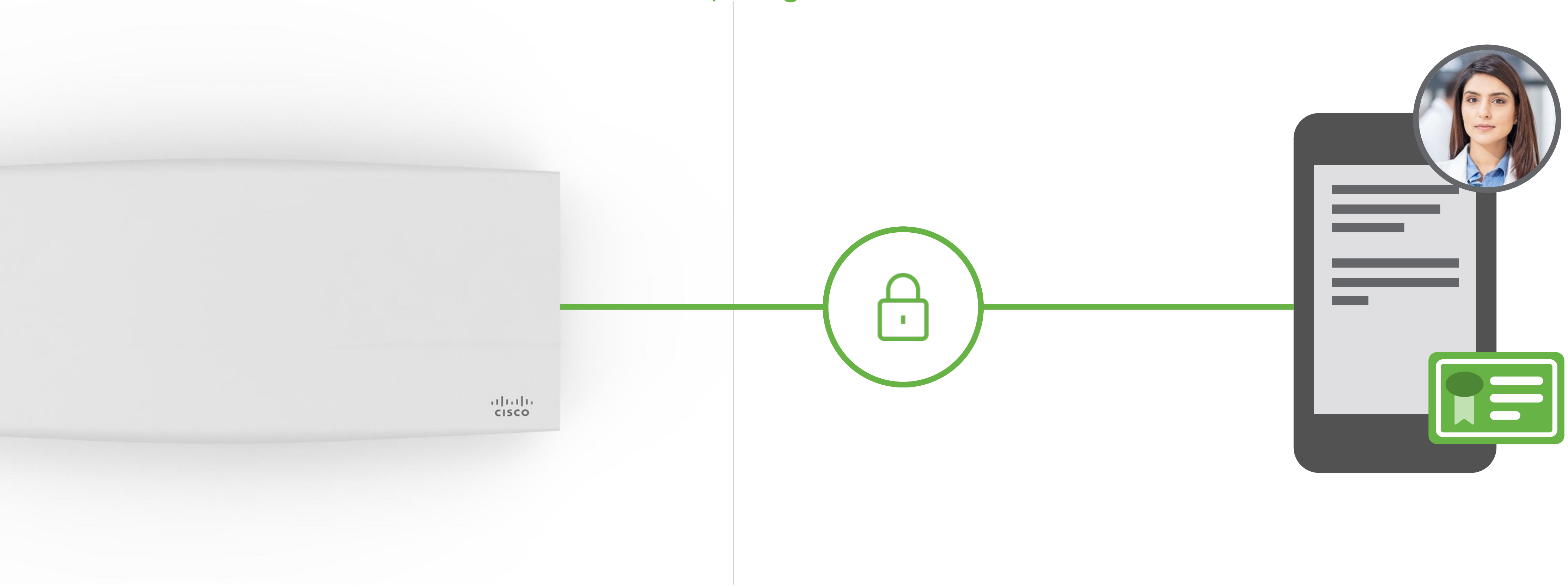
Cisco Clarity

Your last line of defense gives you visibility into network and device traffic.

Meraki

Meraki Trusted Access

Enables personal devices to access critical resources without requiring installation of an MDM



