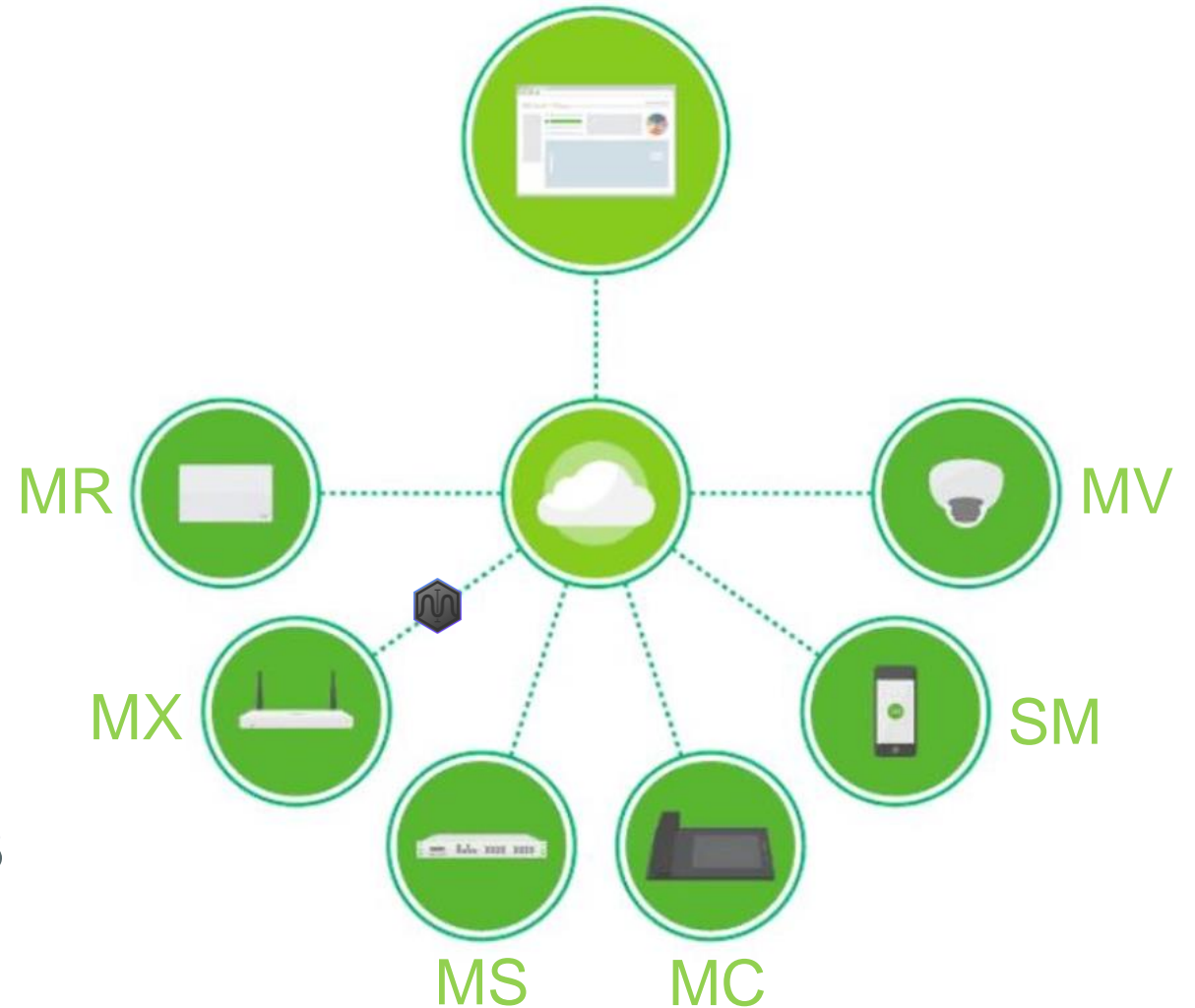


Cisco Meraki FULL STACK

The DASHBOARD



Tech Update 27FEB-18 & 01MAR-18

Nicholas Swiatecki | SE Cisco

Alvaro Ramos Gutierrez | SE Cisco

Peter Henry Andersen | SE Cisco

Agenda

Introduction – MX / vMX, MS, MR, SM, MV & MI – Overview!

Cisco Meraki END to END

- MX & feature enhancements + vMX Azure “HOW TO”
- MS & feature enhancements
- MR & feature enhancements + Wireless Health
- SM & feature enhancements + Cisco Security Connector
- MV & feature enhancements
- MI = Insight

Introduction

Single pane of glass management for the enterprise



Cloud Managed WiFi (2006)

Cloud Managed Network (<-2010/11->)

Cloud Managed Enterprise (2015/16/17/18+)



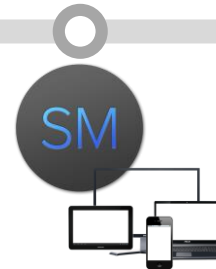
Cisco Meraki MR
Wireless LAN



Cisco Meraki MS
Ethernet Switches



Cisco Meraki MX
Security Appliances



Cisco Meraki SM
MDM/EMM



Cisco Meraki MC
Phones



Cisco Meraki MV
Cameras



Cisco Meraki
Insight

Cisco Meraki END to END

Cisco Meraki Cloud Managed Security



Identity-Based Firewall

Automatically assigns firewall and traffic shaping rules, VLAN tags, and bandwidth limits to enforce the right policies for each class of users.



Intrusion Prevention

Protects critical network resources from the latest security threats and vulnerabilities.



Auto VPN

Securely connects branch locations using mesh or hub-and-spoke topologies.



Content Filtering

Block undesirable web content across 70+ categories, and leverage cloud lookups to filter billions of URLs.



Anti-Malware / Anti-Phishing

Scans HTTP traffic for malware, trojans, and phishing schemes to allow users to securely surf the web.



High Availability & Failover

Provides device and connection integrity through multiple uplinks, warm spare failover, and self-healing VPN.



Application Visibility & Control

Identify which applications are being used, and then prioritize critical apps while limiting recreational apps.



Centralized Management

Seamlessly manage campus-wide WiFi deployments and distributed multi-site networks from a single pane-of-glass.

MX Security Appliances: UPDATE

MX Portfolio – Fall 2017

Teleworker



Z1

Z3

~5 users

802.11ac Wireless & PoE (Z3)

FW throughput: 50, 100 Mbps

Small Branch



MX64

MX65

~50 users

802.11ac wireless & PoE (MX65)

FW throughput: 250 Mbps

Medium Branch



MX84

MX100

~200 users

~500 users

FW throughput: 500 Mbps FW throughput: 750 Mbps

Large Branch, Campus or, Concentrator



MX250

~2,000 users

FW throughput: 4 Gbps



MX400

~2,000 users

FW throughput: 1 Gbps



MX450

~10,000 users

FW throughput: 6 Gbps



MX600

~10,000 users

FW throughput: 1 Gbps

Virtual













vMX100 for AWS & Azure

VPN throughput: 500 Mbps

VPN & SD-WAN features

MX Security Appliances: UPDATE

Introducing MX250 & MX450 Security Appliances

	MX250	MX450
Interfaces		
WAN	 2 x 10G SFP+	 2 x 10G SFP+
LAN	 8 x 1G RJ45	 8 x 1G RJ45
	 8 x 1G SFP	 8 x 1G SFP
	 8 x 10G SFP+	 8 x 10G SFP+
Firewall Throughput	4 Gbps	6 Gbps
Recommended Clients	2,000	10,000
VPN Throughput	1 Gbps	2 Gbps

MX Security Appliances: UPDATE

Introducing the Meraki Z3 Teleworker Gateway

Integrated PoE and 802.11ac Wave 2 in one, powerful package



802.11ac Wave 2 wireless
802.1x port authentication

PoE port for desk phone

Optional desk stand



MX Security Appliances: UPDATE







Introducing Meraki Z3 Teleworker Gateway

Meraki Z1



Meraki Z3



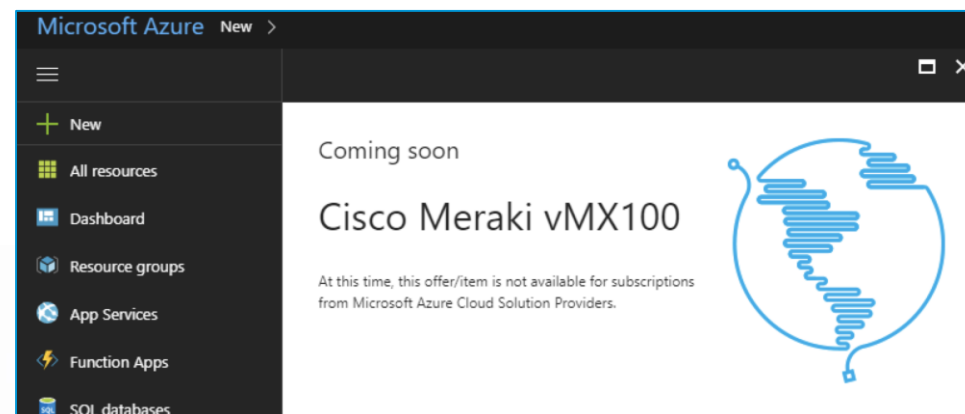
WAN	 1 x 1GbE	 1 x 1GbE
LAN	 4 x 1GbE	 4 x GbE (1 x PoE)
WLAN	 802.11n	 802.11ac wave 2
Firewall Throughput	50 Mbps	100 Mbps
VPN Throughput	10 Mbps	50 Mbps
802.1x port authentication	No	Yes
Vertical desktop mount	No	Yes
Recommended clients	5	5

MX Security Appliances: UPDATE

Introducing vMX100 for Azure

Introducing support for Microsoft Azure
Same as vMX for AWS, now for Azure

- 500 Mbps VPN throughput
- Same license



Cisco Meraki

vMX setup with MS Azure (Pay As You Go) method

Cisco Meraki DASHboard

- Create a MX NETWORK – Add your vMX license

Create network

Setup network

Networks provide a way to logically group, configure, and monitor devices. This is a useful way to separate physically distinct sites within an Organization. ⓘ

Network name

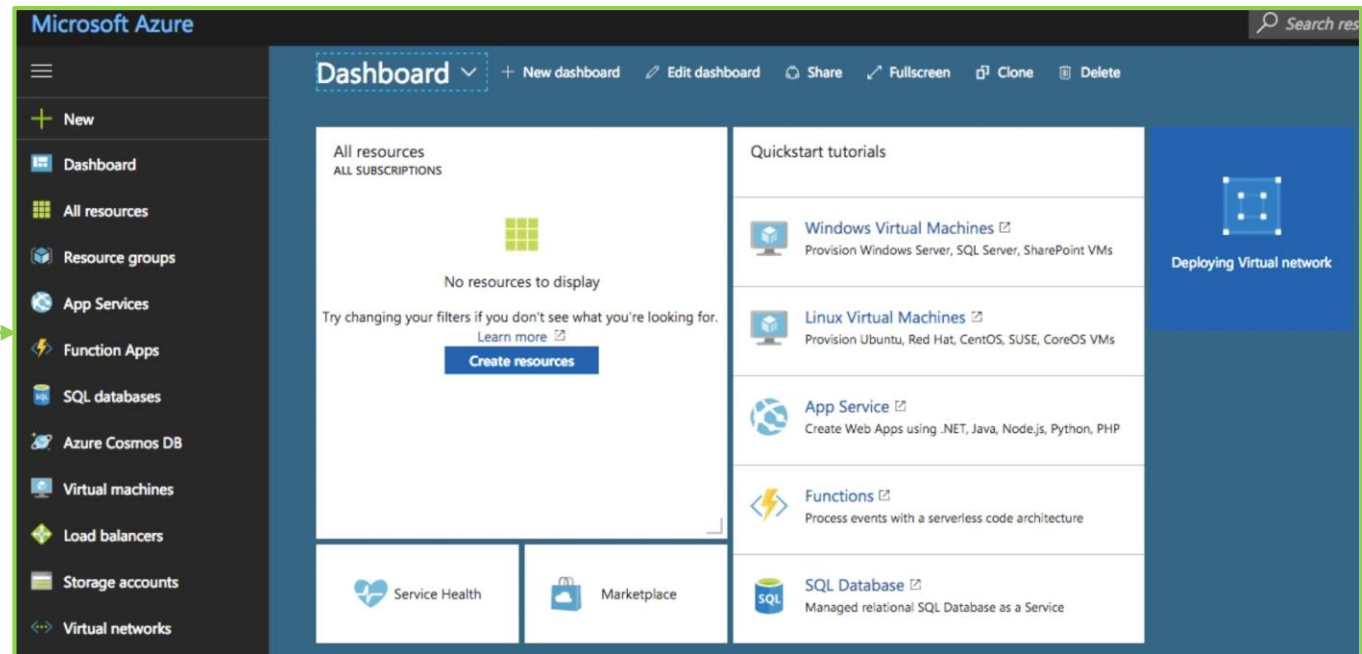
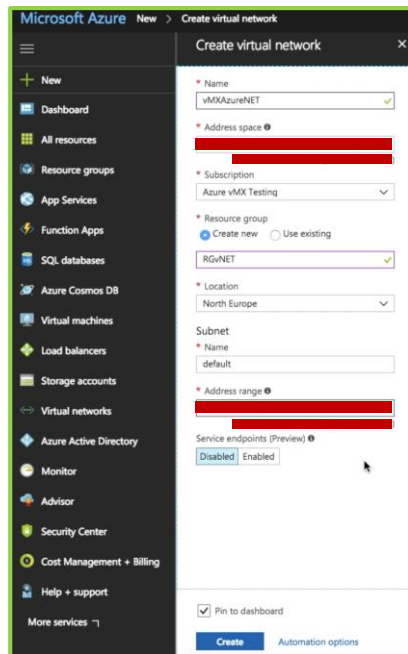
Network type ⓘ

Network configuration Default Meraki configuration

- Go to your MS Azure Portal and continue on next slide...

