



Meraki Security

SD-Wan, Meraki Gateway, Meraki Switch

Andrej Jeleník
Systems Engineer
Jun 2021

Meraki MX - One Unified Platform

Industry Leading SD-WAN
Meets Industry Leading Security



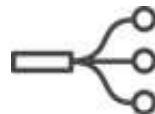
MX - Security and SD-WAN appliance

Feature highlights



Security

NG Firewall, Client VPN,
Site to Site VPN,
IDS/IPS, AMP



Networking

SD-WAN, 3G/4G Cellular,
Static/Dynamic Routing,
Link Balancing



Application Control

Traffic Shaping, Content
Filtering, Geo Firewall
Rules

A complete unified threat management solution

Appliance Models scaling from teleworker and small branch to campus /
datacenter

MX Portfolio

Teleworker



Z3

5 users
802.11ac Wave 2 Wireless & PoE
FW throughput: 100 Mbps
CAT 3 LTE (Z3C)



Z3C

Small Branch



MX64

~50 users
802.11ac Wireless*
FW throughput: 250 Mbps



MX67/68

~50 users
802.11ac **Wave 2*** & PoE
FW throughput: **450 Mbps**



MX67C/68CW

~50 users
802.11ac **Wave 2*** & PoE
FW throughput: **450 Mbps**
CAT 6 LTE

Medium/Large Branch



MX84

~200 users
FW throughput: 500 Mbps



MX100

~500 users
FW throughput: 750 Mbps

Campus or Concentrator



MX250

~2,000 users
FW throughput: 4 Gbps



MX450

~10,000 users
FW throughput: 6 Gbps

Virtual



**vMX for major
Public Clouds**
VPN & SD-WAN features

More information: <https://meraki.cisco.com/product-collateral/mx-family-datasheet?file>

NEW

MX Appliances

Cost-effective **gigabit**
SD-WAN branch connectivity

Available from 6 July 2021



RECOMMENDED USE

Small branch

WAN PORTS

x1 Gigabit Ethernet SFP
x2 Gigabit Ethernet RJ45

FIREWALL THROUGHPUT

1Gbps

SITE-TO-SITE VPN THROUGHPUT

500Mbps



RECOMMENDED USE

Small-medium branch

WAN PORTS

x2 Gigabit Ethernet SFP
x2 Gigabit Ethernet RJ45

FIREWALL THROUGHPUT

1Gbps

SITE-TO-SITE VPN THROUGHPUT

500Mbps



RECOMMENDED USE

Medium-large branch

WAN PORTS

x2 10 Gigabit Ethernet SFP+
x2 2.5 Gigabit Ethernet RJ45

FIREWALL THROUGHPUT

2Gbps

SITE-TO-SITE VPN THROUGHPUT

800Mbps



RECOMMENDED USE

Large branch

WAN PORTS

x2 10 Gigabit Ethernet SFP+
x2 2.5 Gigabit Ethernet RJ45

FIREWALL THROUGHPUT

3Gbps

SITE-TO-SITE VPN THROUGHPUT

1Gbps

A License For Every Use Case

1:1 ratio of devices to licenses. Pair your chosen MX appliance(s) with the relevant license for your use case.



Enterprise

Essential SD-WAN features

Secure connectivity & basic security



*All I need is Auto
VPN and a firewall*



Advanced Security

All enterprise features plus:

Fully featured
unified threat management



*I connect to the internet,
so I need UTM security too*



Secure SD-WAN Plus

All advanced security features plus:

Advanced analytics with ML
Smart SaaS quality of experience



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

A License For Every Use Case

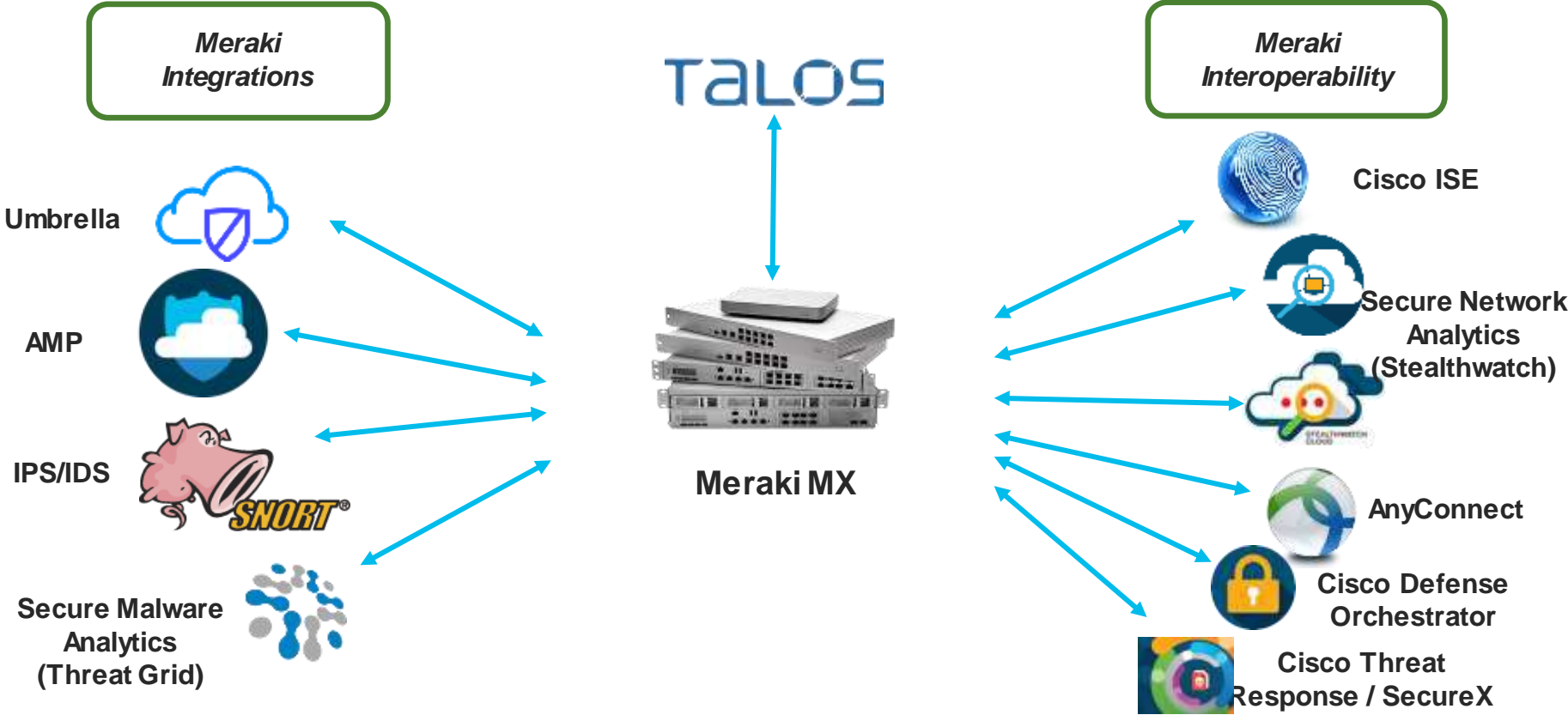
Features by License Option			
Feature	Enterprise	Advanced Security	Secure SD-WAN Plus
Centralized management	✓	✓	✓
Zero-touch firmware updates	✓	✓	✓
True zero-touch provisioning	✓	✓	✓
24x7 enterprise support	✓	✓	✓
Open APIs	✓	✓	✓
Automatic WAN failover	✓	✓	✓
Sub-second site-to-site VPN failover	✓	✓	✓
Sub-second dynamic path selection	✓	✓	✓
Stateful firewall	✓	✓	✓
VLAN to VLAN routing	✓	✓	✓
Advanced Routing	✓	✓	✓
Uplink Load Balancing/failover	✓	✓	✓
3G / 4G cellular failover	✓	✓	✓
Traffic shaping/prioritization	✓	✓	✓
Site-to-site VPN	✓	✓	✓
Client VPN	✓	✓	✓
MPLS to VPN Failover	✓	✓	✓
Splash pages	✓	✓	✓
Configuration templates	✓	✓	✓
Group Policies	✓	✓	✓

Client connectivity alerts	✓	✓	✓
Essential SD-WAN	✓	✓	✓
Source-Based Routing	✓	✓	✓
Local Breakout (IP based)	✓	✓	✓
Geography based firewall rules		✓	✓
Intrusion detection & prevention		✓	✓
Content filtering		✓	✓
Youtube for Schools		✓	✓
Web Search Filtering		✓	✓
Cisco Advanced Malware Protection (AMP)		✓	✓
Umbrella DNS Integration**		✓	✓
Threat Grid Integration**		✓	✓
Web App Health Analytics			✓
WAN Health Analytics			✓
VoIP Health Analytics			✓
Smart breakout			✓

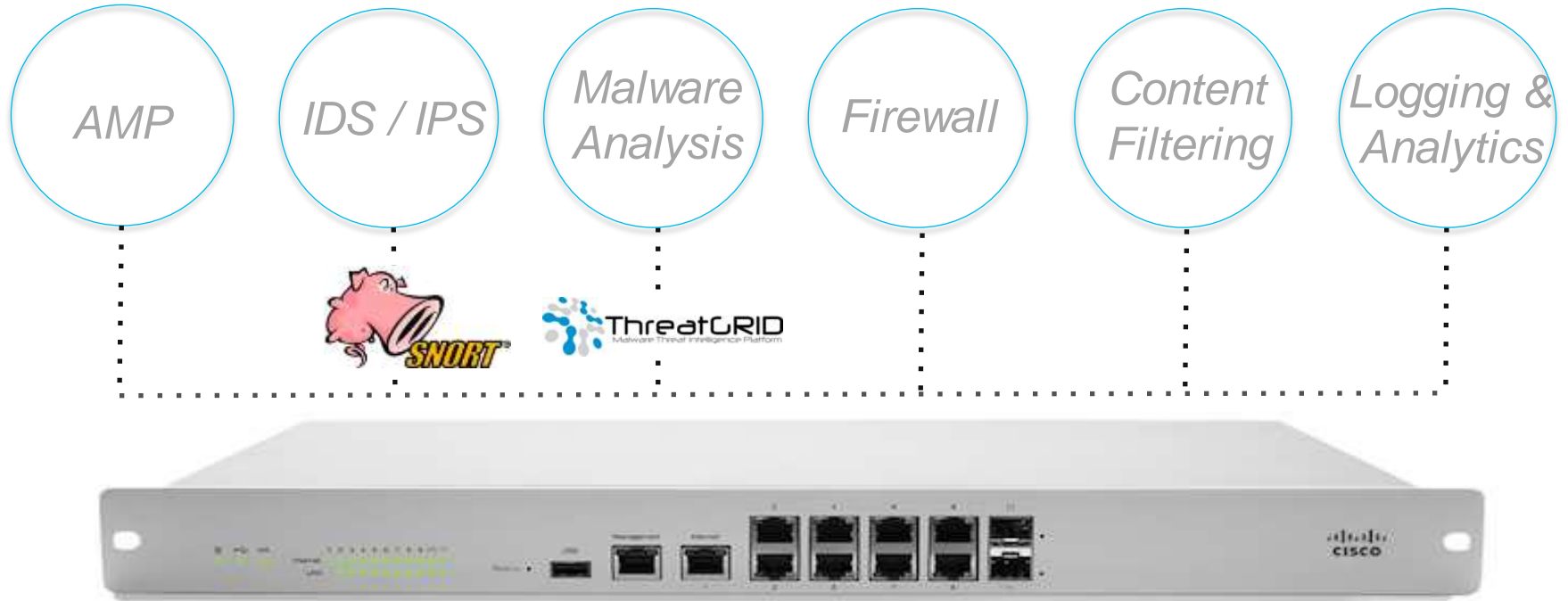
**Requires a separate license

More information: https://documentation.meraki.com/zGeneral_Administration/Licensing/Meraki_MX_Security_and_SD-WAN_Licensing