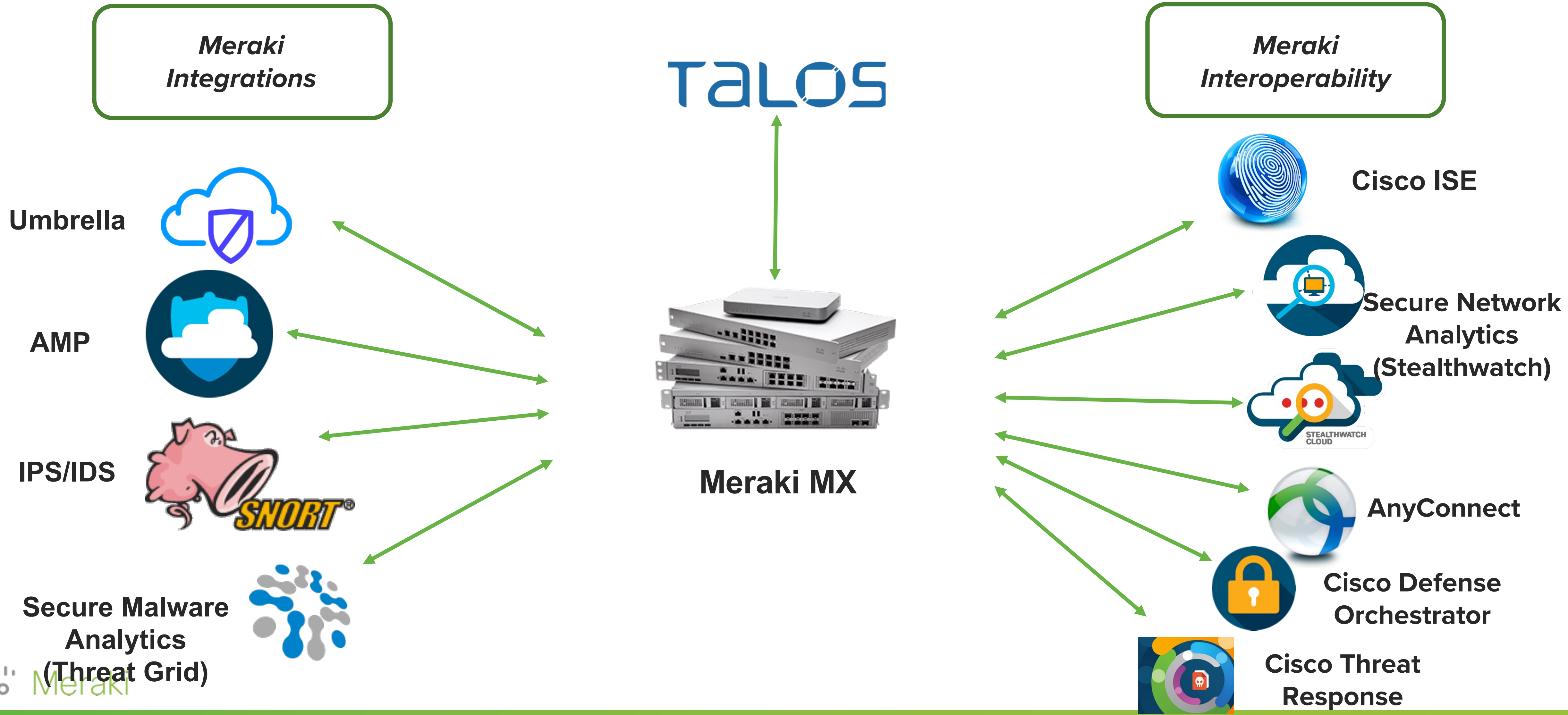
Systems Manager licensing

A complete enterprise feature set in a single product: SM

	SM Free Trial	Enterprise License
Annual cost	Free for 30 days	$40 / device
Complete feature set with ongoing updates	✓	✓
24/7 phone and email support	✓	✓

Cisco Integrations

Meraki MX integrations and interoperability



Meraki Integrations

Umbrella

AMP

IPS/IDS

Secure Malware Analytics (Threat Grid)