MS Azure Portal

- Create a Virtual Network via your MS menu options “Virtual Networks”



MS Azure Portal

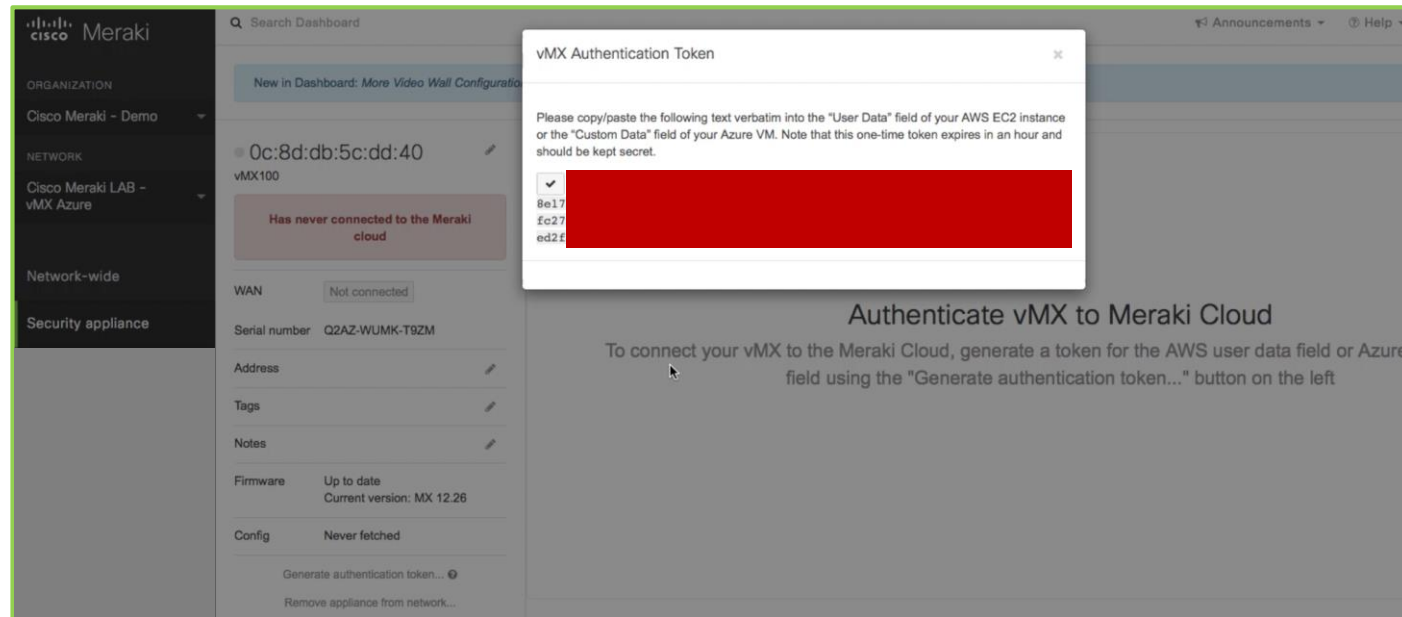
- Create a Cisco Meraki vMX via your MS menu options “New”
- Search for “vmx100” or “Cisco Meraki vMX”
- Below will show and choose highlighted - Click “Create”

The screenshot shows the Microsoft Azure Marketplace interface. The left sidebar contains navigation options: New, Dashboard, All resources, Resource groups, App Services, Function Apps, and SQL databases. The main area is titled 'Marketplace > Everything' and shows a search for 'Cisco Meraki vMX100'. The search results are displayed in a table with columns for NAME, PUBLISHER, and CATEGORY. Two results are shown: 'Cisco Meraki vMX100 (Staged)' and 'Cisco Meraki vMX100'. The second result is circled in red.

NAME	PUBLISHER	CATEGORY
Cisco Meraki vMX100 (Staged)	Cisco Systems, Inc.	Compute
Cisco Meraki vMX100	Cisco Systems, Inc.	Compute

Cisco Meraki DASHboard

- Switch to your Cisco Meraki “Dashboard” and generate vMX TOKEN
- Copy it - switch back to the MS Azure Portal and paste in the required field!



The screenshot displays the Cisco Meraki Dashboard interface. On the left, a navigation sidebar shows 'ORGANIZATION' (Cisco Meraki - Demo), 'NETWORK' (Cisco Meraki LAB - vMX Azure), 'Network-wide', and 'Security appliance'. The main content area shows details for a vMX100 device, including its MAC address (0c:8d:db:5c:dd:40), WAN status (Not connected), Serial number (Q2AZ-WUMK-T9ZM), Address, Tags, Notes, Firmware (Up to date, Current version: MX 12.26), and Config (Never fetched). A 'Generate authentication token...' button is visible at the bottom of the device details. A modal dialog box titled 'vMX Authentication Token' is open in the center, displaying a redacted token value. The dialog text reads: 'Please copy/paste the following text verbatim into the "User Data" field of your AWS EC2 instance or the "Custom Data" field of your Azure VM. Note that this one-time token expires in an hour and should be kept secret.' Below the text, a redacted token is shown with a checkmark icon to its left. The background of the dashboard is dimmed, and a 'Generate authentication token...' button is visible at the bottom of the device details.

MS Azure Portal

- Follow the 4 STEPS to getting your MS Azure / Cisco Meraki vMX up!
- Your Cisco Meraki vMX token you generated in previous slide..
- Paste it into the field in the MS Azure portal and continue below STEPS..

The screenshot shows the 'Basics' step of the 'Create Cisco Meraki vMX100' wizard in the Microsoft Azure portal. The left sidebar contains the navigation menu with 'New' at the top. The main content area is divided into two columns. The left column shows a progress indicator with four steps: 1. Basics (selected), 2. Deployment Details, 3. Summary, and 4. Buy. The right column contains the configuration fields for the 'Basics' step: VM Name (AzurevMX100), Meraki Authentication Token (redacted), Subscription (Azure vMX Testing), Resource group (RGvMX100), and Location (North Europe). An 'OK' button is visible at the bottom right.

The screenshot shows the 'Deployment Details' step of the 'Create Cisco Meraki vMX100' wizard in the Microsoft Azure portal. The left sidebar is the same as in the previous screenshot. The main content area shows the progress indicator with four steps: 1. Basics (Done), 2. Deployment Details (selected), 3. Summary, and 4. Buy. The right column contains the configuration fields for the 'Deployment Details' step: Virtual Network (vMXAzureNET), Subnets (Review subnet configuration), and VM size (1x Standard D2 v3). An 'OK' button is visible at the bottom right.

MS Azure Portal

- Follow the below STEPS to getting your MS Azure / Cisco Meraki vMX up!

Validation passed	
Basics	
Subscription	Azure vMX Testing
Resource group	RGvMX100
Location	North Europe
VM Name	AzurevMX100
Meraki Authentication Token	[REDACTED]
Deployment Details	
Virtual Network	vMXAzureNET
Subnet	default
Subnet address prefix	[REDACTED]
VM size	Standard D2 v3

OK Download template and parameters

to your Azure subscription.

Prices for Marketplace offerings are set forth here, and the legal terms associated with any Marketplace offering may be found in the Azure portal; both are subject to change at any time prior to deployment.

Neither subscription credits nor monetary commitment funds may be used to purchase non-Microsoft offerings. These purchases are billed separately. If any Microsoft products are included in a Marketplace offering (e.g., Windows Server or SQL Server), such products are licensed by Microsoft and not by any third party.

The highlighted Marketplace purchase(s) are not covered by your Azure credits, and will be billed separately.

You cannot use your Azure monetary commitment funds or subscription credits for these purchases. You will be billed separately for marketplace purchases.

Co-Admin Access Permission

By checking the box and clicking "Create" I give permission for the template provider referenced above (the "Provider") to have Administrative-level access to one or more Azure resources in order to provide support and management services for the template. In the event of an issue arising from a Provider's services or failure to provide services, your sole recourse is with the Provider. Unless Microsoft is the Provider, Microsoft (I) does not approve, monitor or manage the Provider's access, and (ii) bears no responsibility whatsoever for acts or omissions of a Provider.

I agree to the terms and conditions above.

Terms of use

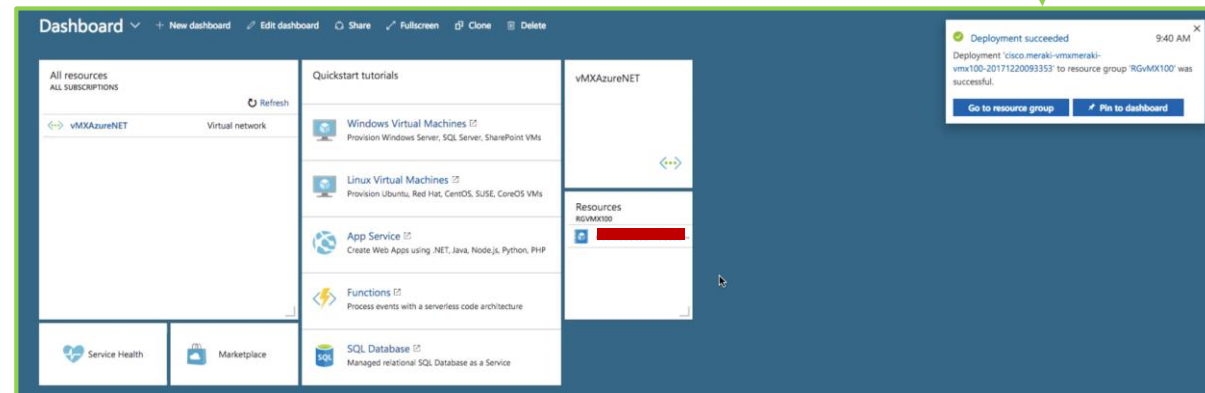
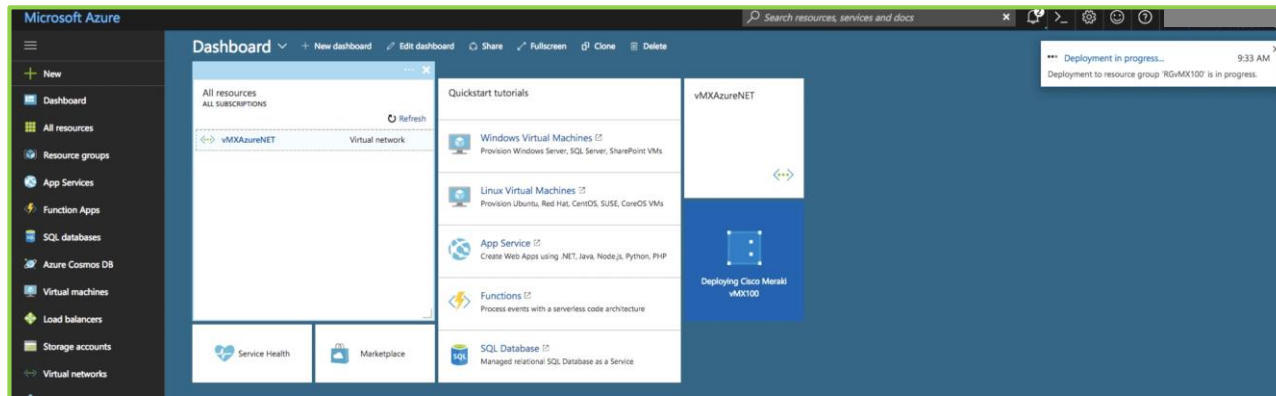
By checking the box and clicking "Create", I (i) agree to the Provider's Terms of Use and Privacy Statement linked above as well as the legal terms and privacy statement(s) associated with each Marketplace offering that will be deployed using this template, if any; (ii) authorize Microsoft to charge or bill my current payment method for the fees associated with my use of the offering(s), including applicable taxes, with the same billing frequency as my Azure subscription, until I discontinue use of the offering(s); and (iii) agree that, unless Microsoft is the Provider, Microsoft may share my contact information and transaction details with any third-party sellers of the offerings deployed by this template. Microsoft assumes no responsibility for any actions performed by third-party templates and does not provide rights for third-party products or services. See the Azure Marketplace Terms for additional terms.