Meraki MX integrations



MX Advanced Security Features & Capabilities



Advanced Malware Protection for Meraki MX



Enhanced Threat Defense

Automatic protection against an ever-growing list of known malicious files, plus malware sandboxing with Threat Grid



Contextual Visibility

Security Center makes it easy to ensure you have the latest information about attacks on your network



Rapid Detection

Automatic alerting when a downloaded file is found to be malicious after the fact



Ease of Management

Enable best-in-class malware protection with just two clicks

- **220 million** known malicious files
- **407 million** known clean files
- **1.5 million** new incoming malware samples per day
- **1.6 million** devices using AMP globally
- **3.1 billion** lookup requests per day



Threat Grid Cloud – Malware Analysis

Prioritize Threats



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

Security Center the last month - Filter - 218 matching events

Summary Events

Time	Type	Source	Destination	Disposition	Action	Details
Apr 20 0:23:29	File Disposition Changed			Malicious		Disposition was Untrusted and has been seen 1 time: 809a8baf7d10c4022380a912c25842266ef965d01368bde04dea105e8c2a43f
Apr 19 23:52:01	File Analyzed	198.19.7.11	00:30:36:3c:27:a7	Malicious	Allowed	95 Threat score 2 Behavioral indicators URL: http://198.19.7.11/malware /8d9a8baf7d10c4022380a912c25842266ef965d01368bde04dea105e8c2a43f
Apr 19 23:18:43	File Disposition Changed			Malicious		Disposition was Untrusted and has been seen 1 time: 809a8baf7d10c4022380a912c25842266ef965d01368bde04dea105e8c2a43f
Apr 19 23:33:01	File Analyzed	198.19.7.11	00:30:36:3c:27:a7	Malicious	Allowed	95 Threat score 10 Behavioral indicators URL: http://198.19.7.11/malware /8d9a8baf7d10c4022380a912c25842266ef965d01368bde04dea105e8c2a43f
Apr 19 21:14:54	File Disposition Changed			Malicious		Disposition was Untrusted and has been seen 1 time: 1897a8935a9b623593a46a2734858a071a4b6e75ea2088d421884de
Apr 19 16:53:01	File Analyzed	198.19.7.11	00:30:36:3c:27:a7	Malicious	Allowed	24 Threat score 11 Behavioral indicators URL: http://198.19.7.11/malware /8d9a8baf7d10c4022380a912c25842266ef965d01368bde04dea105e8c2a43f

Malicious Allowed

95 Threat score

10 Behavioral indicators

8d9a8baf7d10c4022380a912c25842266ef965d01368bde04dea105e8c2a43f analyzed

URL: <http://198.19.7.11/malware/8d9a8baf7d10c4022380a912c25842266ef965d01368bde04dea105e8c2a43f>

Apr 19 17:53:01 File Analyzed 198.19.7.11 00:30:36:3c:27:a7 Malicious Allowed 95 Threat score 2 Behavioral indicators
URL: http://198.19.7.11/malware/8d9a8baf7d10c4022380a912c25842266ef965d01368bde04dea105e8c2a43f

42 pages 10 results per page

Intrusion Detection and Prevention (IDS/IPS)

Intrusion detection and prevention

Mode ⓘ

Ruleset ⓘ

Whitelisted rules ⓘ

Rule	Actions
<input type="button" value="MALWARE-OTHER self-signed SSL certificate with default Int..."/>	X

[Whitelist an IDS rule](#)

Prevention or Detection

Connectivity: contains rules from current and past two years and CVSS score of 10

Balanced: contains rules from current and past two years and CVSS score of 9 or greater

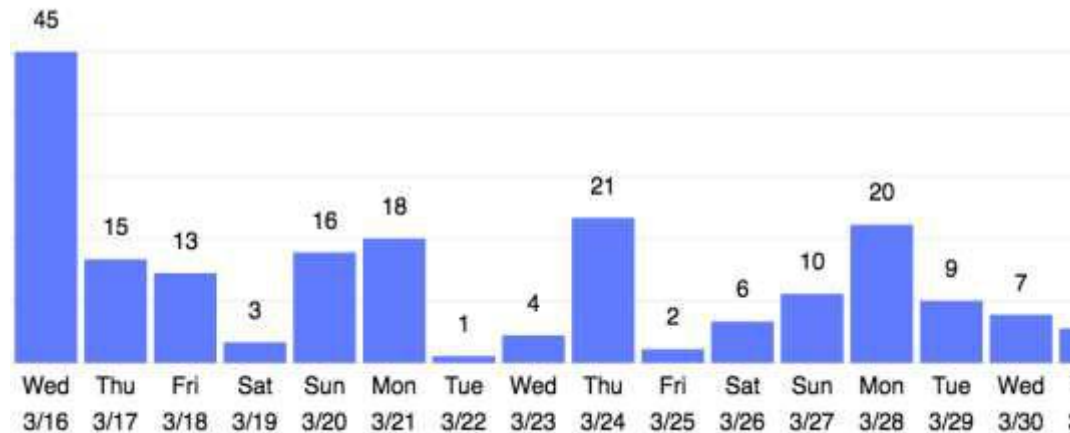
Security: contains rules from current and past three years and CVSS score of 8 or greater



Security Center

Events Over Time

Shows number of events matching configuring filters



Most Prevalent Threats

Detection of IDS/IPS signatures and scanned of blocked files through AMP

Threat	Occurrences
APP-DETECT Steam game URI handler	130
BROWSER-IE Microsoft Internet Explorer HTML DOM invalid DHTML texnode creation attempt	34
BROWSER-IE Microsoft Internet Explorer userdata behavior memory corruption attempt	12
FILE-FLASH Adobe Flash Player mp4 size memory corruption attempt	6
EXPLOIT-KIT Javascript obfuscation technique - has been observed in Rmayana/DotkaChef/DotCache exploit kit	2
BROWSER-PLUGINS Microsoft Windows Scripting Host Shell ActiveX function call access	2
FILE-FLASH Adobe Flash Player ActiveX URL import attempt	1

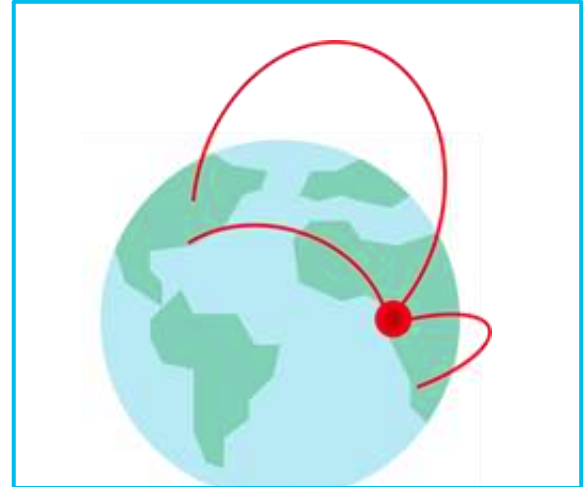
Intuitive, next-generation firewall capabilities



Application aware firewall



Content Filtering



Geo-IP based firewall

MX Network Objects

Consolidate firewall rules using logical groups and aliases

Layer 3

Inbound rules Inbound traffic will be restricted to the services and forwarding rules configured below.

Inbound firewall logging **Enabled** Disabled

Outbound rules

Search by policy, description, network object, etc.

#	Policy	Rule description	Protocol	Source	Src port	Destination	Dst port
1	Deny	Guest	Any	Guest	Any	Any	Any
2	Deny		TCP	Any	Any	Guest	Any
3	Allow		UDP	ATMs	Any	internal systems	6000-43007
4	Deny	Access to ATM	TCP	ATMs, internal systems		ATMs	Any
5	Deny	to d-fires	UDP	ATMs, internal systems		d-file system	Any

Site-to-Site Auto VPN in Three Clicks



Meraki Auto VPN

The ability to configure site-to-site, Layer 3 IPsec VPN tunnels in just three clicks in the Cisco Meraki dashboard over any WAN link

Automatically configured VPN parameters

The Cisco Meraki dashboard uniquely acts as a broker between MXs in an organization, negotiating VPN routes, authentication and encryption protocols, and key exchange automatically to create hub-and-spoke or mesh VPN topologies

Redundancy built-in

MXs with two uplinks will automatically self-heal to re-negotiate VPN tunnels if a primary uplink goes down

MX VPN Enhancements

- IKEv2 Encryption
 - Stronger Encryption
 - 3rd party VPN connectivity extended to more vendors that only supports IKEv2

Organization-wide settings

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

Note: Security appliances running firmware less than version 15.12 do not have support for IKEv2.