Meraki MX

Meraki Interoperability

Cisco ISE

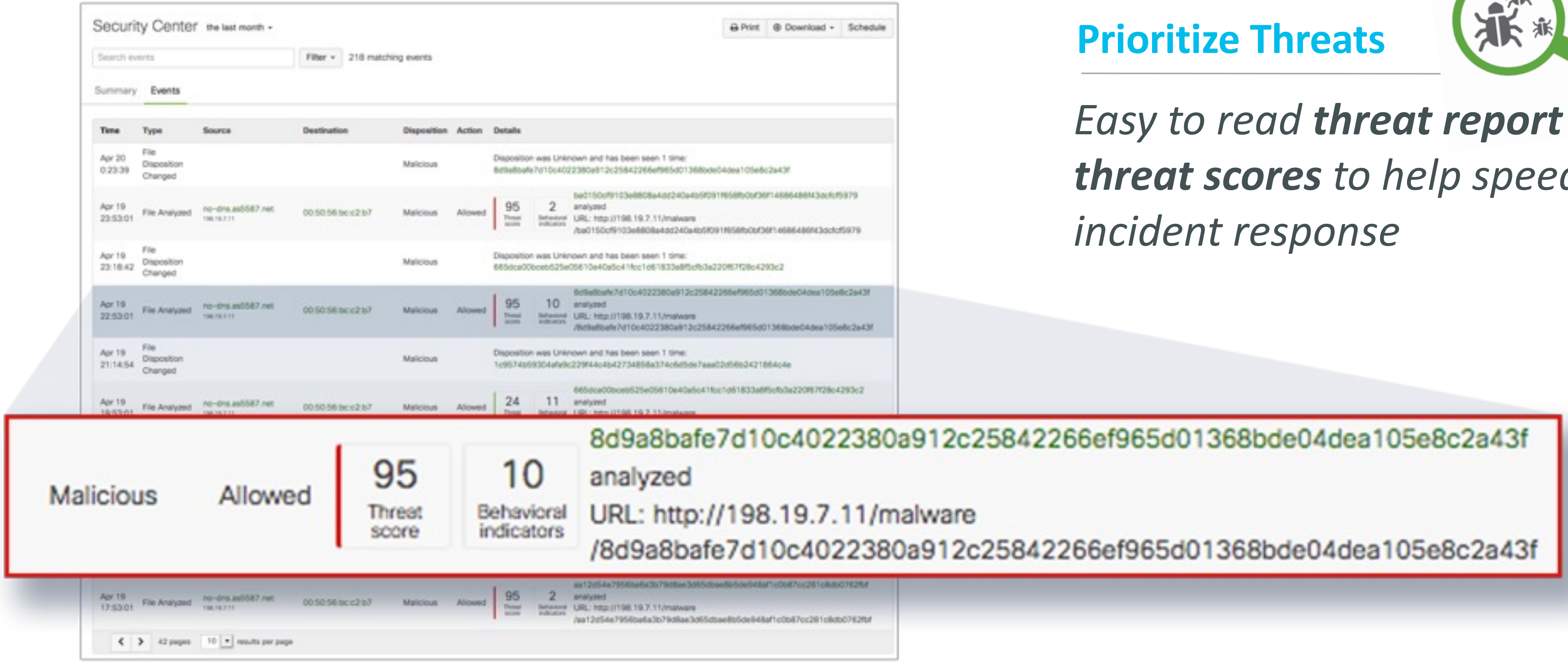
Secure Network Analytics (Stealthwatch)

AnyConnect

Cisco Defense Orchestrator

Cisco Threat Response

Threat Grid Cloud – Malware Analysis



Security Center the last month ▾

218 matching events

Time	Type	Source	Destination	Disposition	Action	Details
Apr 20 0:23:39	File Disposition Changed			Malicious		Disposition was Unknown and has been seen 1 time: 8d9a8bafe7d10c4022380a912c25842266ef965d01368bde04dea105e8c2a43f
Apr 19 23:53:01	File Analyzed	no-dns.as5587.net 198.19.7.11	00:50:56:bc:c2:b7	Malicious	Allowed	95 Threat score 2 Behavioral indicators ba0150cf9103e8808a4dd240a4b5f091f658fb0bf36f14686486f43dcfcf5979 analyzed URL: http://198.19.7.11/malware /ba0150cf9103e8808a4dd240a4b5f091f658fb0bf36f14686486f43dcfcf5979
Apr 19 23:18:42	File Disposition Changed			Malicious		Disposition was Unknown and has been seen 1 time: 665dca00bceb525e05610e40a5c41fcc1d61833a8f5cfb3a220f67f28c4293c2
Apr 19 22:53:01	File Analyzed	no-dns.as5587.net 198.19.7.11	00:50:56:bc:c2:b7	Malicious	Allowed	95 Threat score 10 Behavioral indicators 8d9a8bafe7d10c4022380a912c25842266ef965d01368bde04dea105e8c2a43f analyzed URL: http://198.19.7.11/malware /8d9a8bafe7d10c4022380a912c25842266ef965d01368bde04dea105e8c2a43f
Apr 19 21:14:54	File Disposition Changed			Malicious		Disposition was Unknown and has been seen 1 time: 1c9574b59304afa9c229f44c4b42734858a374c6d5de7aaa02d56b2421864c4e
Apr 19 19:53:01	File Analyzed	no-dns.as5587.net 198.19.7.11	00:50:56:bc:c2:b7	Malicious	Allowed	24 Threat score 11 Behavioral indicators 665dca00bceb525e05610e40a5c41fcc1d61833a8f5cfb3a220f67f28c4293c2 analyzed URL: http://198.19.7.11/malware
Apr 19 17:53:01	File Analyzed	no-dns.as5587.net 198.19.7.11	00:50:56:bc:c2:b7	Malicious	Allowed	95 Threat score 2 Behavioral indicators aa12d54e7956ba6a3b79d8ae3d65dbae8b5de948af1c0b87cc281c8db0762fbf analyzed URL: http://198.19.7.11/malware /aa12d54e7956ba6a3b79d8ae3d65dbae8b5de948af1c0b87cc281c8db0762fbf