I agree to the terms and conditions above.
 I give Microsoft permission to use and share my contact information so that Microsoft or the Provider can contact me regarding this product and related products.

Create

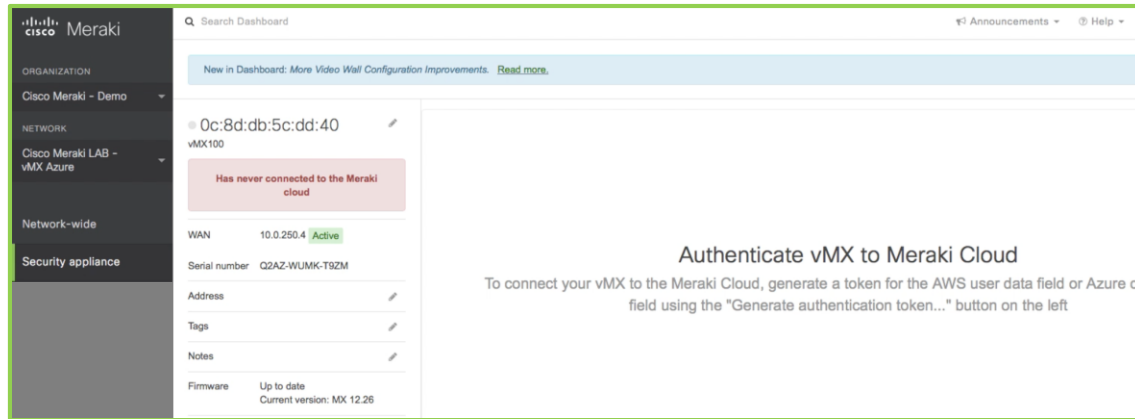
MS Azure Portal

- The STEPS have been followed and now you'll see a vMX being processed.

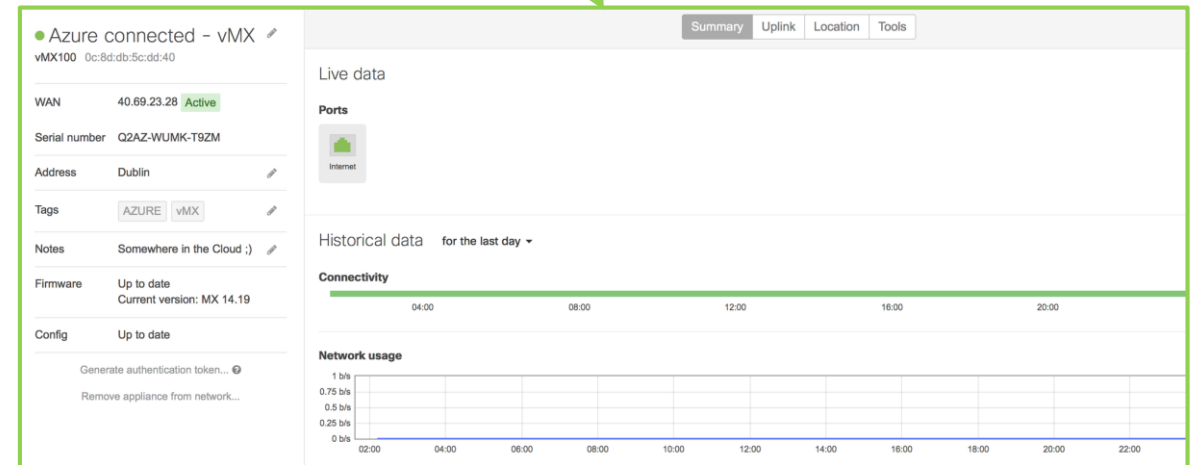


Cisco Meraki DASHboard

- Your newly deployed Cisco Meraki vMX100 is now active with MS Azure



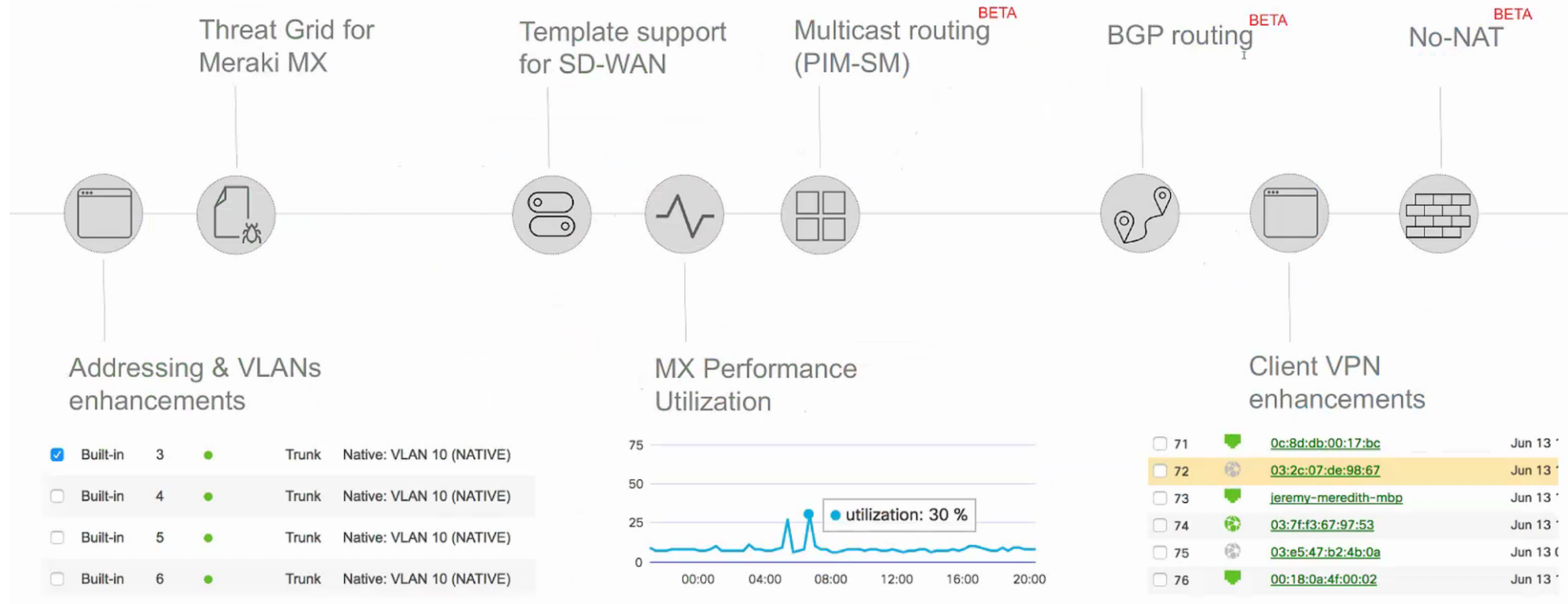
Refresh browser



Now you can create HUBS / SPOKES Auto VPN
Connect your "MS Azure" Servers and more to the mix.
Enjoy 😊

MX Security Appliances: UPDATE

MX Product Updates – Past 6 Months



MX Security Appliances: ENTERRISE or ADVANCED

Feature	Enterprise license	Advanced Security license
Stateful firewall	✓	✓
VLAN to VLAN routing	✓	✓
Link bonding / failover	✓	✓
3G / 4G failover	✓	✓
Traffic shaping / prioritization	✓	✓
WAN optimization	✓	✓
Site-to-site VPN	✓	✓
Client VPN	✓	✓
MPLS to VPN Failover	✓	✓
Splash pages	✓	✓
Configuration templates	✓	✓
HTTP content caching	✓	✓
Group Policies	✓	✓
Client connectivity alerts	✓	✓
SD-WAN	✓	✓
Geography based firewall rules		✓
Intrusion detection / prevention		✓
Content filtering		✓
Anti-virus and anti-phishing		✓
Youtube for Schools		✓
Web Search Filtering		✓
AMP / Anti-malware		✓



Experience the Benefits of Cloud Management

1. 24/7 – 365 support included.
2. Next Business Day HW Replacement.
3. All WAN/SEC features available*
4. Firmware updates ready on appliance.
5. Security updates auto updated.
6. New features auto updated in Dashboard
7. LIC time for 1, 3, 5, 7 or 10yr
8. LIC is not locked to HW
9. ENT to ADV and ADV to ENT up/downgrade possible
10. Cisco Meraki NOW – 24/7-2-OS Support **









**Additional service purchase

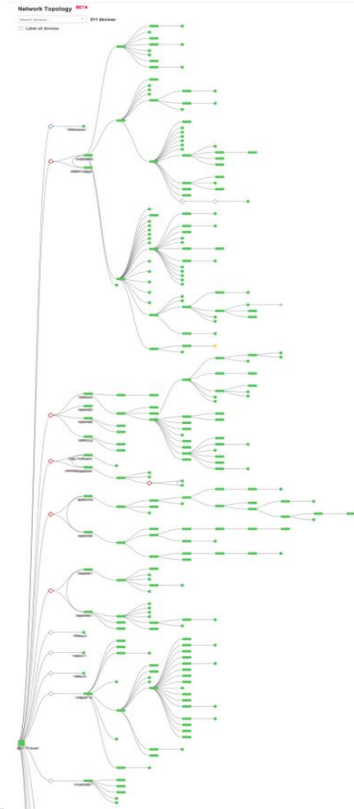
Cisco Meraki Cloud Managed LAN



Cloud Managed Switches












Gigabit Ethernet Built for Management

 Cloud Managed	 Virtual Stacking	 Layer 7 Visibility	 Layer 3 Scalability	 Voice & Video QoS	 Network Topology	 Remote Live Tools	 Enterprise Security
--	---	---	--	--	---	--	--



The MS Series

Meraki Access Switching Portfolio – Fall 2017

	New MS120-8	New MS120	New MS210	MS225	MS250	MS350
						
	Compact	Small branch, SOHO	Branch & small campus	Branch & small campus	Branch & Campus	Campus, Multigigabit
Uplink options 	1G SFP x 2	1G SFP x 4	1G SFP x 4	10G SFP+ x 4	10G SFP+ x 4	10G SFP+ x 4
PoE options 	PoE/PoE+ 67W (LP model) 124W (FP model)	PoE/PoE+ 370W (P,LP models) 740W (FP models)	PoE/PoE+ 370W (P,LP models) 740W (FP models)	PoE/PoE+ 370W (P,LP models) 740W (FP models)	PoE/PoE+ 370W (P, LP models) 740W (FP models)	PoE/PoE+/UPoE 370W (P, LP models) 740W (24X, FP models)
Stacking capabilities 	Virtual	Virtual	Virtual, 80G physical Compatible Physical Stacking		Virtual, 80G physical	Virtual, 160G physical
Routing capabilities 	-	-	Static only	Static only	Static, Dynamic 4K routed hosts	Static, Dynamic 96K routed hosts
Power capabilities 	External(non-PoE/LP) Internal(FP), fanless architecture	Internal	Internal Optional RPS	Internal Optional RPS	Field replaceable Optional redundant PSU	Field replaceable Optional redundant PSU and Fan

The MS Series – Campus / Distribution



MS410 Series

1G FIBER AGGREGATION

160G Stacking

10G SFP+ Uplinks

16 / 32 × SFP gigabit ethernet

2 × stacking ports

1 × management port with auto-MDIX

Removable PSU
Field Replaceable

Up to 2 × 250W PSU

1 × PSU included, redundant PSU sold separately



MS425 Series

10G FIBER AGGREGATION

160G Flexible Stacking

40G QSFP+ Uplinks

16 / 32 × SFP+ 10 gigabit ethernet

2 × QSFP+

1 × management port with auto-MDIX

Removable PSU
Field Replaceable

Up to 2 × 250W PSU

1 × PSU included, redundant PSU sold separately

Streamlined MS Accessories



New power supply model numbers for MS320/350

MA-PWR-250WAC
MA-PWR-640WAC
MA-PWR-1025WAC



New fan model numbers

MA-FAN-18K for MS420
MA-FAN-16K for MS350



New 3m Twinax option

MA-CBL-TA-3M

Feature Enhancements - MS

Dynamic ARP Inspection **BETA**

DAI status: Disabled

Configure Trusted Ports from the [Ports](#) page.