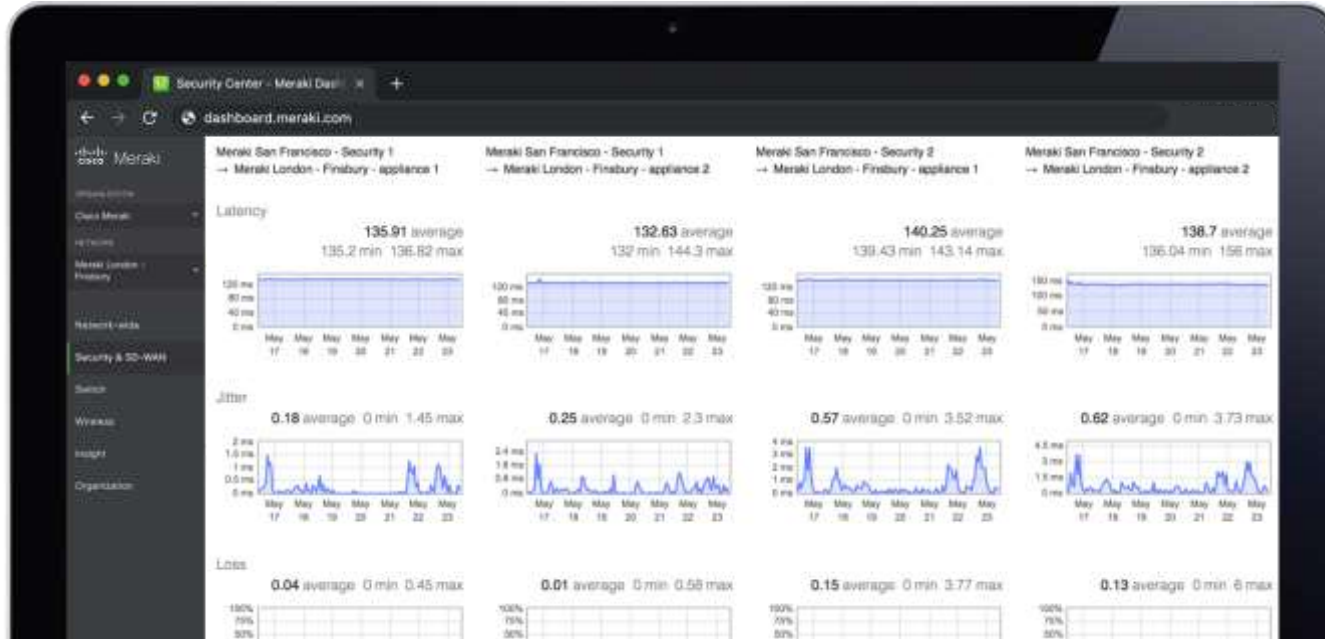
Non-Meraki VPN peers: 0

Name	IKE Version <small>BETA</small>	IPsec policies	Public IP	Local ID	Remote ID ⓘ	Private subnets	Preshared secret
<input type="text"/>	<input type="checkbox"/> IKEv1 <input checked="" type="checkbox"/> IKEv2	Default	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

[Add a peer](#)

Real-Time VPN Performance Monitoring

Latency | Jitter | Loss | MOS

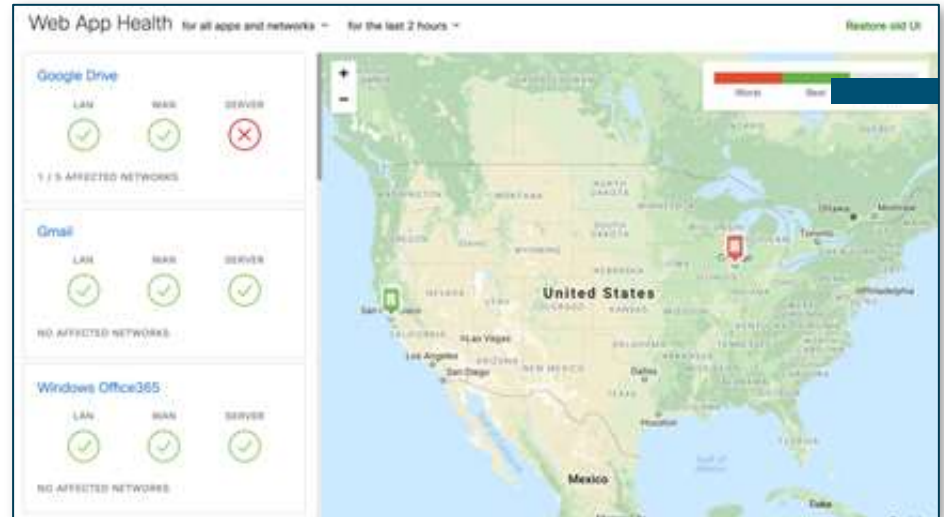




MI
Meraki Insight

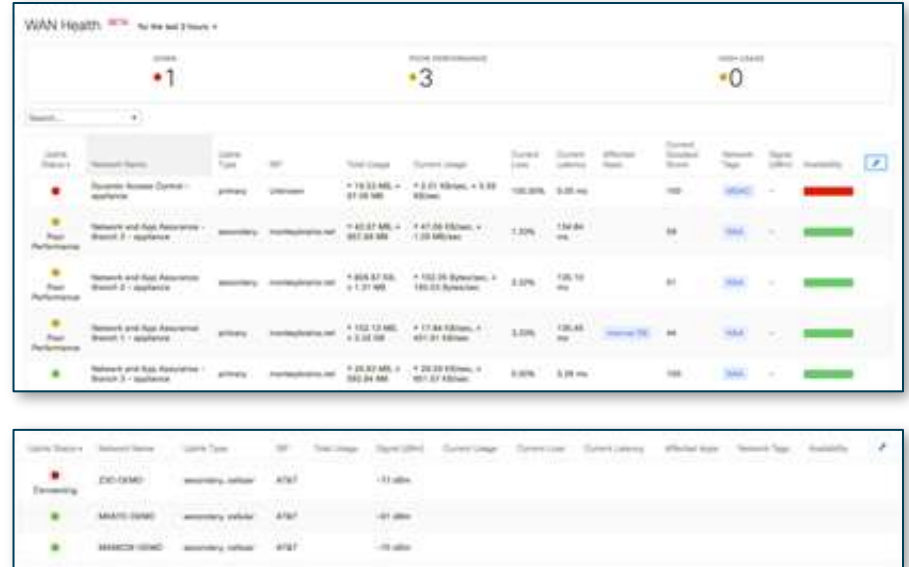
Web Application Health

- Monitor performance for apps travelling via **VPN or public Internet**
- **End-to-end** visibility for SaaS application experience
- Network performance analytics and troubleshooting, including the **LAN, WAN, servers and domains**
- Accelerate IT and **reduce time-to-resolution**



WAN Health

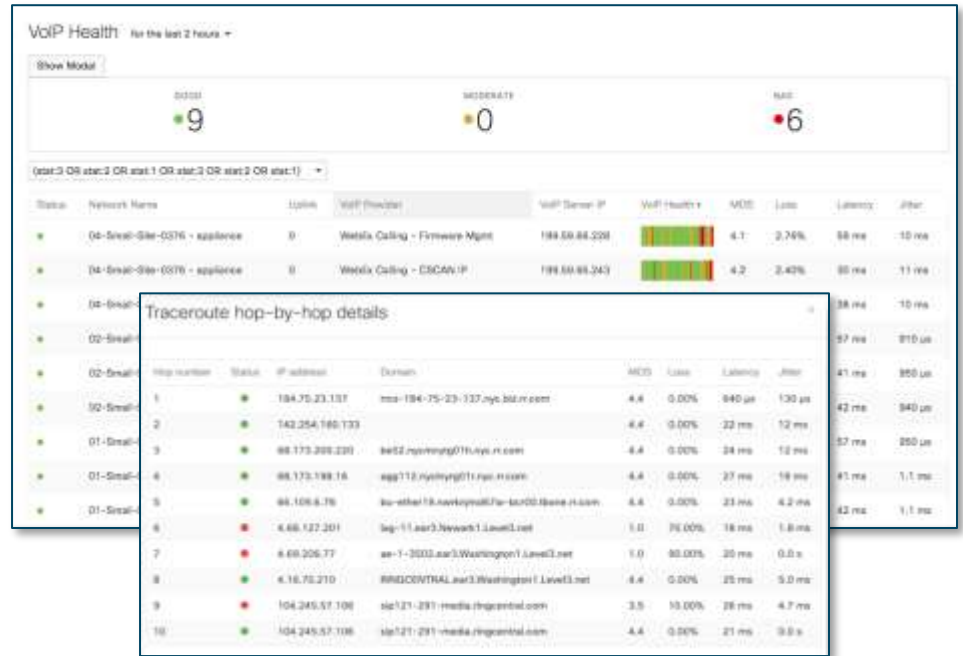
- At-a-glance **health of all MX uplinks across all sites**
- Quickly **identify downed uplinks**, including cellular, across all sites
- Easily monitor signal **strength for cellular uplinks** across all locations
- Quickly isolate sites with **underperforming uplinks** to make the case for switching ISP or adding cellular as failover
- **Discover** which sites are most reliant on cellular as failover



Monitor the health of all MX uplinks including cellular across all sites

VoIP Health

- Track the performance of **SaaS and on-prem based VoIP** services over all uplinks
- **Simple to set up** – add VoIP servers by domain name or IP addresses
- Quickly identify the cause of VoIP quality degradation through **detailed hop-by-hop analysis**
- Active monitoring of VoIP servers allows for **‘virtual’ PoC** for multiple vendors



MG

Meraki Cellular Gateway

The simplest path to wireless WAN



Unlocks the potential of wireless WAN



Precision placement for optimal cellular signal strength



Pair with any router to deliver failover or primary cellular support

The MG21 and MG21E



- Integrated CAT6 modem with up to 300Mbps
- DC / PoE power in
- **2x Ethernet ports for HA**
- Nano SIM card slot
- **IP67 rated**
- Multi-surface mounting bracket (wall, ceiling, and tabletop)
- **LTE connectivity out-of-the-box**
- **External antennas***
 - Dipole included
 - Patch available as an accessory
- **API support**

*Available on MG21E model

NEW

MG

Cellular Gateway

Agile **gigabit** cellular connectivity

Available from 6 July 2021

MG41



THROUGHPUT

1.2Gbps download
150Mbps upload

POWER

PoE
DC

SIM

Dual physical SIM

BANDS

Full coverage including FirstNet band 14

WEATHERPROOFING

IP67

ANTENNA

Internal and external models

MG41E



Connectivity Statistics

The screenshot displays the Meraki dashboard interface. On the left is a navigation sidebar with sections for Organization, Network, and Cellular. The main content area is titled '#hot-cats' and includes a map, address, and cellular status. The 'Configuration' section is expanded to show details for General, Cellular, and Live data.

Organization: Simple IT Solutions

Network: SF Office - Headqu...