< > 42 pages 10 ▾ results per page

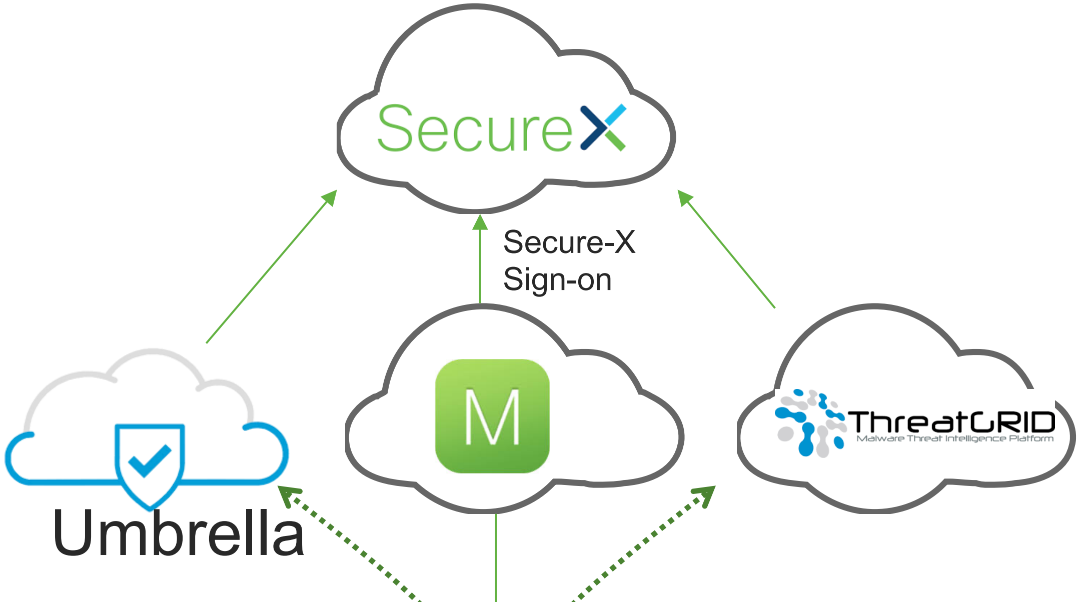
Malicious Allowed 95 Threat score 10 Behavioral indicators

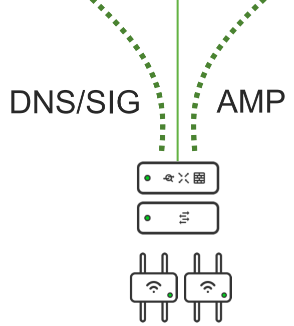
8d9a8bafe7d10c4022380a912c25842266ef965d01368bde04dea105e8c2a43f
analyzed
URL: http://198.19.7.11/malware
/8d9a8bafe7d10c4022380a912c25842266ef965d01368bde04dea105e8c2a43f