Whitelisted snoop entries

MAC address	VLAN	IP address

Access policies

Name: Access policy #1

Authentication method: Meraki authentication

Authenticated users: Manage the list of users authorized for this Access Policy on the [Users](#) page.

Systems Manager Sentry security: Enabled: Allow devices with following tag scopes access to network

Network name	Scope	Tags
Cisco Meraki - LAB DEM...	With ANY of	Mac devices

Guest VLAN: [Empty]

Systems Manager enrollment: Systems Manager Enrollment enabled

Systems Manager Sentry enrollment network: Cisco Meraki - LAB DEMO AAR - systems manager

Switch ports: There are currently 0 Switch ports using this policy

Multicast settings

IGMP Snooping

IGMP snooping examines IGMP membership report messages to limit multicast traffic to the subset of interfaces on which interested hosts reside.

Switches/Stacks	IGMP snooping	Flood unknown multicast traffic
Choose switches...	Enabled	Enabled
Default	Enabled	Enabled

[Set multicast settings for another switch or stack](#)

Access policies

Name: Access policy #1

Authentication method: my RADIUS server

RADIUS servers

#	Host	Port	Secret	Actions

RADIUS testing: RADIUS testing enabled

RADIUS CoA support: RADIUS CoA enabled

RADIUS accounting: RADIUS accounting enabled

RADIUS accounting servers

#	Host	Port	Secret	Actions
1				

Host Mode: Single-Host

Access policy type: 802.1x

Guest VLAN: [Empty]

Voice VLAN clients: Require authentication

URL redirect walled garden: Walled garden is disabled

Systems Manager enrollment: Systems Manager Enrollment disabled

Systems Manager Sentry enrollment network: Meraki GRID - Skyport - systems manager

Storm Control

Storm Control

Storm control monitors the level of the defined traffic types over 1 second intervals. If traffic of the defined types exceeds the defined limit, excess packets will be dropped. The storm control rate defined is applied to each port based on the port's total available bandwidth.

Traffic types	% of available port bandwidth
Multicast	20 %
Broadcast	10 %
Unknown unicast	5 %

Add a storm control rule

Staged Upgrades **BETA**


Upgrade Status: Scheduling

Default upgrade time: Tuesday 12 AM CET









Upgrade policy: The switches in this network are configured to run the latest available firmware. Last upgraded on Saturday, February 3, 2016 at 16:00 CET

Try beta firmware: Yes

Cisco Meraki Cloud WLAN



Cloud Managed Wireless

 Centralized Management Seamlessly manage campus-wide WiFi deployments and distributed multi-site networks from a single pane-of-glass.	 Multigigabit Ethernet Pass 2.5Gbps of traffic over a single cable in order to take full advantage of high speed 802.11ac Wave 2 wireless.	 Location Analytics Reveal powerful metrics such as visitor capture rate, user visit time, and repeat visits by listening for wireless devices.	 Application Visibility & Control Identify which applications are being used, and then prioritize critical apps while limiting recreational apps.
 High Capacity 802.11ac RF optimization with real-time spectrum analysis enables high performance wireless in dense, demanding environments.	 Automatic RF Optimization Automatically optimize WiFi by measuring channel utilization, signal strength, throughput, and interference.	 Dedicated Security Radio Instantly detects interference, vulnerabilities, and attacks on all channels.	 Identity-Based Firewall Automatically assigns firewall and traffic shaping rules, VLAN tags, and bandwidth limits to enforce the right policies for each class of users.

Deployments Made Simple

1

Configure wireless network settings in dashboard

2

Mount and plug in access point

3

APs automatically pull configurations from the cloud

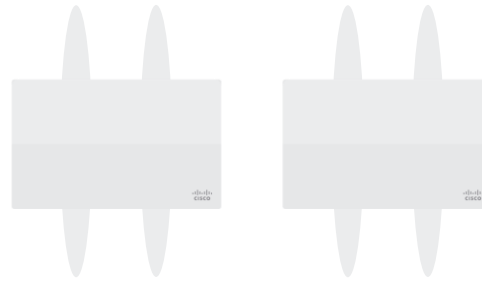
4

APs self-optimize RF for peak performance

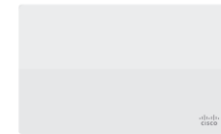
Smart wireless also means having the right hardware



One-sized coverage
(omnidirectional) does not suit
all indoor scenarios



Sometimes basic, rapidly
deployed outdoor coverage
is needed



Other times, entry-level
wireless is the answer

Cisco Meraki Cloud WLAN – AP range INDOOR

Below is 4 Radio AP's

2,4 + 5Ghz – Scanning – BLE radios



MR53E  

HIGH-DENSITY COVERAGE
4x4:4-stream MU-MIMO

Multigigabit and external antenna connectors

Recommended for focused coverage and flexibility



MR53  

HIGH-DENSITY COVERAGE
4x4:4-stream MU-MIMO

Multigigabit

Recommended for general coverage



MR52  

HIGH-DENSITY COVERAGE
4x4:4-stream MU-MIMO

Recommended for general coverage



MR42E  

GENERAL PURPOSE WIRELESS
3x3:3-stream MU-MIMO

External antenna connectors

Recommended for focused coverage and flexibility



MR42  

GENERAL PURPOSE WIRELESS
3x3:3-stream MU-MIMO

Recommended for general coverage



MR33  

GENERAL PURPOSE WIRELESS
2x2:2-stream MU-MIMO

Recommended for general, low-density coverage

Below is 4 Radio AP's

2,4 + 5Ghz – Scanning – BLE radios



MR30H  

BASIC COVERAGE
2x2:2-stream MU-MIMO

Integrated 4-port gigabit switch

Recommended for hospitality and in-room coverage

Below is 2 Radio AP

2,4 + 5Ghz radios



MR20

BASIC COVERAGE
2x2:2-stream MU-MIMO

Recommended for entry-level, very low-density coverage

Cisco Meraki Cloud WLAN – AP range OUTDOOR

Below is 4 Radio AP's

2,4 + 5Ghz – Scanning – BLE radios



MR84  

HIGH-DENSITY RUGGEDIZED COVERAGE

4x4:4-stream MU-MIMO

Multigigabit and external antenna connectors

Recommended for focused coverage and flexibility



MR74  

GENERAL PURPOSE RUGGEDIZED WIRELESS

2x2:2-stream MU-MIMO

External antenna connectors

Recommended for focused coverage and flexibility

Below is 2 Radio AP

2,4 + 5Ghz radios



MR70

BASIC RUGGEDIZED COVERAGE

2x2:2-stream MU-MIMO

Integrated omni-directional antennas

Recommended for entry-level, low-density coverage and rapid outdoor deployments

New entry-level APs for very low-density deployments



MR20

Basic wireless, very low density deployments

802.11ac Wave 2 **2x2:2-stream** MU-MIMO

\$549



MR70

Entry-level outdoor wireless, extremely easy setup

802.11ac Wave 2 **2x2:2-stream** MU-MIMO

Internal omni antenna: **no external antenna support**

\$1,099

No separate 3rd radio for scanning, no Bluetooth Low Energy (BLE) radio

New indoor APs with smart external antennas



MR53E

Highest density & mission critical

802.11ac Wave 2 **4x4:4-stream** MU-MIMO

Multigigabit support for highest throughputs over existing cabling

\$1,699



MR42E

Focused coverage & flexibility

802.11ac Wave 2 **3x3:3-stream** MU-MIMO







\$1,099

6 antenna options, including BLE antenna (allows Bluetooth coverage to equal WiFi coverage area)

Cisco Meraki Cloud WLAN – Antenna Range







RP-TNC "Cisco" Connectors

External Antennas for Indoor APs

 <p>Dipole Antenna (3.8/5.5 dBi) Contact Sales Learn More</p>	 <p>Dipole Antenna (3/5.7 dBi) Contact Sales Learn More</p>	 <p>Panel Omni Antenna Contact Sales Learn More</p>
 <p>Down-tilt Panel Omni Antenna Contact Sales Learn More</p>	 <p>Wide Patch Antenna Contact Sales Learn More</p>	 <p>Narrow Patch Antenna Contact Sales Learn More</p>

N-TYPE Connectors

External Antennas for Outdoor/Ruggedized APs

 <p>Dual-Band Omni Antennas (4/7 dBi) Contact Sales Learn More</p>	 <p>5 GHz Sector Antenna (13 dBi Gain) Contact Sales Learn More</p>	 <p>2.4 GHz Sector Antenna (11 dBi Gain) Contact Sales Learn More</p>
 <p>Dual-Band Patch Antenna (8/6.5 dBi Gain) Contact Sales Learn More</p>	 <p>Dual-Band Sector Antenna (9/12 dBi Gain) Contact Sales Learn More</p>	 <p>Cisco Stadium Antenna Contact Sales Learn More</p>

The full lineup

The A series (dipole)



\$39 - \$199

The B series (dipole)



\$39 - \$199

The C series (panel omni)



\$399 - \$499

The D series (downtilt panel omni)



\$399 - \$499

The E series (wide patch)



\$399 - \$599

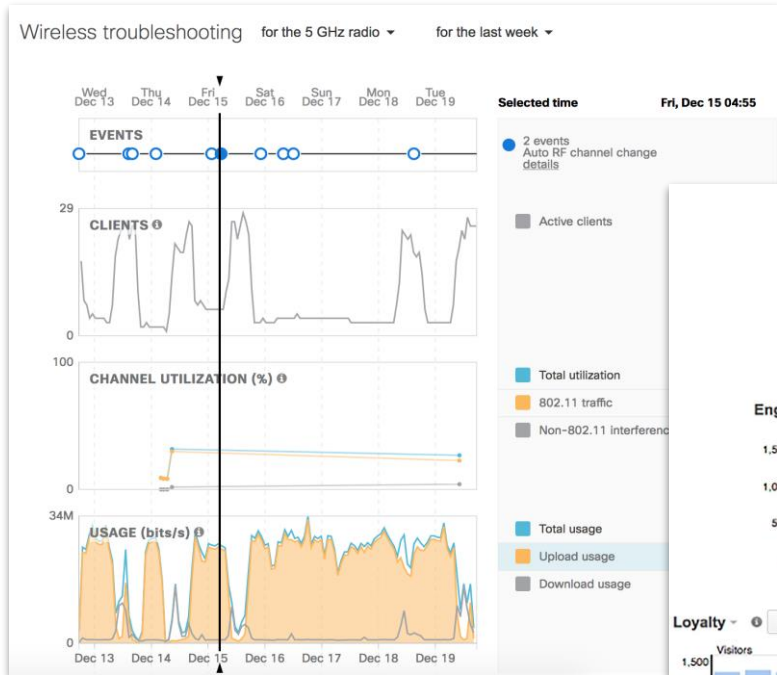
The F series (narrow patch)



\$949

What is smart?