Cellular: 500 Terry A. Francois 04158

Cellular Status: 199.116.75.195 **Active**

Hostname: mg21-yumtyumyun.dynamic-m.com

Serial Number: Q3XX-AAAA-ZZZZ

IMEI: 35911223445566

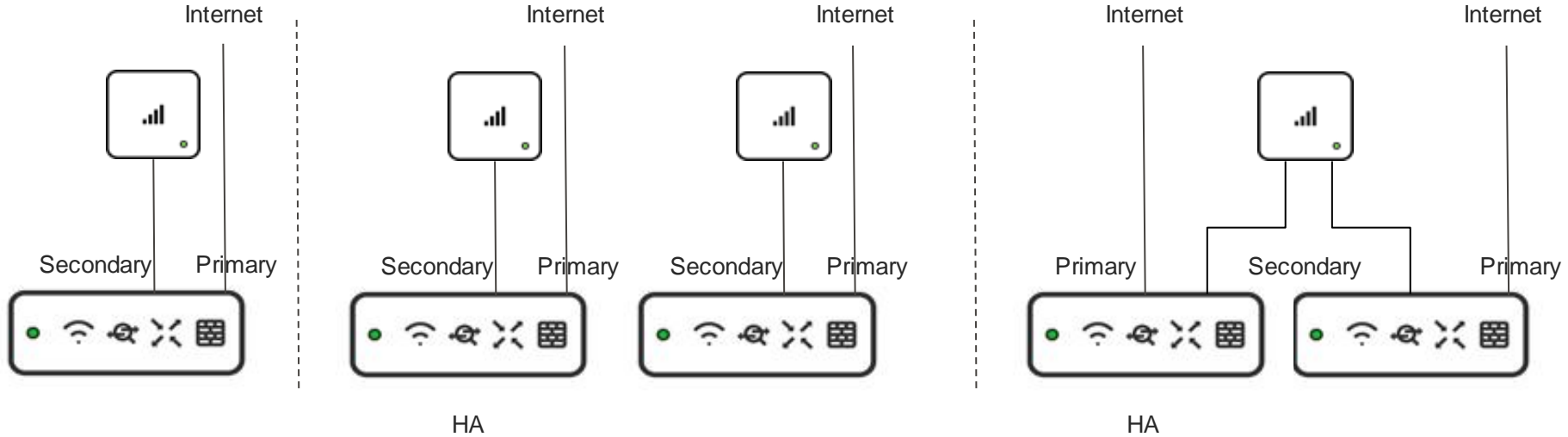
Configuration:

- General:**
 - PUBLIC IP: 199.116.75.195
 - 199-116-75-195.public.monkeybrains.net
- Cellular:**
 - STATUS: Active
 - IP: 100.86.110.143
 - GATEWAY: 100.99.222.1
 - DNS: 8.8.8.8, 8.8.4.4
 - TYPE: 4G
 - STRENGTH: Excellent
 - PROVIDER: AT&T
 - ICCID: 8914800000430866668
 - APN: broadband
- Live data:** This device may need additional configuration on the local status page. [More information here.](#)

Historical Signal Visibility

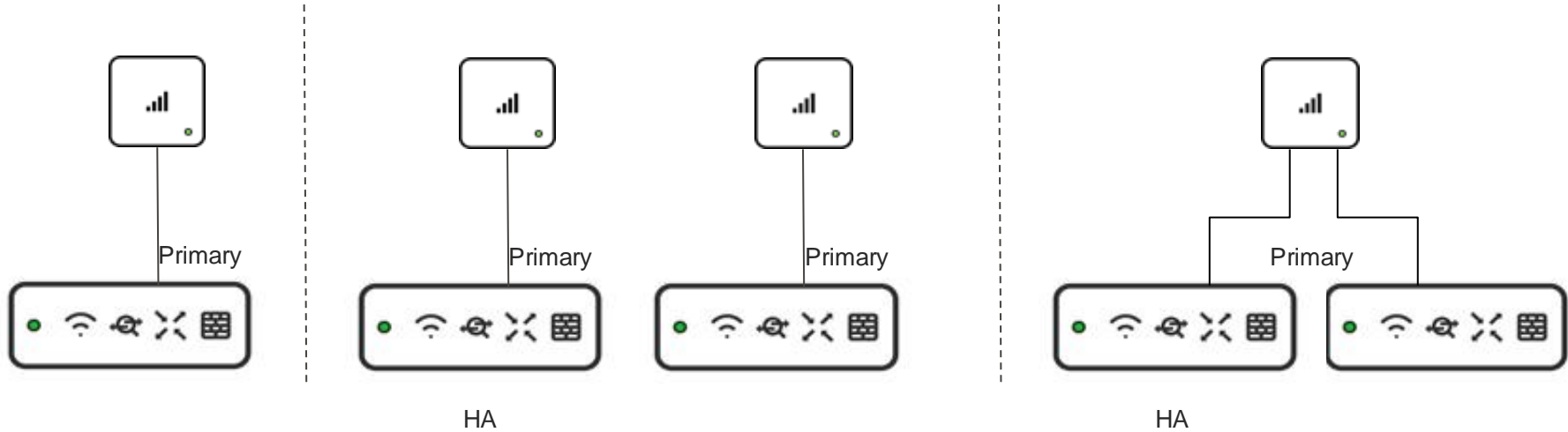


Target Topology: LTE Failover



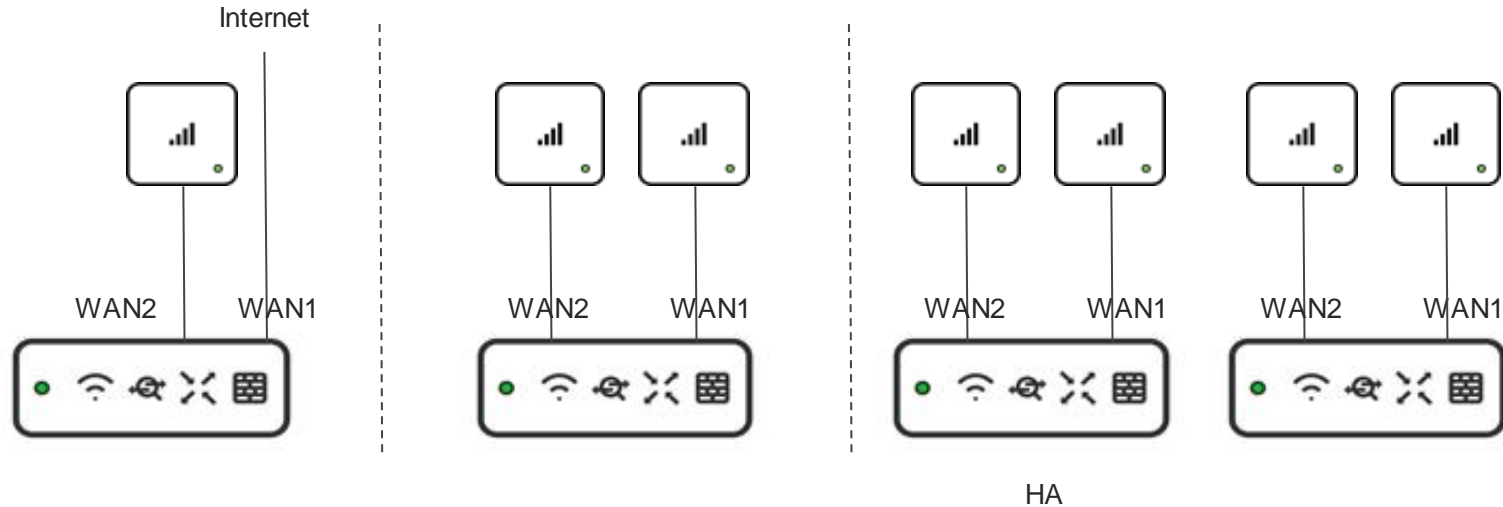
- Failover to LTE in case of Primary WAN outage
- Connect MG to any MX Secondary WAN interface
- Support any 3rd-party router downstream
- Failover decision lies within the router not MG

Target Topology: LTE Primary



- Put MG where LTE signal coverage is optimal
- Connect MG to any MX Primary WAN interface
- Support any 3rd-party router downstream

Target Topology: SD-WAN over LTE



- Support following combinations: Internet-LTE, LTE-LTE
- Connect MG(s) to any MX
- Support any 3rd-party router downstream
- SD-WAN policies are configured on downstream router

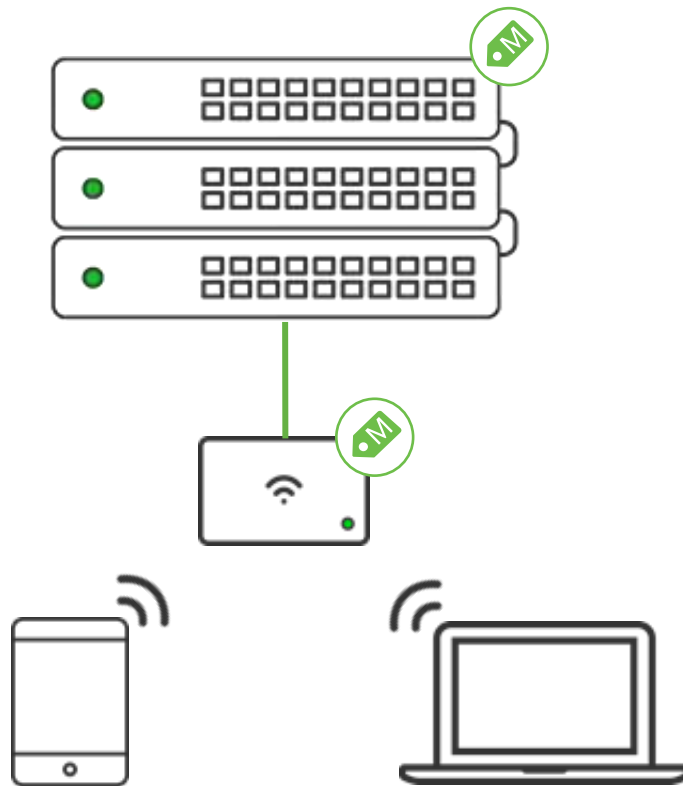
Adaptive Policy

Hardware Requirements:

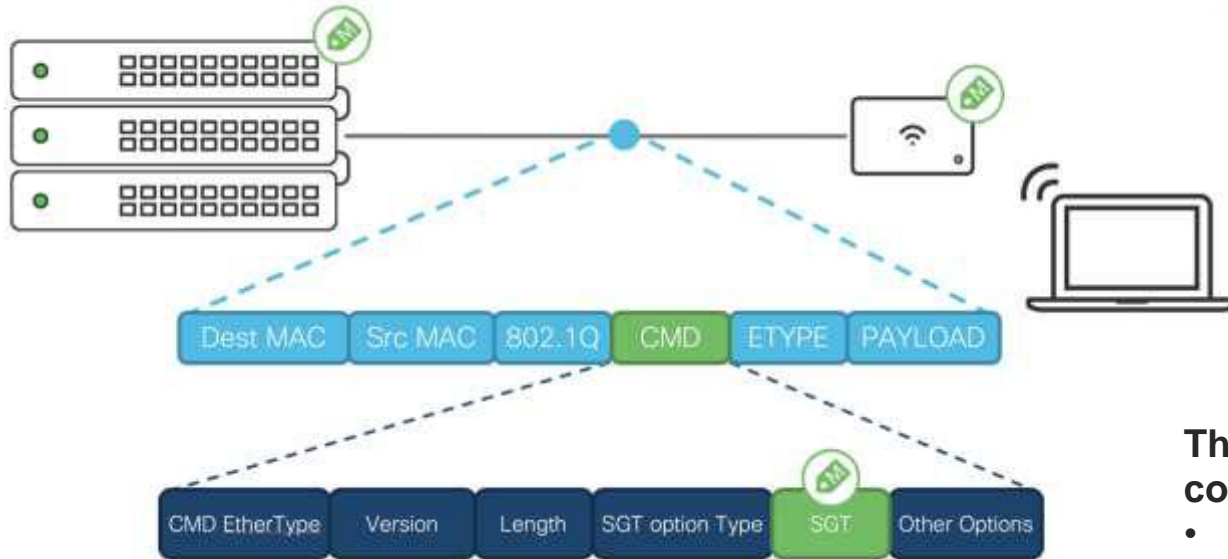
- MS390: all models
- MR: all 802.11ac Wave 2 (Wifi-5) and up excluding MR20 and MR70