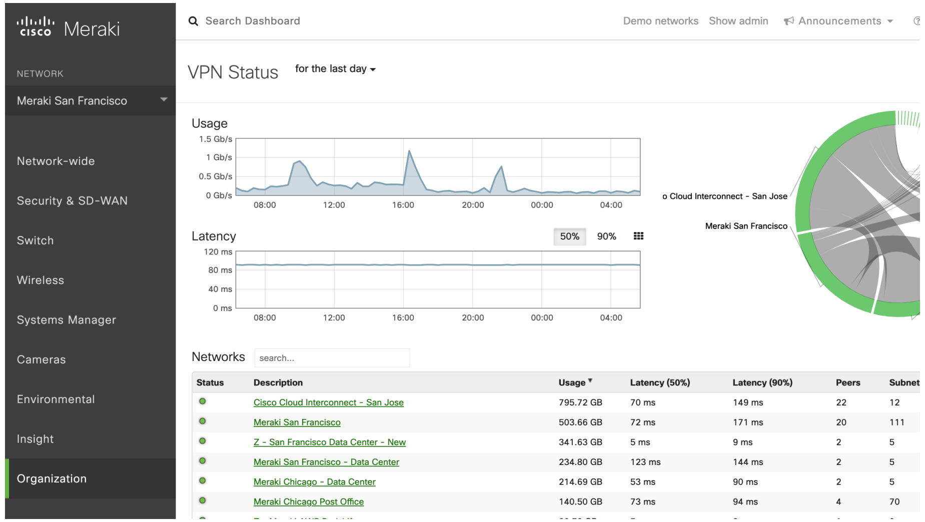
Prioritize Threats

*Easy to read **threat report** with **threat scores** to help speed up incident response*

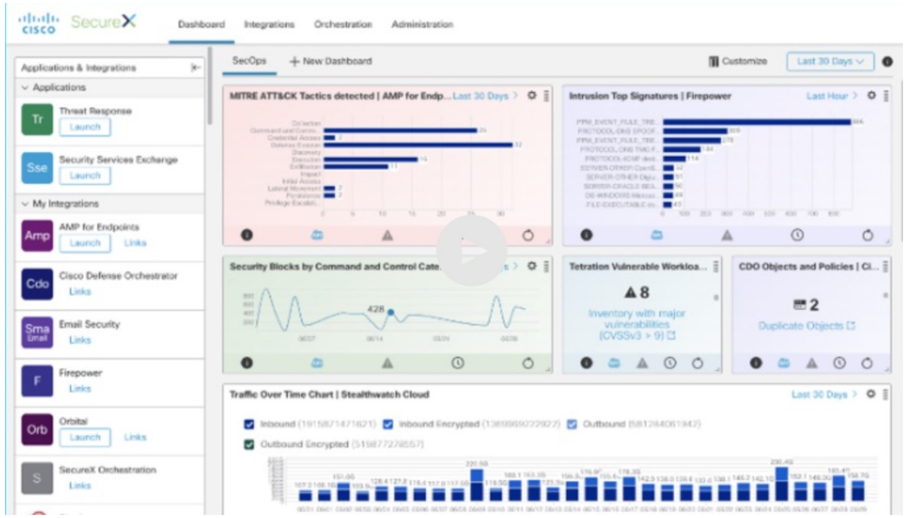
Secure-X







Status	Description	Usage ▾	Latency (50%)	Latency (90%)	Peers	Subnet
●	Cisco Cloud Interconnect - San Jose	795.72 GB	70 ms	149 ms	22	12
●	Meraki San Francisco	503.66 GB	72 ms	171 ms	20	111
●	Z - San Francisco Data Center - New	341.63 GB	5 ms	9 ms	2	5
●	Meraki San Francisco - Data Center	234.80 GB	123 ms	144 ms	2	5
●	Meraki Chicago - Data Center	214.69 GB	53 ms	90 ms	2	5
●	Meraki Chicago Post Office	140.50 GB	73 ms	94 ms	4	70