RF Analytics



Location Analytics



Anomaly Detection

Summary Report from the last week

NETWORK(S): Meraki San Francisco - wireless
DEVICE TAG: All devices
SSID: All SSIDs

Anomalies

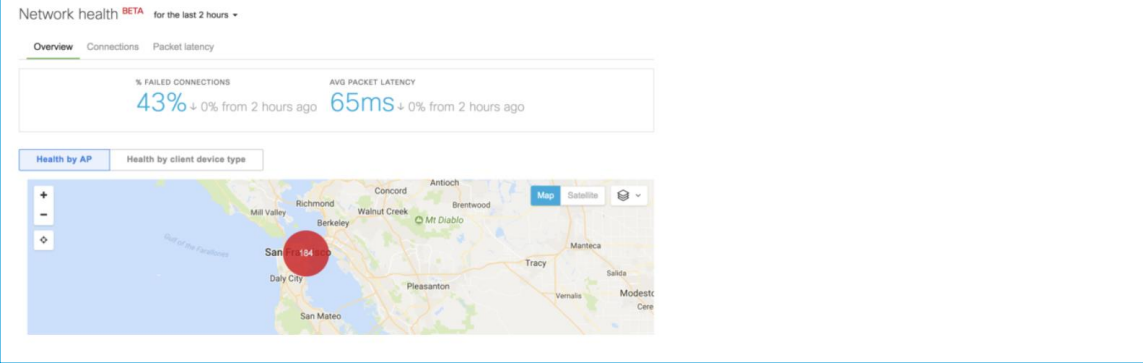
12/17: Above average usage for a Sunday
Bandwidth usage was 256% higher than the last 10 Sundays recorded [View details >](#)
[View 2 more >](#)

Clients with high usage

4 clients used more than 100.00 GB
'X1V2', 'MYU-X260' and 2 other clients

Feature Enhancements - MR

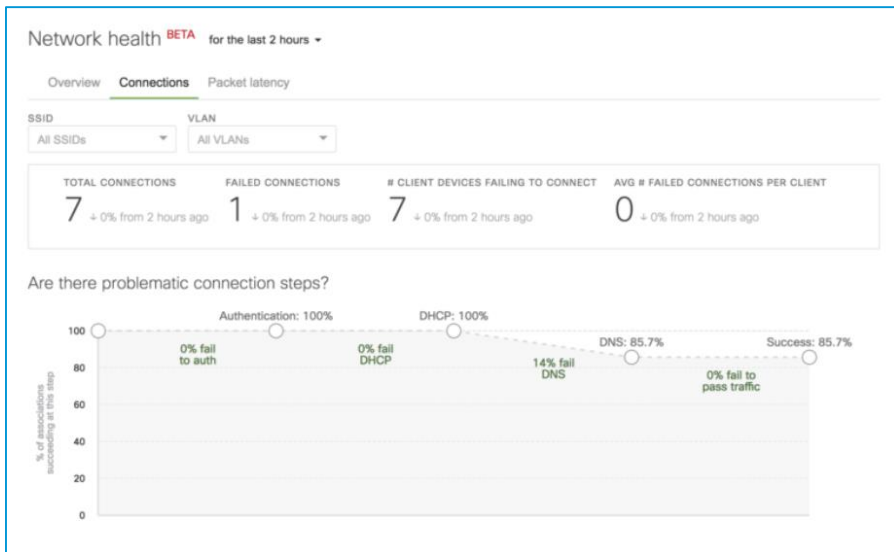
These metrics and anomalies are synthesized into a holistic, network-level view that allows administrators to quickly identify networks with problems that require attention.



Once a client has successfully connected, Wireless Health displays detailed metrics about network latency, identifying which types of traffic are showing performance problems at various thresholds of performance (measured in milliseconds).



Network administrators can drill down and get granular metrics on latency across their network at the AP level and at the device type level, helping them quickly identify the worst-performing APs and clients.



Highest AP → client latency by AP

These APs have the highest average wireless latency to their clients.

AP	Avg wireless latency	% high latency voice	% high latency video	% high latency best effort	% high latency background
3.07	81ms	2%	2%	2%	3%
3.57	45ms	0%	2%	0%	2%
4.01	< 10ms	0%	0%	0%	0%
5.01	< 10ms	0%	0%	0%	0%
4.02	< 10ms	0%	0%	0%	0%

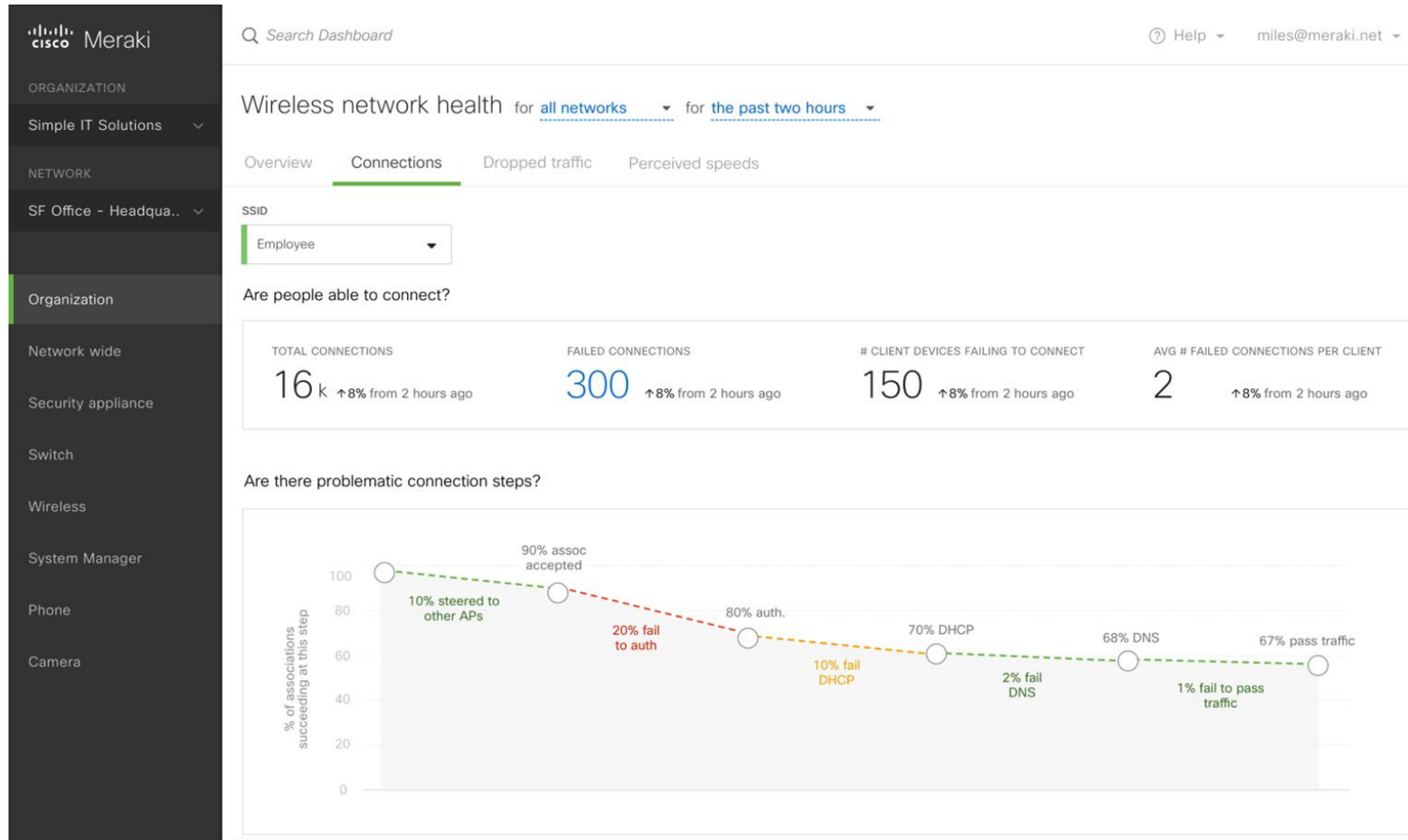
Show more...

Highest AP → client latency by client device type

Device type	# client devices	Avg wireless latency	% high latency voice	% high latency video	% high latency best effort	% high latency background
Windows 10	2	48ms	0%	2%	0%	3%
Chrome OS	2	21ms	2%	0%	0%	0%
Mac OS X 10.12	1	< 10ms	0%	2%	0%	0%
Android	1	< 10ms	0%	0%	2%	0%
Mac OS X 10.11	1	< 10ms	0%	0%	0%	2%

Show more...

One step further: Wireless Health



Metrics and anomaly detection for:

- client network associations
- wireless connection quality (latency)
- capacity (data rate)

Available for Meraki MR access points as a **free** feature update

Feature Enhancements - MR

Enter RF Profiles. This feature allows network administrators to easily customize RF characteristics by deployment and manage diverse MR installations through the configuration of templated radio settings. These settings (which comprise a profile) can then be applied, en masse, to groups of APs. RF Profiles will include predefined templates for typical auditoriums, open offices, and outdoor coverage scenarios to help IT quickly configure wireless settings for maximum performance.

Create an RF Profile

The screenshot shows a 'Create an RF Profile' interface with six profile cards:

- New Profile From Scratch**: A button to create a new profile.
- Auditorium Profile**: For auditorium deployments accommodating a large number of devices. Limits coverage area per AP and optimizes client roaming. Button: **Customize this profile**
- Class Room Profile**: For classroom deployments. Provides good coverage and optimizes client roaming. Button: **Customize this profile**
- Open Office Profile**: For open office deployments. Balances performance and coverage. Button: **Customize this profile**
- Conference Room Profile**: For conference room deployments. Provides good coverage and encourages client roaming once outside of the room. Button: **Customize this profile**
- Outdoors Profile**: For outdoor deployments. Prioritizes coverage and connectivity for distant and legacy clients. Button: **Customize this profile**

RF Profiles allows radio settings to be easily deployed to all the APs applied a given profile.

In high density environments with many client devices trying to connect to a wireless network, IT admins typically deploy more APs to increase overall capacity. But adding more APs introduces interference, since the odds that two APs within earshot of each other use the same channel increases. By ignoring signals that don't meet a certain threshold strength, Rx-SOP allows an AP to ignore clients on neighboring access points who are using the same channel — mitigating their ability to interfere.

The screenshot shows the '5 GHz radio settings' configuration page with the following settings:

- Channel width**: Auto (selected), Manual
- Channel assignment method**: Auto (selected), Manual
- Radio transmit power range (dBm)**: Slider from 1 to 30, set to 7. Labels: Transmit shorter distance (left), Transmit farther (right).
- Minimum received power (RX-SOP)**: Slider from -75 dBm to -90 dBm, set to -80. Labels: Ignore weaker clients (left), Listen for clients further away (right).
- Minimum bitrate**: Slider from 1 to 54 Mbps, set to 11. Labels: Transmit farther (left), Transmit shorter distance (right). A warning box below reads: "No connectivity for some 802.11b devices".

An antenna for any occasion

Internal (current indoor APs)

Wide 360 degree coverage

Ideal for most carpeted offices.

A-Series (\$39 - \$199)

Straight dipoles provide 360 degree coverage pattern

Ideal for low ceiling installations where wall penetration or extended reach are important.

B-Series (\$39 - \$199)

Bendable dipole provides 360 degree coverage pattern

Ideal to deploy when AP is installed on walls tilted downwards, or best-effort deployments where APs are installed on uneven surfaces or walls.

C-Series (\$399 - \$499)

Panel omni. Aesthetically pleasing vs. dipoles

Ideal for low ceiling deployments or open areas, such as the ceiling in center of loading docks, warehouses, etc.

D-Series (\$399 - \$499)

Panel downtilt omni. Aesthetically pleasing vs. dipoles

Higher ceilings (25 ft+) with medium-density usage. If ceiling is too high, can be installed at an angle using arm mount.