Software Requirements:

- MS390: 14 +
- MR: 27 +



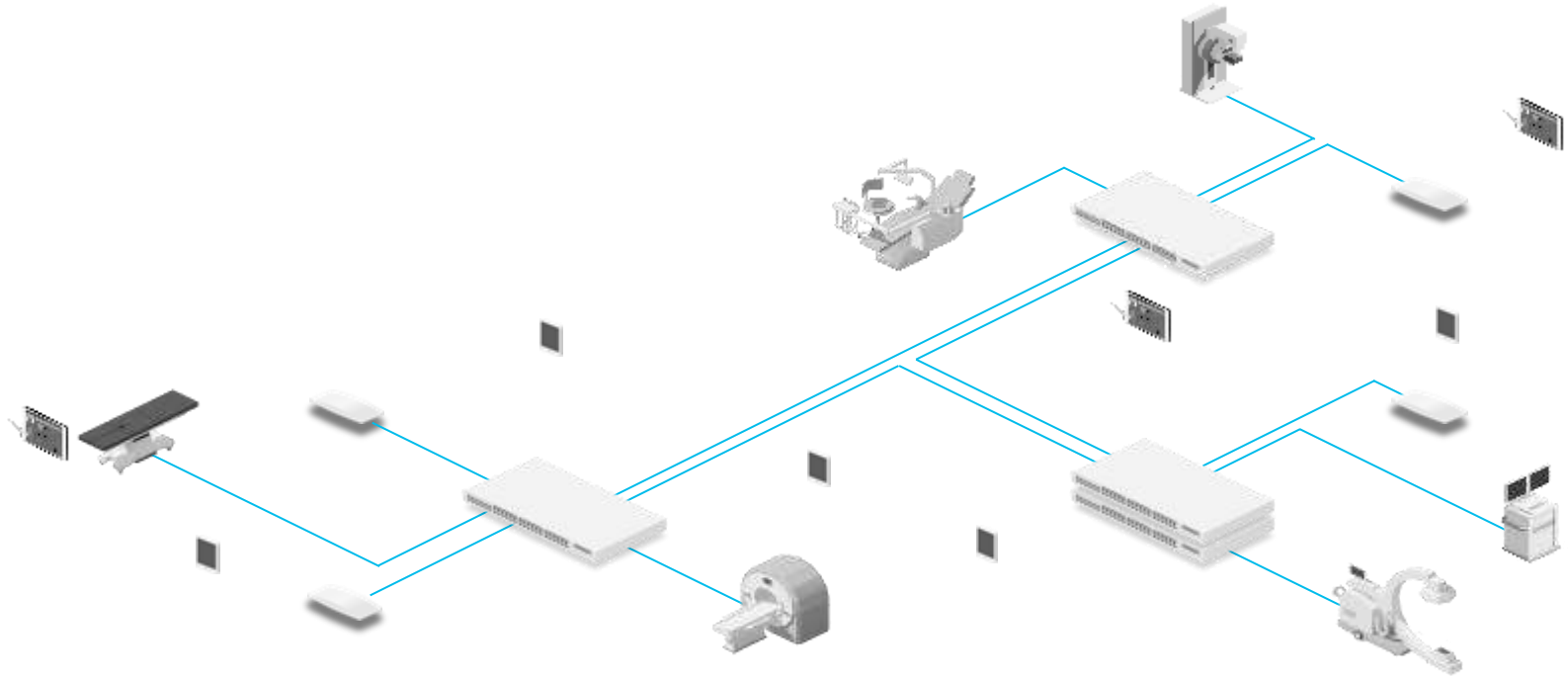
Adaptive Policy



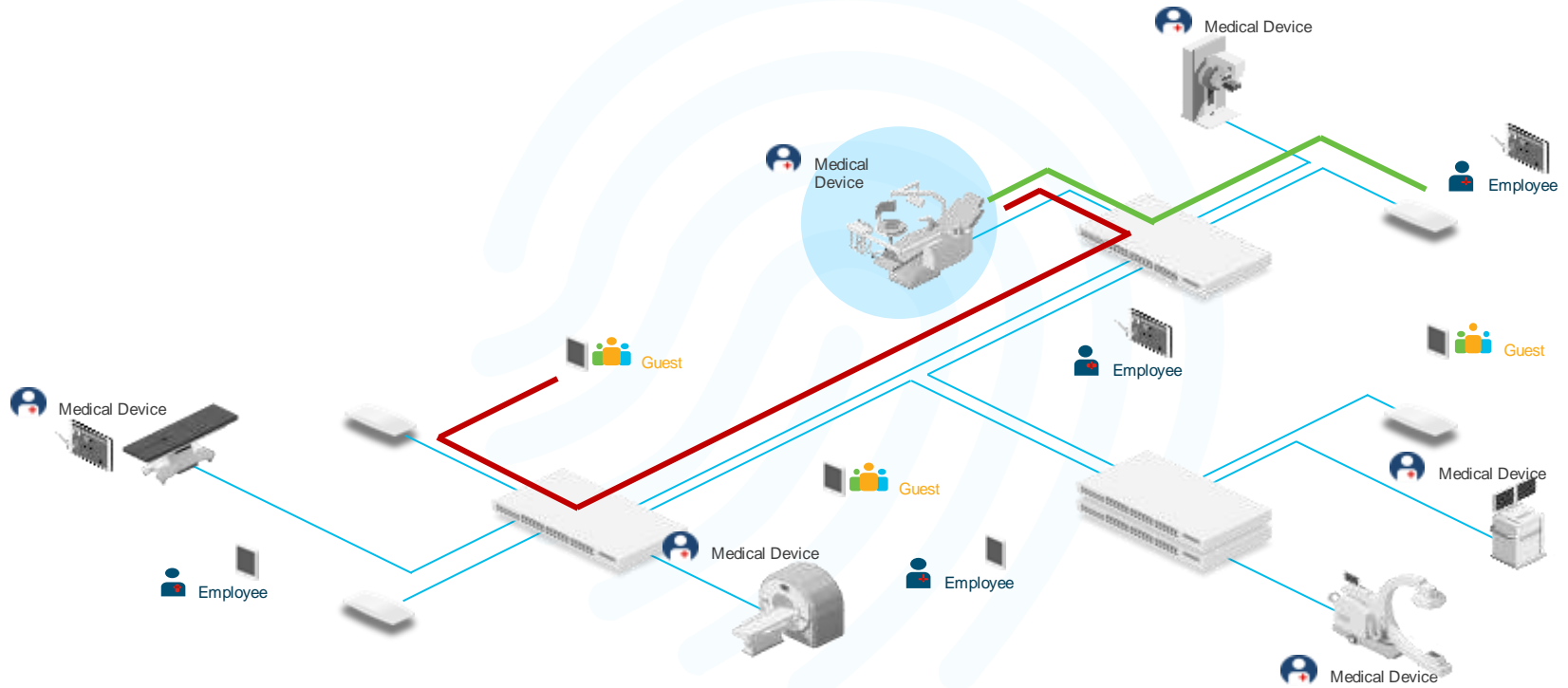
The security policy 3 components:

- Source group (SGT)
- Destination group (SGT)
- Permissions between the groups

Example Architecture: Healthcare



Example Architecture: Healthcare



Policy Configuration between Two Tags

Configure Adaptive Policies

You are making changes to following policies:

Source Group	Destination Group	Custom ACLs	Last-entry Rule
IOT_Device : 10	IOT_Servers : 11		allow all

Configure ACLs

Configure custom ACLs on selected policies. Note if multiple policies are selected, changes made here will overwrite existing ACLs.

#	ACL Name	Description	Rules	Actions
1	MQTT	MQTT Ports	<code>allow tcp src: any, dst: 1883;</code> <code>allow tcp src: any, dst: 1894;</code>	
Last-entry Rule		Will apply as the last ACL entry	Deny	

[Add an entry](#)

[Review changes](#)

The application of a policy is as simple as selecting the source group tag, the destination group tag, and then applying a permission such as Allow or Deny, or selecting custom.

Custom ACLs

The screenshot shows the 'Add adaptive policy ACL' configuration window. The 'Name' field is filled with 'My First Custom ACL'. The 'Description' field is empty. Under 'IP Version', the 'IPv4' radio button is selected. The 'Rules' section contains a table with three entries:

#	Priority	Policy	Protocol	Src port	Dst port	Actions
1	1	Allow	UDP	Any	55	---
2	2	Deny	TCP	Any	80	---
3	3	Allow	TCP	Any	443	---

Below the table is an 'Add ACL Rule' button. At the bottom right of the window are 'Cancel' and 'Create' buttons.