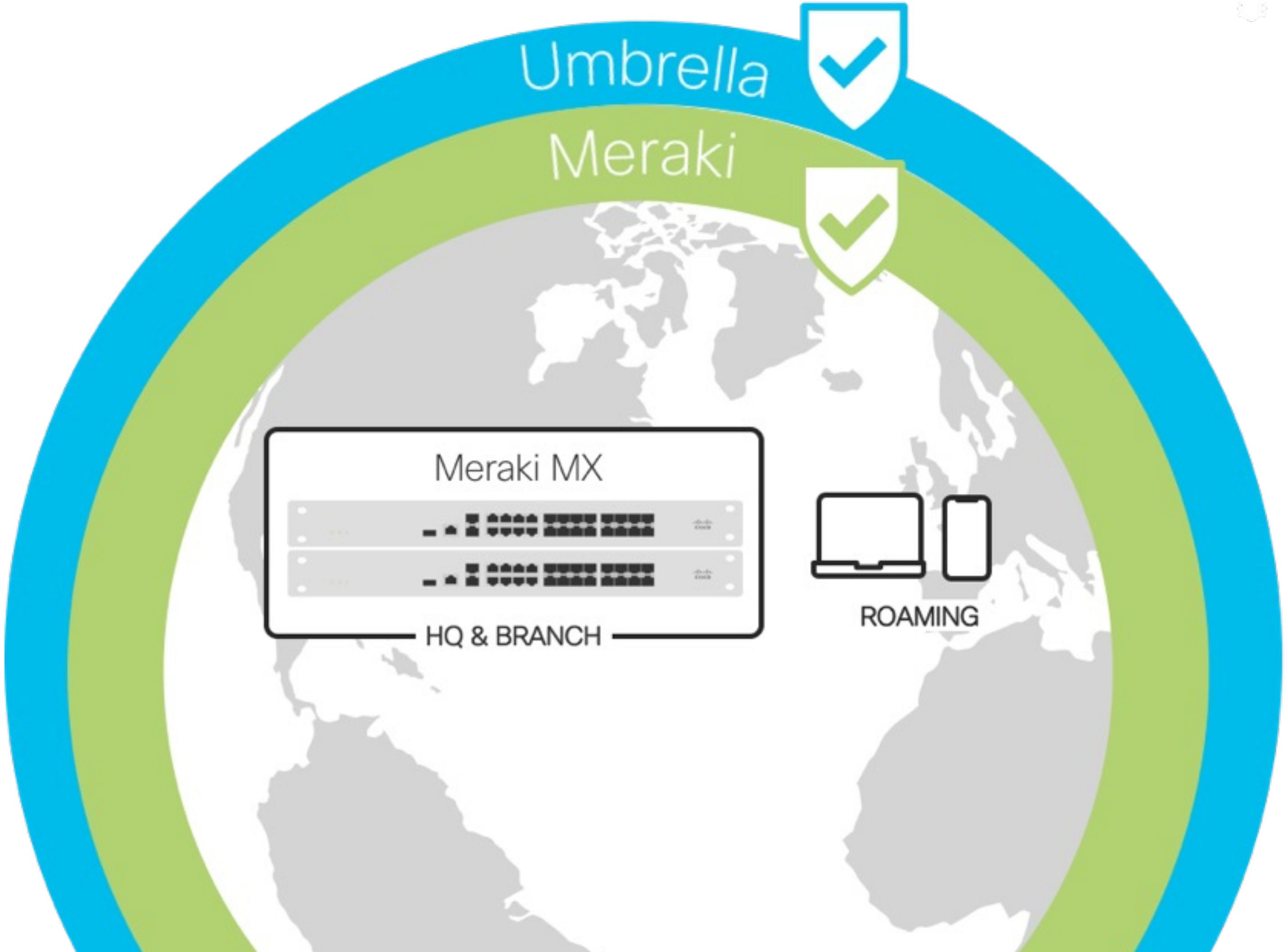


Dashboard for Network Team

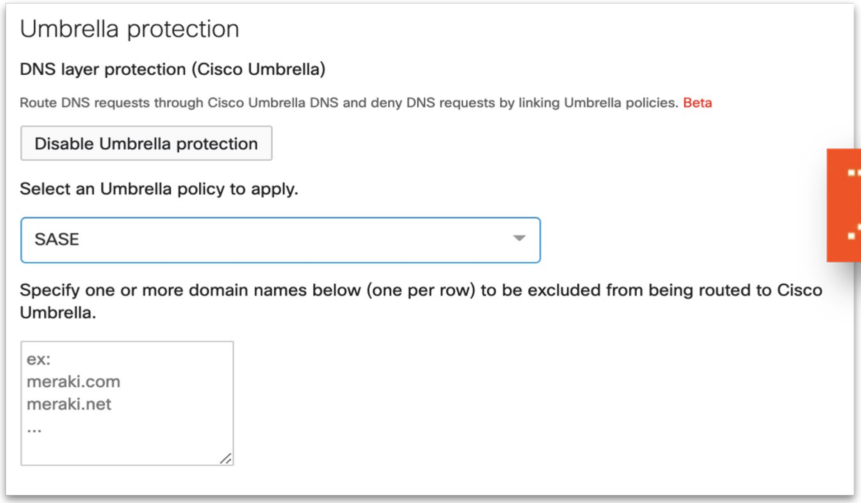
Dashboard for Security Team

Umbrella – DNS layer security*

Meraki + Umbrella Security



Umbrella policies applied per client/per VLAN from Meraki Dashboard



Umbrella protection

DNS layer protection (Cisco Umbrella)

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

Select an Umbrella policy to apply.