E-Series (\$399 - \$599)

Wide patch

Wide coverage area for medium-density deployments in stadiums, warehouse, and auditoriums.

F-series (\$949)

Narrow patch

Narrow coverage area for high-density deployments in areas like stadiums and auditoriums.

AP + antenna orderability & shipping starts
February 13, 2018

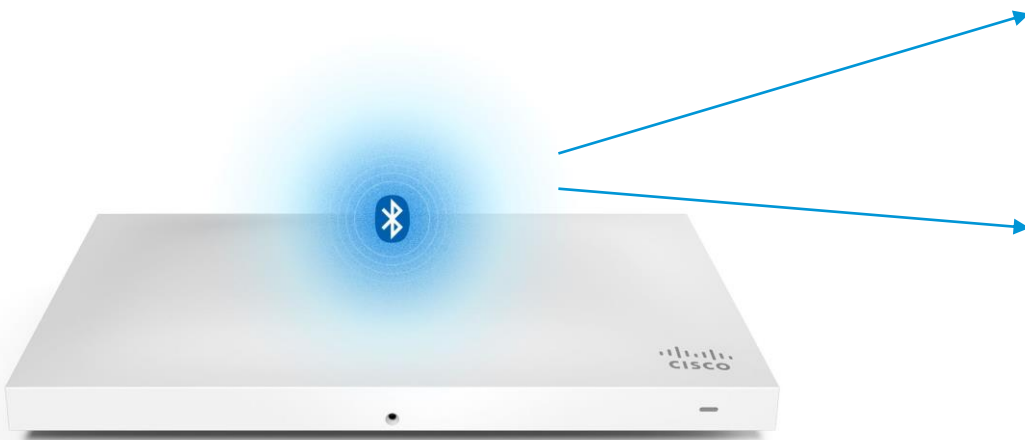
Real-world BLE applications



1. AP deployed in contextual area, configured as specific Beacon.
2. User with context-aware mobile app walks by Beacon location.
3. App hears Beacon, alerts on lockscreen.
4. User launches app for location-related engagement.

5. (Optional) App communicates with backend systems for dynamic content or analytics.

Cisco Meraki CMX – iBeacon built in-to AP



Bluetooth settings

Scanning

Scanning ⓘ On Off

Visit the [Bluetooth clients](#) page to see clients

Beaconing

Use APs as location markers. For more information, see our [documentation](#).

Advertising ⓘ On Off

UUID ⓘ

The UUID is typically used to identify your organization. You can use templates to ensure your networks have the same UUID set.

Major/Minor Assignment Unique Non-unique

Dashboard will automatically assign unique beacon identifiers to each AP.

APs in the same network will advertise the same Major Number and distinct Minor Numbers. These identifiers won't change once set, even if you temporarily disable beaconing.

Node	Major	Minor
MR52 4x4.4 - ACw2 LAG	0	0
MR53 4x4.4 - ACw2 Mjig	0	1
MR30H 2x2.2 - ACw2	0	2
MR33 - 2x2.2ACw2	0	3

To get the per-node major/minor assignment, use the [Meraki Dashboard Devices API](#) or download a csv.

Cisco Meraki Cloud controlled WLAN - LIC

Enterprise License



Experience the Benefits of Cloud Management

Cisco Meraki MR Series

1. 24/7 – 365 support included.
2. Next Business Day HW Replacement.
3. All WLAN features available.
4. Firmware updates ready on appliance.
5. New features auto updated in the Dashboard.
6. Purchase for 1, 3, 5, 7 or 10yr – Not locked to HW
7. Cisco Meraki NOW – 24/7-2-OS Support **

**Additional service purchase



Mobility Reimagined

iOS

android

 Windows

macOS

 Chrome OS

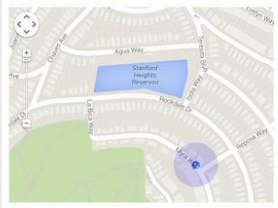
 Windows Phone

SM – Enterprise MDM



Provision

Pre-enroll devices or dynamically add users as they join your network. Deploy wireless and VPN connectivity settings, push apps and content, or restrict usage—based on user groups.



Monitor

Locate and track laptops and mobile devices anywhere in the world. Get real time visibility on device health, security posture, and software and hardware inventory for your entire fleet of devices.

Encryption	Enabled
Firewall	Application firewall
Login required	No
Auto login	Disabled
Screen lock	Disabled
Screen lock delay	15 minutes
Geofencing	Compliant
Security policies	BVOD Corporate

Secure

Ensure security for your organization from devices all the way through to network policies. Protect devices and their data with encryption enforcement, enterprise remote wipe, and integrated network access control.

Network, Meet Device

Every user is unique. Every device, a bit different. Systems Manager keeps the network in the loop about constantly changing devices, automatically tracking device posture and adjusting security policies to match.

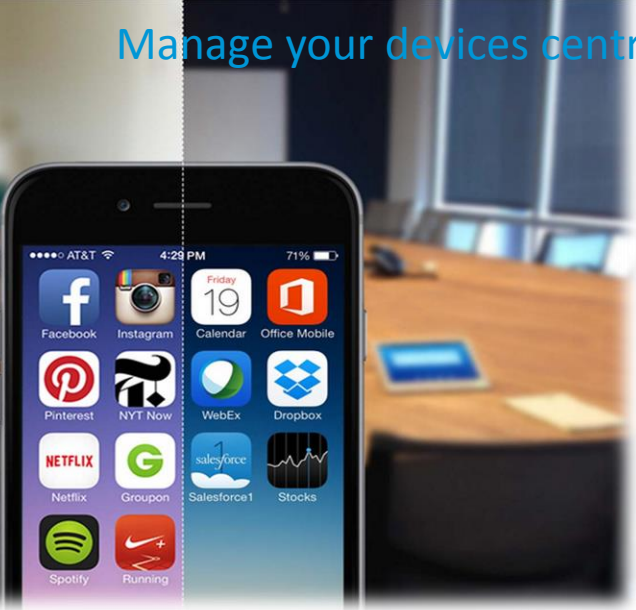


Manage your devices centrally

Contain Your Data

Separate enterprise data from personal data

Don't mess with complicated SDKs or modifying application source code. Systems Manager Enterprise provides secure containerization using native OS tools, allowing secure data sharing among apps without complexity. Whitelist secure applications and blacklist unsupported ones to ensure only approved apps are used, and enable VPN on a per-app basis.



SM – Enterprise MDM – New Features

More Power, More Choice, More Protection



Cisco Security Connector

Protection from malicious sites

Privacy with encrypted DNS

Insight into activity during incidents

Expected Fall 2017

Do Not Disturb

Pause updates for Mission critical endpoints

Control rollouts for App Updates and Kiosk Mode

September 2017

Apple TV Support

Manage Apple TV

Provision WiFi

Out-of-the-box enrollment

Fall 2017

Security Connector – The first security ISO APP

Next phase of the Apple ⁱCisco partnership

- New app that can be deployed on supervised iOS devices
- Enable multiple Cisco security entitlements in a single app
- Expected in the fall of 2017
- Beta available now: <http://cs.co/security-connector-beta>



Security Connector – The first security ISO APP

Basic Requirements

- ✓ Supervised iOS device
- ✓ Subscription to Cisco Meraki Systems Manager (licensed per device)
- ✓ Subscription to Cisco Umbrella (licensed per number of internet-connected users)
- ✓ Subscription to Cisco Clarity (AMP for Endpoints – licensed per device)

Systems Manager

Enable Clarity and Umbrella on iOS devices

Ensure devices are under management and actively share device information with Clarity and Umbrella

Share device posture with Clarity and Umbrella

Licensed per device

Security Connector – The first security ISO APP

Technology Behind the App

Clarity (AMP for Endpoints)

Enable audit of iOS device users and their applications

Visibility into usage and network resources accessed by mobile apps

First vendor to get this level of access to iOS

Licensed by number of devices

Umbrella

Ensure all DNS requests are sent to Umbrella

Adds protection when iOS users are off-network; on public Wi-Fi and cellular networks

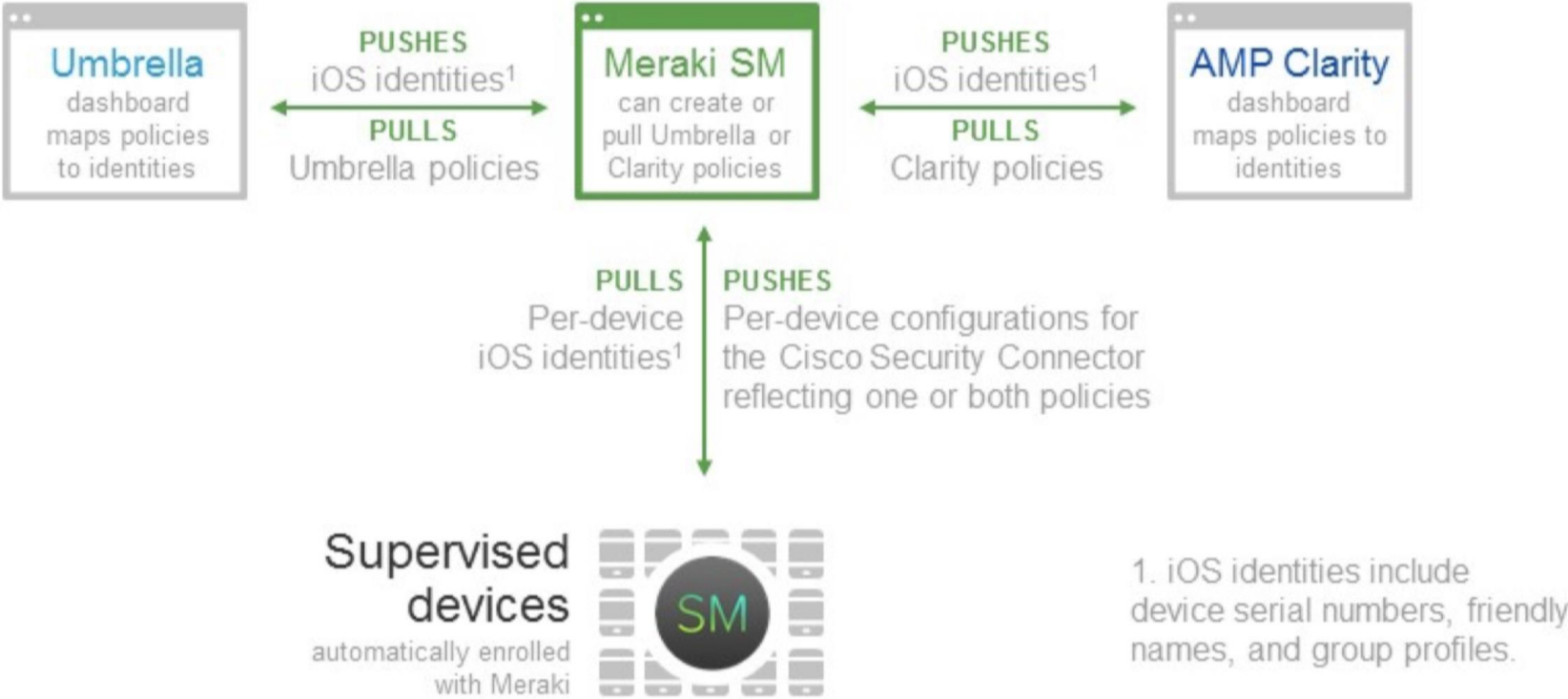
Simplest, most user friendly solution in the market