- Create granular security rules with up to 16 ACE entries per custom ACL
- Up to 10 custom ACLs per tag-to-tag association
- Custom ACLs can be referenced in multiple associations



Novinky ze světa cloudové platformy Cisco Meraki
Part 2

Milan Rášo
Systems Engineer

- Meraki Wireless
- Meraki Health
- Meraki MT - Senzory
- Meraki MV - Kamery

Next generation wireless landscape



More devices



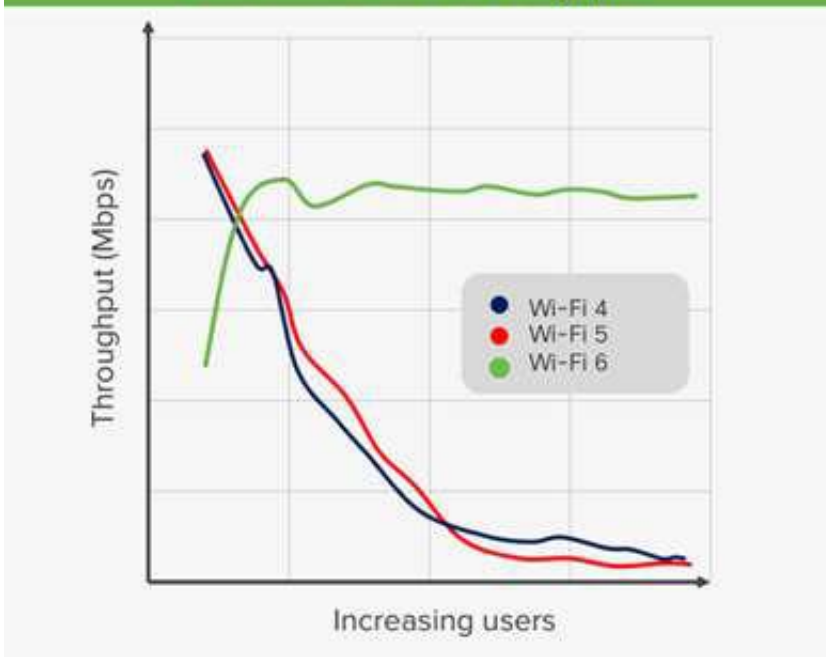
Enhanced experiences



IoT growth

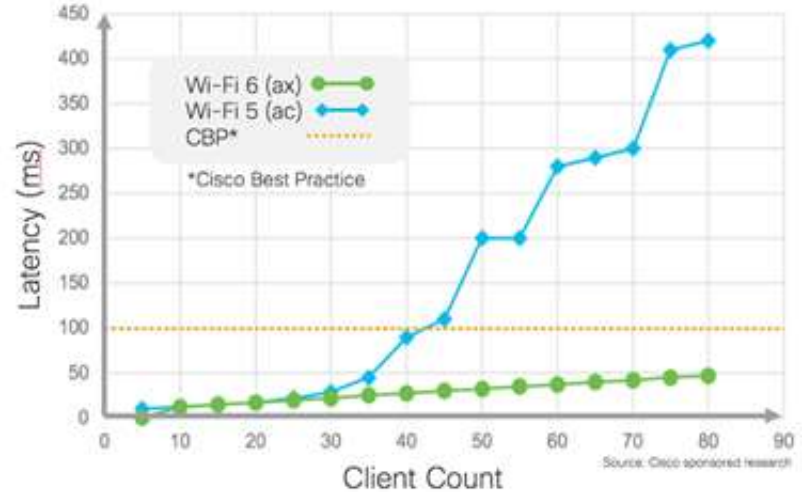
Previous Wi-Fi standards failing at high density

Consistent data throughput



Source: Cisco sponsored research

Linear voice delay



Source: Cisco sponsored research

Wi-Fi 6 key technologies



Backwards compatible

So any legacy clients can connect on both 2.4 and 5G bands



MU-MIMO

Simultaneously communicate with up to 8 clients optimizing high throughput traffic



OFDMA

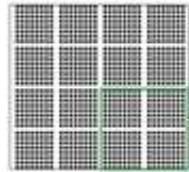
A 20 MHz channel can be split into 9 resource units of 2 MHz to optimize IOT-style small traffic



8x8

More transmit and receive antennas offer high throughput and reliability

802.11ax 1024 QAM



1024 QAM

Sends 37% more traffic over 802.11ac Wave-2 similar to having more pixels on your TV



BSS Color

Lowers co-channel interference and saves battery life



Target Wakeup Time

AP Schedules wake-up calls to clients lowering air contention and saves battery life

Wi-Fi 6 clients are mainstream



Apple
iPhone 11 & 12



Samsung
Galaxy Fold



Samsung
Galaxy S10 & S10E



Samsung
Galaxy Note 10

Meraki wireless

High Performance



MR36

2 Stream, 4-Radio

Medium Density,
High Performance



MR44

4 Stream (5GHz),
2 Stream (2.4GHz),
4-Radio, mGig

High Density,
High Performance



MR46/E

4 Stream, 4-Radio,
mGig, external
antenna

Ultra High Density
Ultra High Performance



MR56

8 Stream, 4-Radio,
mGig

High
Performance



MR76

2 Stream, 4-Radio




















High Density,
High Performance



MR86

4 Stream, 4-Radio,
mGig

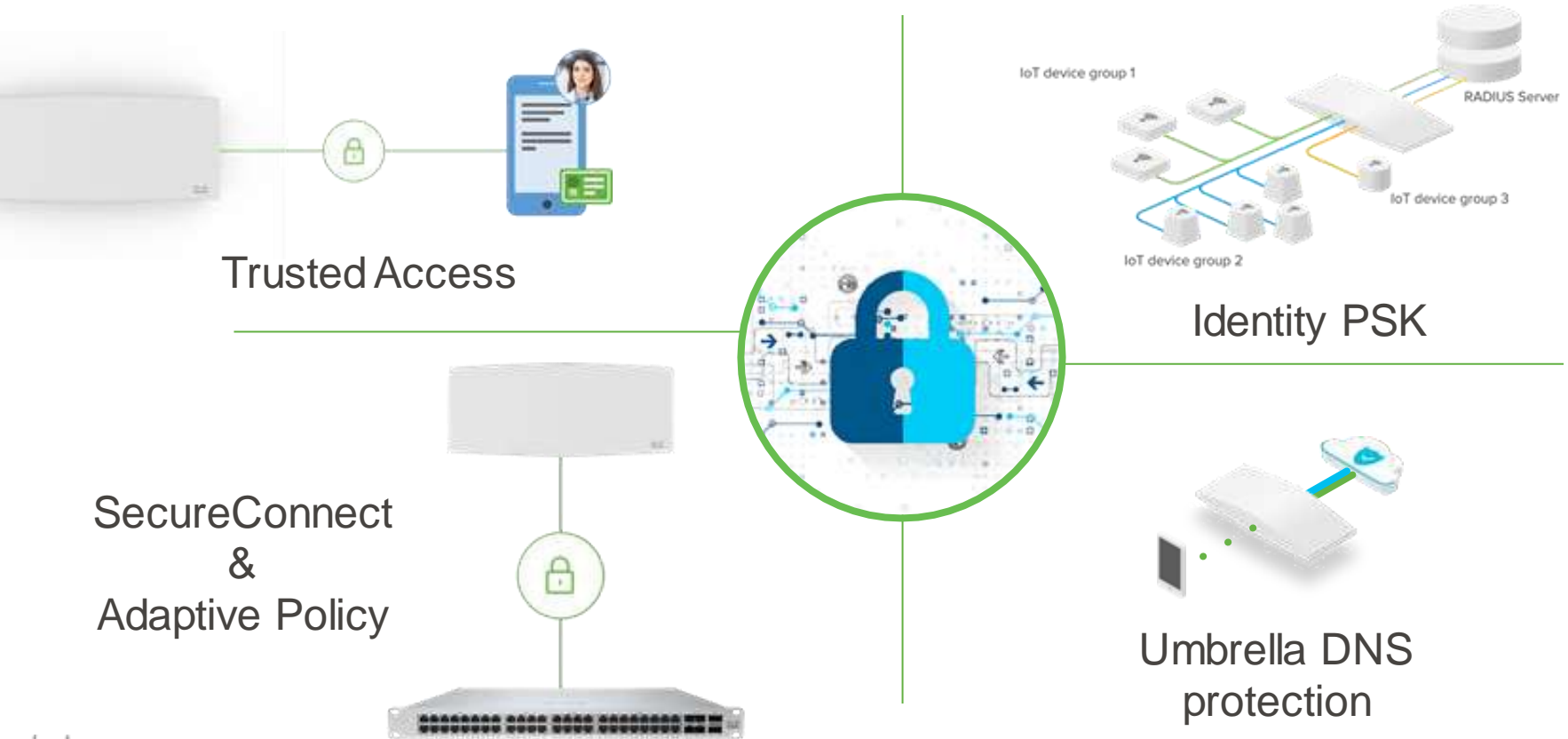
Wi-Fi 5 Portfolio – EoS with exceptions

	Hospitality	Entry	General Purpose		High density		
Indoor	 <p>MR30H </p> <p>2 Stream, 4-Radio 802.11ac Wave 2 4-port switch 1 PoE-out port</p>	 <p>MR20</p> <p>2 Stream, 2-Radio 802.11ac Wave 2</p>	 <p>MR33 </p> <p>2 Stream, 4-Radio 802.11ac Wave 2</p>	 <p>MR42 </p> <p>3 Stream, 4-Radio 802.11ac Wave 2</p>	 <p>MR42E </p> <p>4 Stream, 4-Radio 802.11ac Wave 2, Multigigabit</p>	 <p>MR52 </p> <p>MR53 </p> <p>4 Stream, 4-Radio 802.11ac Wave 2, Multigigabit</p>	 <p>MR53E </p>
Outdoor		 <p>MR70</p> <p>2 Stream, 2-Radio 802.11ac Wave 2</p>	 <p>MR74 </p> <p>2 Stream, 4-Radio 802.11ac Wave 2</p>		 <p>MR84 </p> <p>4 Stream, 4-Radio 802.11ac Wave 2, Multigigabit</p>		

4-Radio = 2.4GHz & 5GHz client serving radios, dual-band scanning radio, BLE radio