SASE

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

ex:
meraki.com
meraki.net
...

**MX15 firmware required*

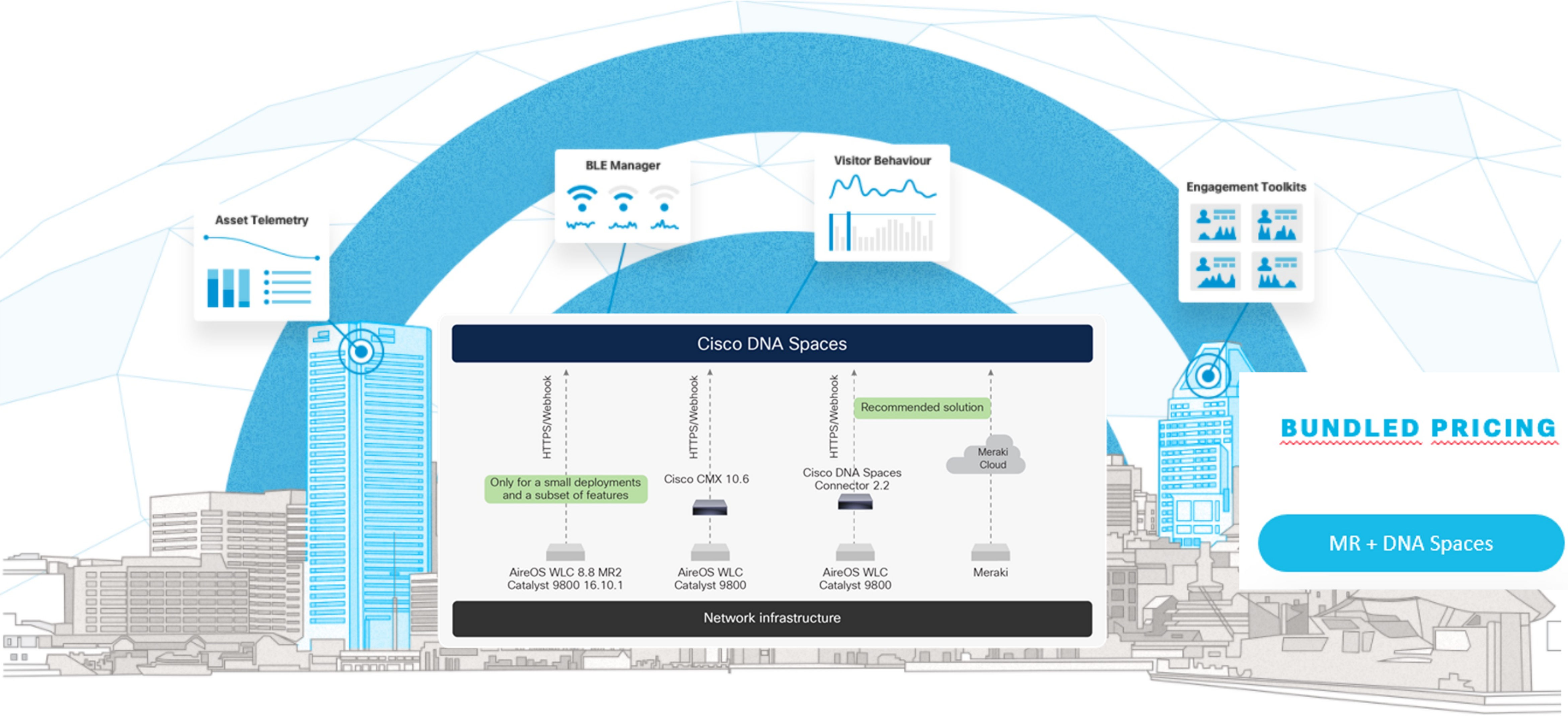
Meraki ISE Integration

Wired Network Access Control

Compatibility Matrix: https://community.cisco.com/t5/security-documents/how-to-integrate-meraki-networks-with-ise/ta-p/3618650

- Wired (MS)
  - Host Modes
  - Policy Types
  - Automated Segmentation
- Differentiators
  - Ease of Creating Access Policies
  - Ease of Deployment
  - Powerful workflows using API calls

Safe “Return to Work” with DNA Spaces + MR



BUNDLED PRICING

MR + DNA Spaces

Thank you!