Licensed by number of user seats

Security Connector – The first security ISO APP

Seamless UX for admin-users

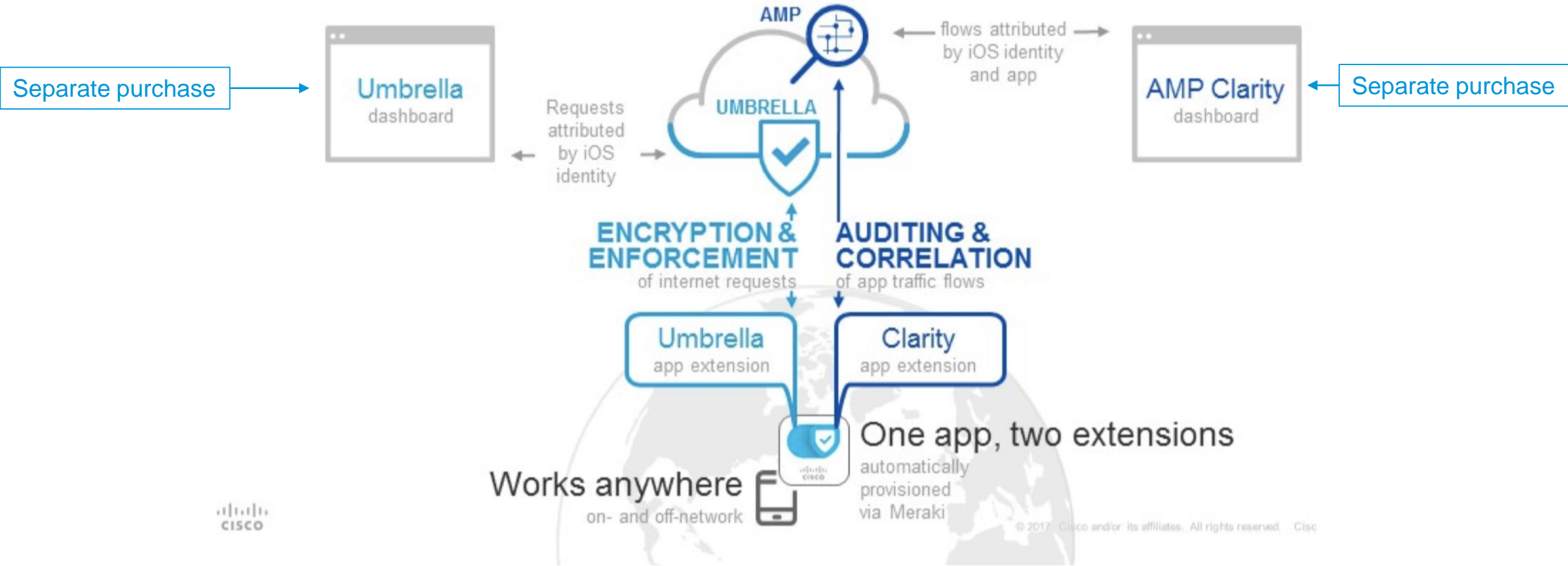
One-time registration syncs all products together



Security Connector – The first security ISO APP

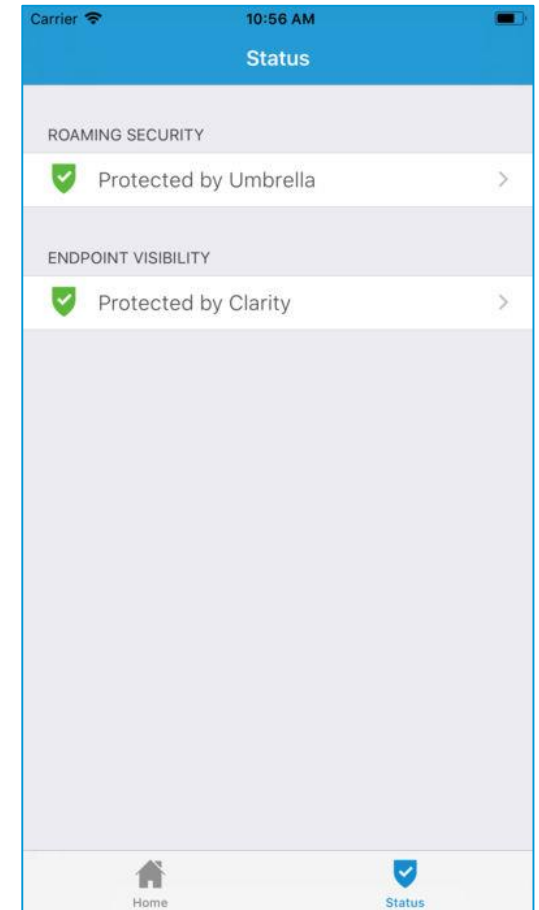
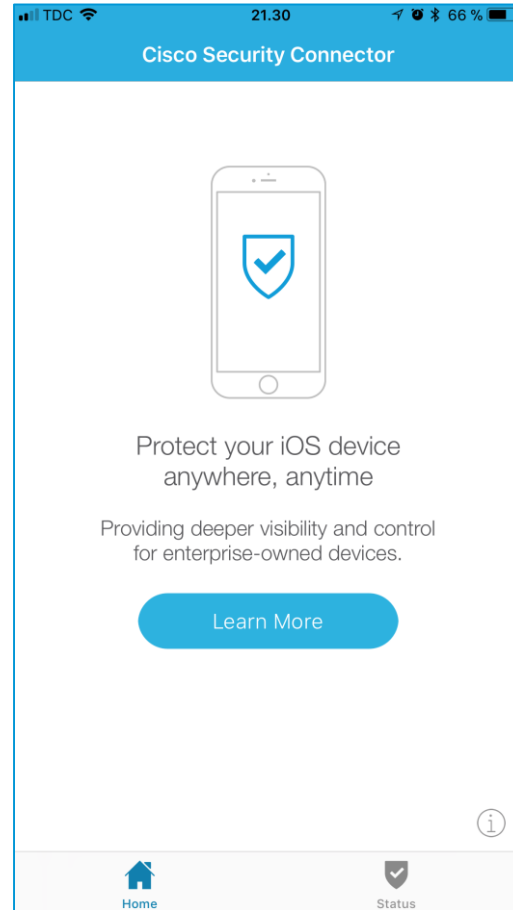
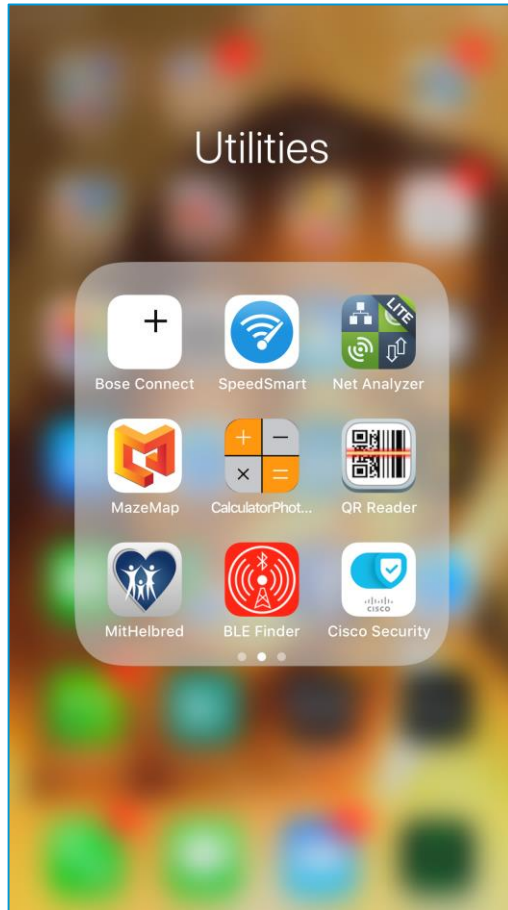
Zero-touch UX for end-users

Visibility, control, and privacy



© 2017 Cisco and/or its affiliates. All rights reserved. Cisco

Security Connector – The first security ISO APP



Provision and Monitor devices centrally

Introducing Do Not Disturb

Schedule when changes won't be applied

- Point of Sale devices don't receive app & profile updates during business hours
- Students don't receive app updates during class
- Only push OS updates after hours



Provision and Monitor devices centrally

Introducing support for Apple TV

Manage Apple TV with Cisco Meraki Systems Manager

- Use Apple TV to display content in stores, office buildings, and classrooms
- Wirelessly share iOS and macOS content to Apple TV with AirPlay



Cisco Meraki Cloud controlled MDM - LIC

Enterprise License



Experience the Benefits of Cloud Management

Cisco Meraki MR Series

1. 24/7 – 365 support included.
2. All EMM features available.
3. New features auto updated in the Dashboard.
4. Purchase for 1, 3, 5yr

Cloud Managed Security Cameras



Centralized Cloud Management

The Meraki dashboard provides secure monitoring and management of all your cameras from anywhere in the world.



Edge Storage

128GB of high write endurance solid state storage on each camera eliminates the need for an NVR.



Optimized Retention

Use motion-based retention and scheduled recording to customize video storage plans for every deployment.



Advanced Analytics

Industry-leading analytics and machine learning capabilities onboard each MV12.



Motion Search

Dynamically and retroactively select areas of interest in a video stream to find that missing laptop, then export clips directly from the dashboard.



Encrypted By Default

Video is encrypted at rest and during transport by default, with automated TLS certificate provisioning.



Granular Access Controls

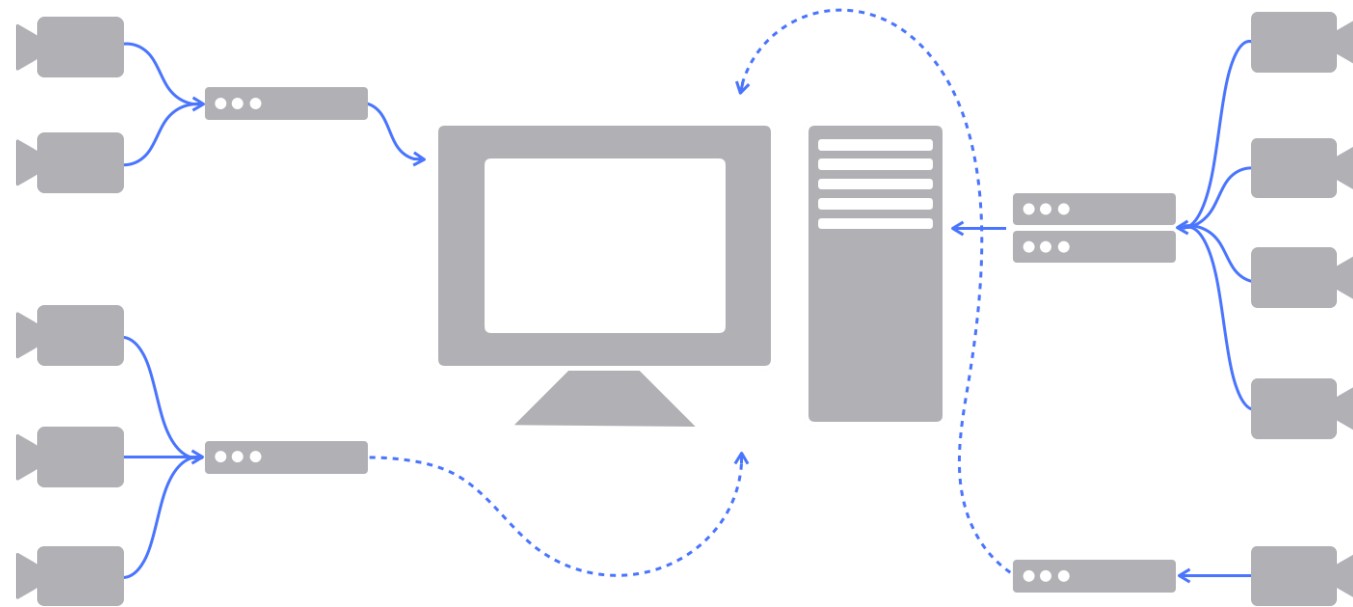
Easily define who can see which video streams, view historical footage, and export video, all from the dashboard.