Security

Automating security for wireless

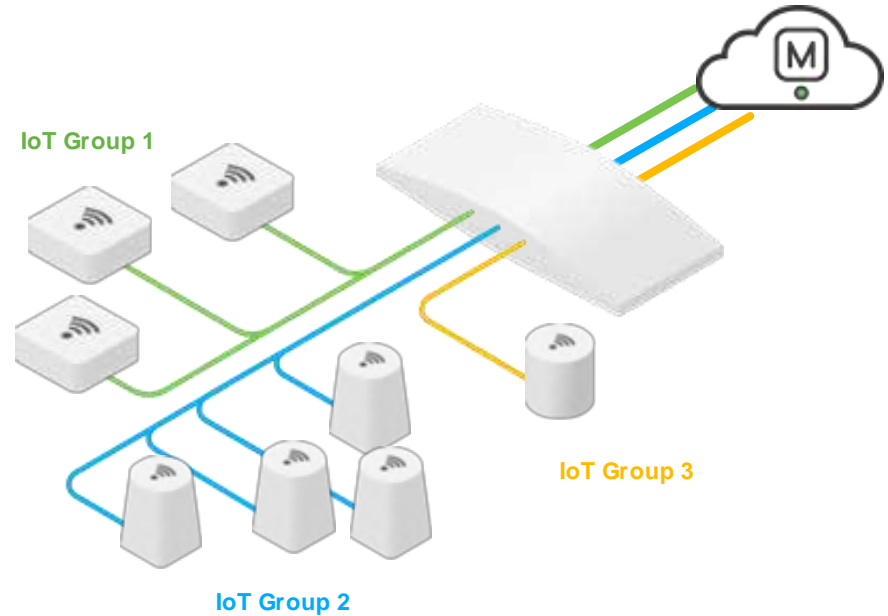


INTRODUCING

Identity PSK

Unique policies per group of IoT devices on a single SSID

Enabled with MR Devices



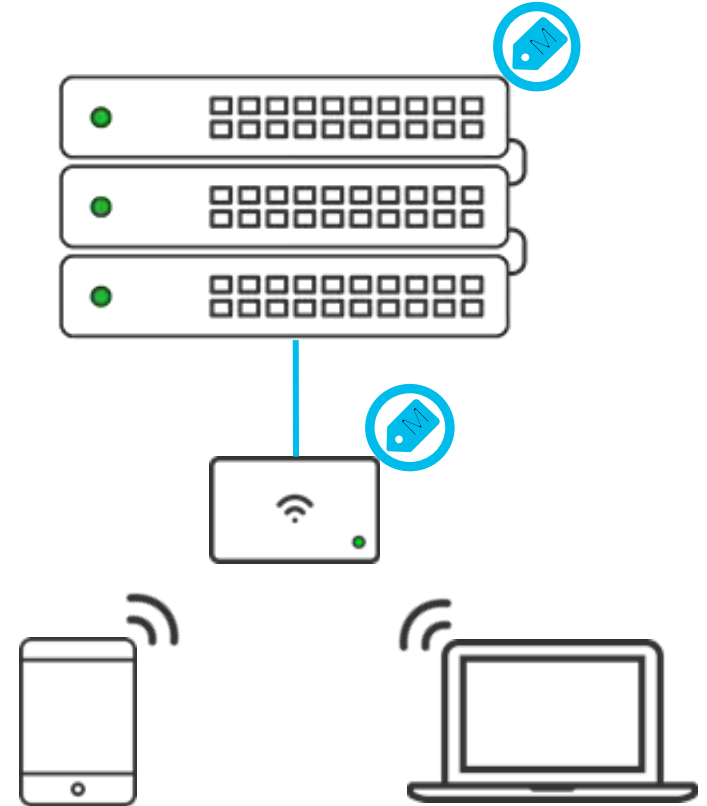
iPSK can now be used with either RADIUS based implementation or using Meraki Dashboard based on the use case.
iPSK with RADIUS was released with MR26.7

Adaptive Policy

Tag based identity and policy enforcement

- Utilize Security Group Tags to identify traffic source and destination
- Organization wide access control policy based on business intent
- Micro-segmentation
- Tags can be assigned via:
 - Static SSID mapping
 - Dynamic RADIUS response
 - Static IP Subnet to SGT mappings
- Supported on:
 - All Meraki 802.11ac wave 2 and Wi-Fi 6 MR APs
 - All Meraki MS390 switching platforms

Available with MR Advanced License Only



Umbrella + Meraki: A Match Made in the Cloud

- Simplest way to deploy Umbrella across a wireless network
- Conveniently enable Umbrella policies directly in the Meraki dashboard
- Create granular policies on a per-SSID basis or by using Meraki group policies



Umbrella + Meraki MR



Meraki MR licensing



Enterprise License

Full Wireless feature set and functionality

Meraki Health

L7 visibility

Location analytics

Application control

Auto RF

SecureConnect

Identity based firewall

Advanced License

All enterprise features, plus:

Umbrella DNS Security integration

Adaptive Policy*

[* When combined with compatible switch]

Meraki Health end-to-end assurance



Meraki Health

INTRODUCING

Client Performance
Ability to gauge performance
with the client's view along with
color coding to provide context.



Meraki

INTRODUCING

Health

Access Point Performance
Ability to gauge performance
with the Access Points' view
along with color coding to
provide context.



Meraki Health

INTRODUCING

Client Timeline

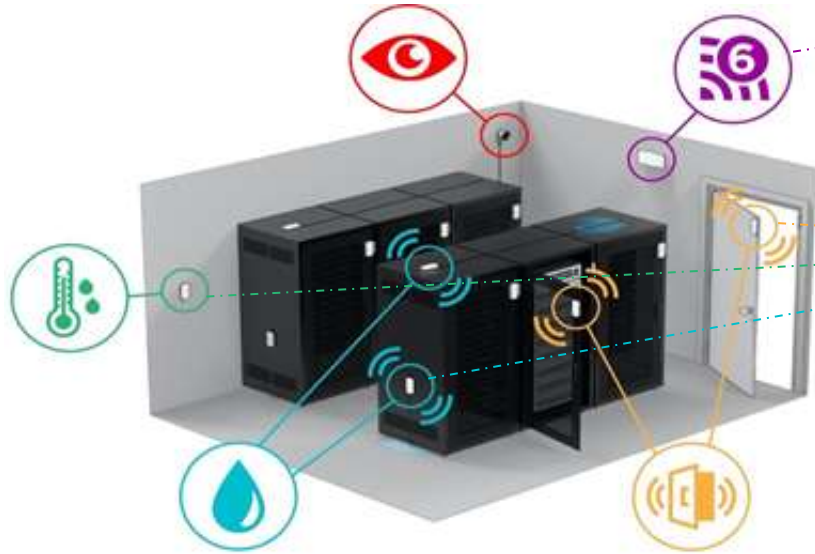
Client timeline provides an easy to understand summary of events that happened during the client's journey throughout the network.

Customers can filter events using severity.

The screenshot displays the Meraki Health Client Timeline interface. At the top, there are filters for SSID (set to 'AP'), AP (set to 'AP 100'), RADIUS (set to '2.2 & 3.3'), RADIUS ATOP (set to 'All connections'), and FAILURE SEVERITY (set to 'All severities'). The main area shows a list of events, each with a timestamp and a description of the connection attempt. The events are as follows:

- Apr 3, 3:18 PM**: Successful connection to SSID **SSC_Wifi** for 14 minutes on AP **Green-Village_KC_112**. TIME TO CONNECT: 401 ms, RADIUS SERVER: 23 ms, 10:28:02:78.
- Apr 3, 4:14 PM**: Successful connection to SSID **SSC_Wifi** for a few seconds on AP **Green-Village_KC_112**. TIME TO CONNECT: 561 ms, RADIUS SERVER: 18 ms, 10:28:02:78.
- Apr 3, 4:39 PM**: Successful connection to SSID **SSC_Wifi** for 12 minutes on AP **Green-Village_KC_112**. TIME TO CONNECT: 590 ms, RADIUS SERVER: 22 ms, 10:28:02:78.
- Apr 3, 1:00 PM**: Failed connection to SSID **SSC_Wifi** on AP **Green-Village_KC_305** during authentication because the password was incorrect. Includes details: SSID: SSC_Wifi, RADIUS SERVER: 28 ms, 10:28:02:78, and a note that the SSID password was reconfigured. A link is provided to check the SSID password configuration.
- Apr 3, 10:00 AM**: Successful connection to SSID **SSC_Wifi** for 2 minutes on AP **Green-Village_KC_112**. TIME TO CONNECT: 349 ms, RADIUS SERVER: 25 ms, 10:28:02:78.
- Apr 3, 1:04 PM**: Successful connection to SSID **SSC_Wifi** for 5 minutes on AP **Green-Village_KC_112**. TIME TO CONNECT: 9454 ms, RADIUS SERVER: 19 ms, 10:28:02:78.
- Apr 3, 1:28 PM**: Successful connection to SSID **SSC_Wifi** for 23 minutes on AP **Green-Village_KC_112**. TIME TO CONNECT: 5331 ms, RADIUS SERVER: 17 ms.
- Apr 3, 12:23 PM**: Successful connection to SSID **SSC_Wifi** for 4 minutes on AP **Green-Village_KC_112**. TIME TO CONNECT: 250 ms, RADIUS SERVER: 20 ms, 10:28:02:78.
- Apr 3, 11:17 AM**: Failed connection to SSID **SSC_Wifi** on AP **Green-Village_KC_112** during authentication. Includes details: SSID: SSC_Wifi, AUTHENTICATION FAILURE ERROR CODE: 15, and RADIUS SERVER: 24 ms, 15.

Seamless analytics of environmental data

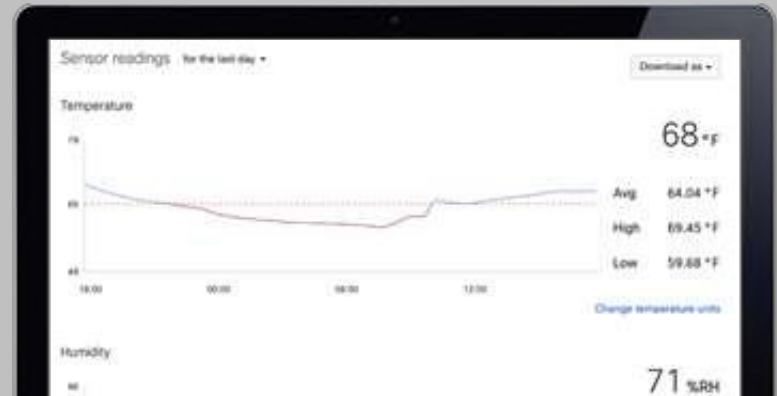


Meraki MR
Gateway



Meraki MT
Sensor

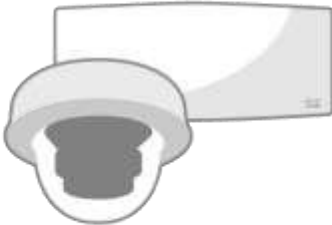
NEW



An all-in-one solution



Bluetooth® Low Energy (BLE) Connectivity



Cloud management



MT sensors

MR / MV gateway

Meraki dashboard

Powered by the **Meraki platform**

Meraki **sensors** (MT)



Meraki MT10

Temperature & humidity sensor



Meraki MT11

Temperature probe sensor



Meraki MT12

Water leak sensor



Meraki MT20

Door open/close
(intrusion) sensor



Five-year battery



Bluetooth® Low Energy



Five days of on-board
data storage



Proactive alerting

Built with **security** in mind



Protected by
Trust Anchor module
(TAm)



Certificate-
based
authentication



Encrypted
by default



Secure OTA
updates

Ecosystem Ready

Access **current** or **historical** sensor readings via **API**

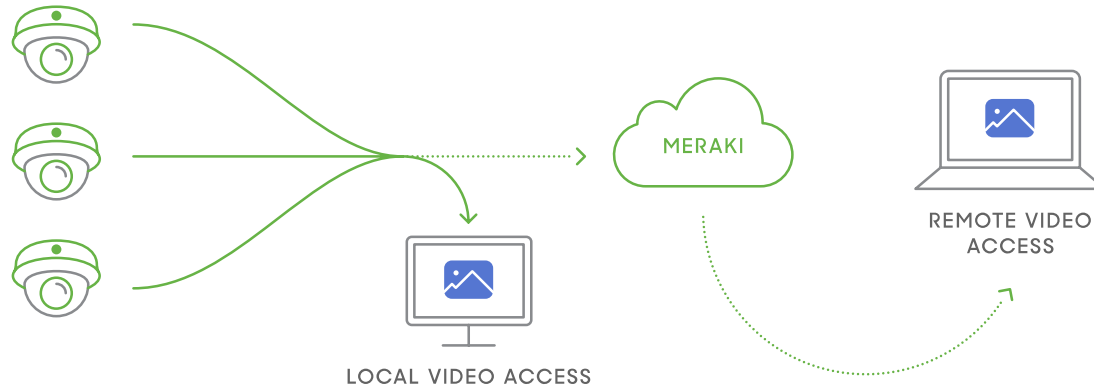
Use **webhooks** for powerful and flexible **alerting**

Aggregate sensor data with third party systems for **customized solutions**



MV – Camera's update

Cutting Edge Architecture



EASY ON THE NETWORK



Less than 50kpbs upstream bandwidth per camera when not watching video

ACCESS ANYWHERE



View locally, or view remotely via cloud proxy streaming, from the Meraki dashboard

SMART PROCESSING



Video is analyzed on camera, motion indexed in the cloud, improving search and analytics



MV2 Specifications

- Indoor fixed-lens camera
- 4MP sensor and 1080p HD video recording up to 20fps
- Wide Field-of-View (104° Horizontal)
- Low-Light mode with IR range of 8m/26ft
- Audio recording supported with built-in microphone
- Wireless capable (802.11ac 2.4GHz & 5GHz)
- Same features as MV12



Freedom of Installation

USB Type-C powered



Two accessories for power

SKU

MA-PWR-USB-XX

MA-PWR-ETH

What is it?



Max Power

10W (5A, 2V)

12.95W (802.3af)

USB-C Cable

~3m (10 ft)

1m

Connectivity

Wireless

Ethernet via Dongle

Two modes of operation

	Without Cloud Archive	Cloud Archive
Video Playback	Live only	Live and Historical
Video Storage	No on-board video storage	Azure
Video Exports	No stored Video	From Azure
Motion Search	Not supported	Supported
Snapshot API	<u>Live Only</u>	<u>Live Only</u>

Install it anywhere






Mobile Wireless onboarding

- Secure wireless onboarding using mobile app
- Enables self-service installation
- No pre-staging required
- To connect to Dashboard, the camera needs a connection to wireless network
- The Information about the wireless network lives on the Dashboard



Camera as a hotspot


-  Hidden SSID
-  Hashed PSK
-  Unique per camera




Securely exchanging wireless info


 Cisco TAM



 Verify the identity

 Decrypt info

 Connect to SSID

 Check-in to Dashboard

Perfect MT companion



**BLE gateway for
MT**



**Magnetic mounting
ideal for server closets**



**Visual data with
sensor alerts &
readings**

Meraki Vision



20%

Network admins

Network and IT admins in charge of all network infrastructure




80%

Camera-only users

Police and public safety officers, front desk workers, facilities, loss prevention and profit protection, school administrators

Network Connected Cisco Store Meraki Vision

Cameras Video Walls **SmDoorRight**



Map data ©2021 Google Terms of Use

- CSR
- MerchLeft
- MerchRight
- POS
- SmDoorLeft
- SmDoorRight**
- 360 Store Front
- 360 Store Middle
- 360 Store POS
- BCA

Sun, Feb 28th 7:00:36 am NOW

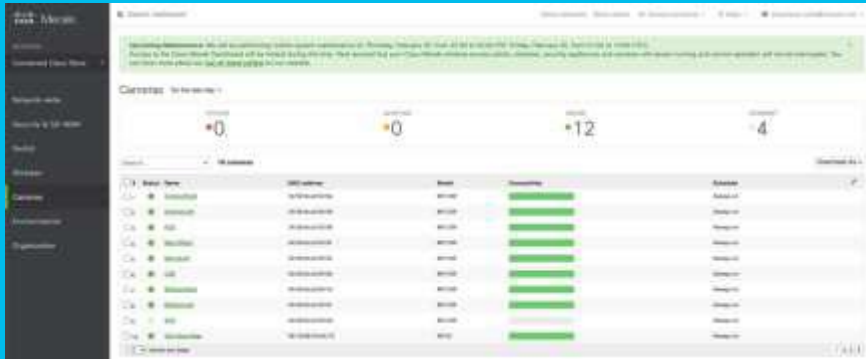
7:00:36 am

15 min

Video feed Motion search Exports

Back to dashboard [Feedback](#)

Simplifying IT for network admins



Meraki Dashboard

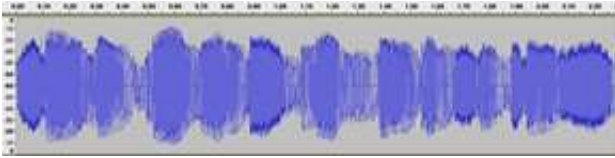
Simplifying physical security for camera-only users



Meraki Vision

MV Audio Analytics

Classifying audio into a particular class

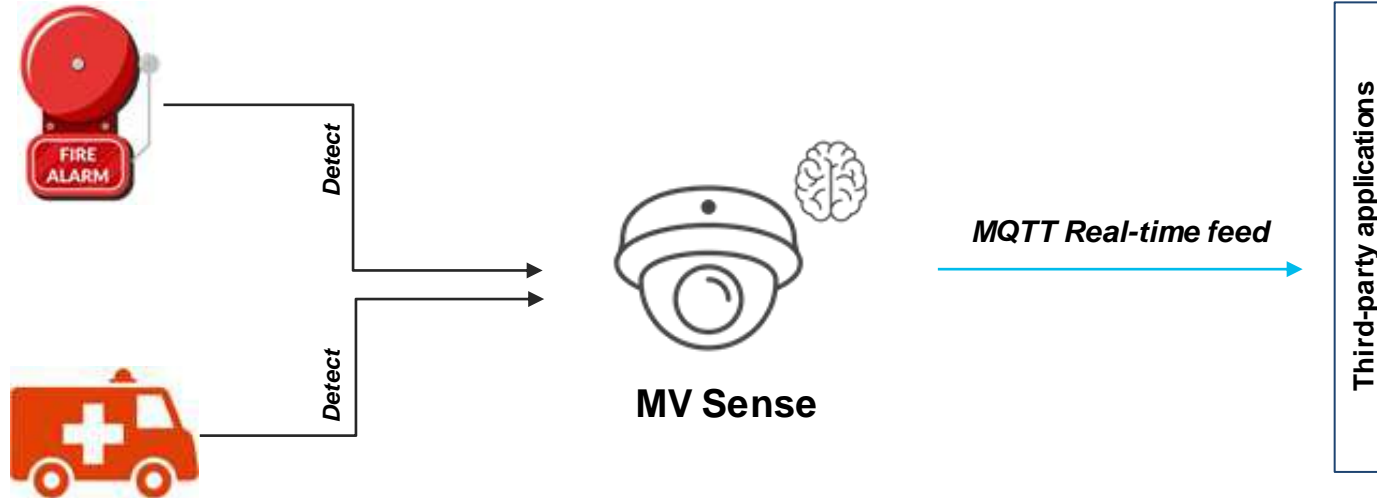


Audio classification

Audio Class A : Yes

Confidence : 80%

Audio Analytics with MV Sense



Integrating Alarm system to Camera



Two new MQTT topics

Merakimv/<S/N>/audio_detections

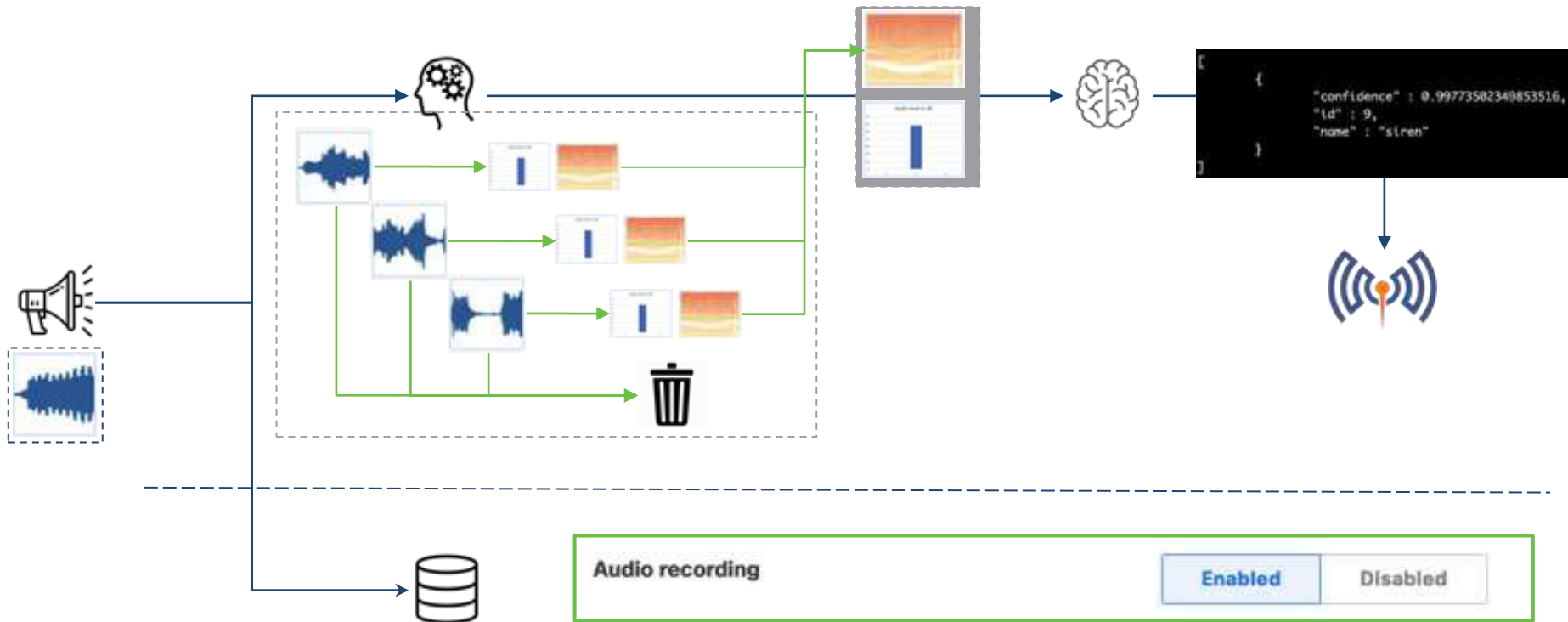
```
{  
  "confidence": 0.8,  
  "id": 0,  
  "class": "fireAlarm"  
}
```

Merakimv/<S/N>/audio_analytics

```
{  
  "audioLevel": 58  
}
```

Fire alarms & emergency sirens

Architecture



Thank you