Firmware Always Up-to-Date

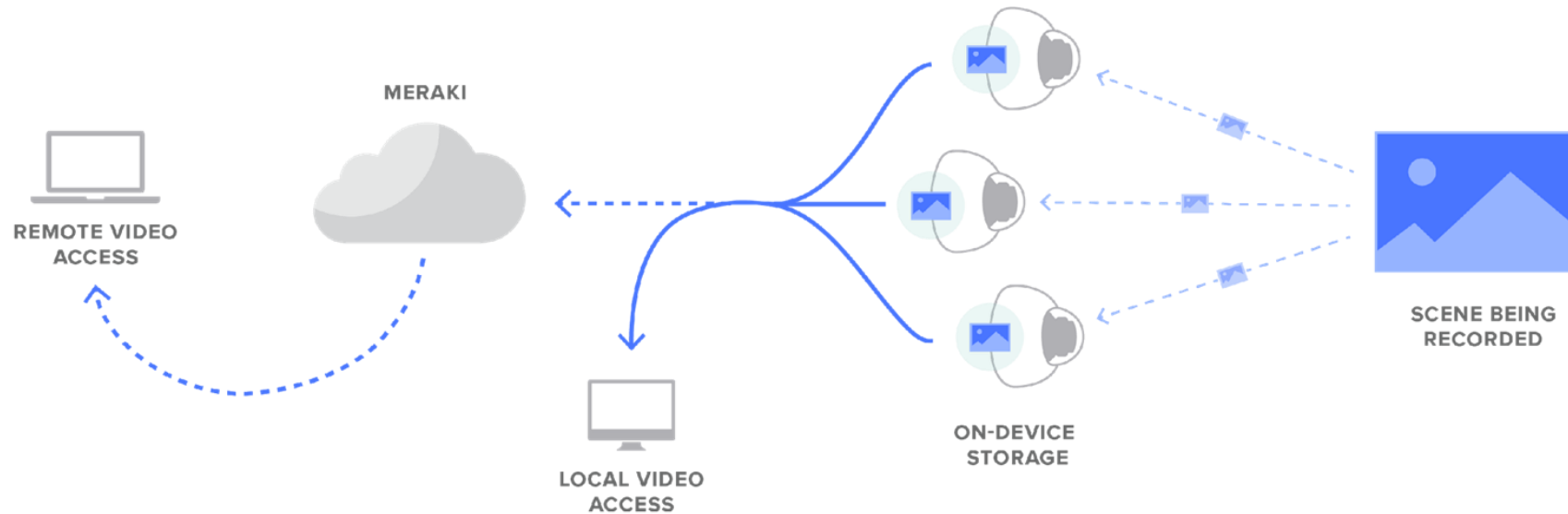
Feature releases, firmware updates, and bug fixes are always pushed automatically and at no additional cost with active license.

A Traditional Security Camera Deployment



Network video recorders (NVRs), servers, on-premises hardware
Multiple software packages, manual configuration, and **complexity**
Huge network vulnerability

1 Year Ago, Meraki Launched MV



Revolutionary architecture

On-board video storage and processing (no NVR)

Automatic video streaming with no standalone software

Focused on solving problems, not building features

But what if your security cameras could do more...?



Optimize which video you keep, and which gets tossed



Better **understand** customer behavior patterns



Learn and provide more insights over time

Utilize cameras as sensors for added business intelligence

Introducing MV12



3 SKUs – 256GB and 128GB storage models

High definition 1080p

Microphone

Wireless capable

Compact form factor

Qualcomm Snapdragon processor

Advanced on-board analytics and machine learning

*A family of indoor
mini dome
cameras designed
with more than just
security in mind*

MV12 Model Details



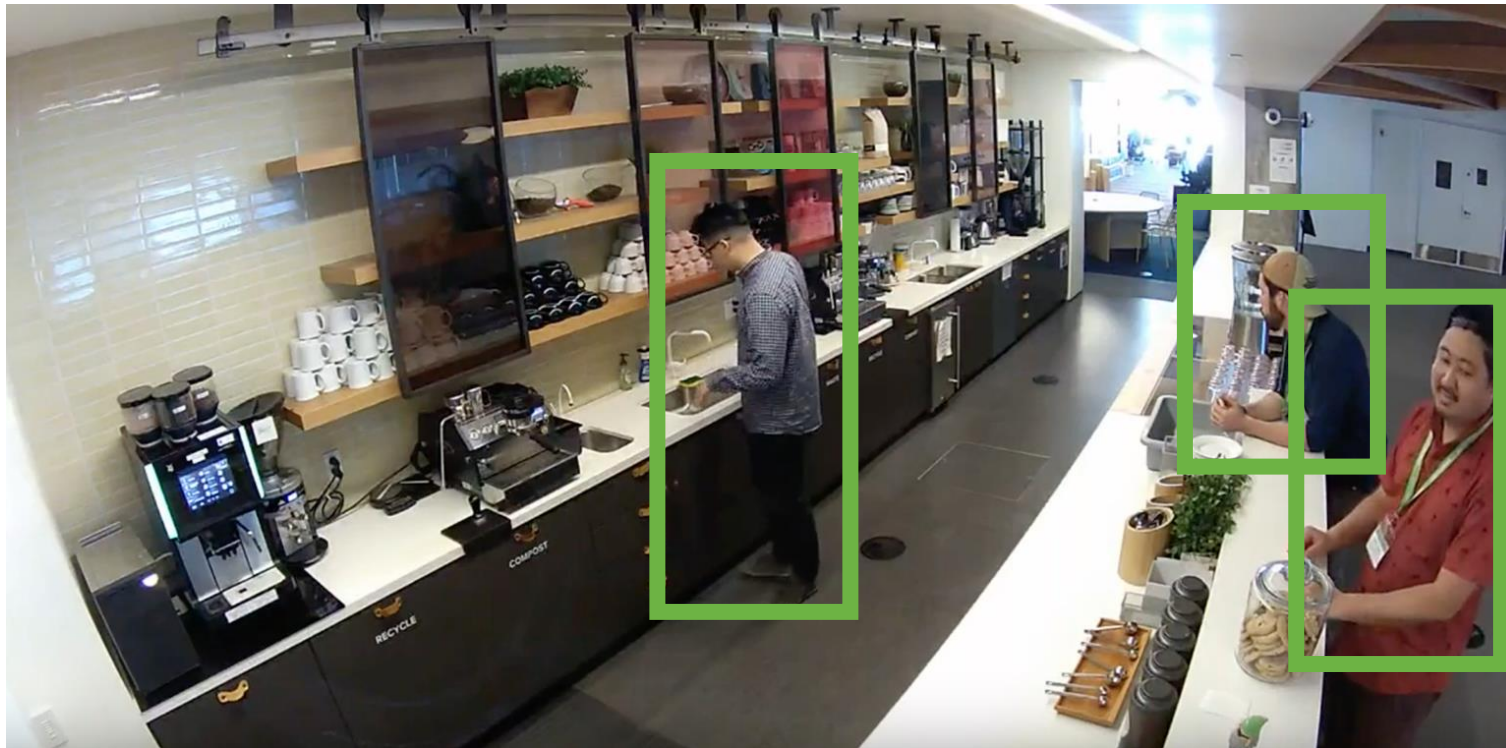
MV12N

MV12W

MV12WE

Storage (GB)	256	256	128
Field of View	Narrow	Wide	Wide
Use Case	Doorways	Whole Room/Area	Entry-Level Option
Resolution	1080p	1080p	1080p
List Price (USD)	\$1199	\$1199	\$999

Object Detection



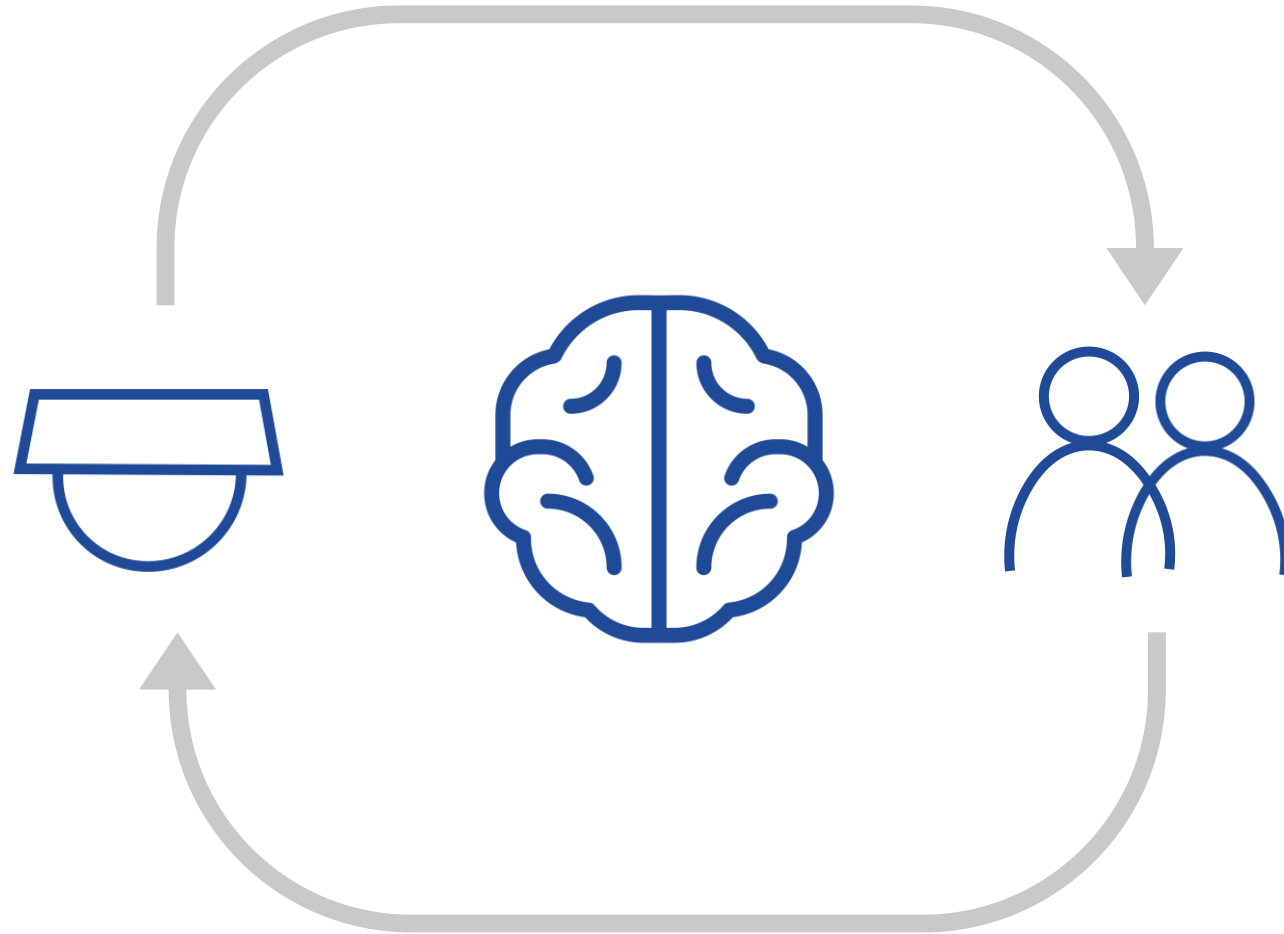
FUNCTIONALITY:

Anonymized person detection for business intelligence

EXAMPLE USE CASE:

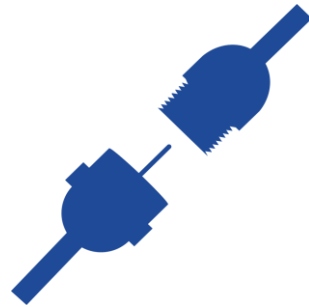
Better understand in-store customer behavior patterns

What is machine learning?



More Functionality with Less Effort

Replace your legacy analog deployment without re-cabling:



Power from existing cables +
Meraki power converter



All data (management, video,
metadata) travels wirelessly

True “rip & replace” of outdated deployments with minimal downtime

The MV Lineup



MV12

Fixed lens (3 SKUs)
Compact form factor
Advanced analytics



MV21

Varifocal (zoom capable)
Easy installation
Multipurpose



MV71

Varifocal (zoom capable)
IP66/IK10 rated
Demanding environments

INDOOR

OUTDOOR

MV12

AVAILABLE SPRING 2018

Cisco Meraki Cloud controlled SEC/CAM - LIC

Enterprise License



Experience the Benefits of Cloud Management

Cisco Meraki MR Series

1. 24/7 – 365 support included.
2. Next Business Day HW Replacement.
3. All MV features available.
4. Firmware updates ready on appliance.
5. New features auto updated in the Dashboard.
6. Purchase for 1, 3, 5, 7 or 10yr – Not locked to HW
7. Cisco Meraki NOW – 24/7-2-OS Support **

**Additional service purchase
expected MAY18

Introducing ...

Meraki Insight

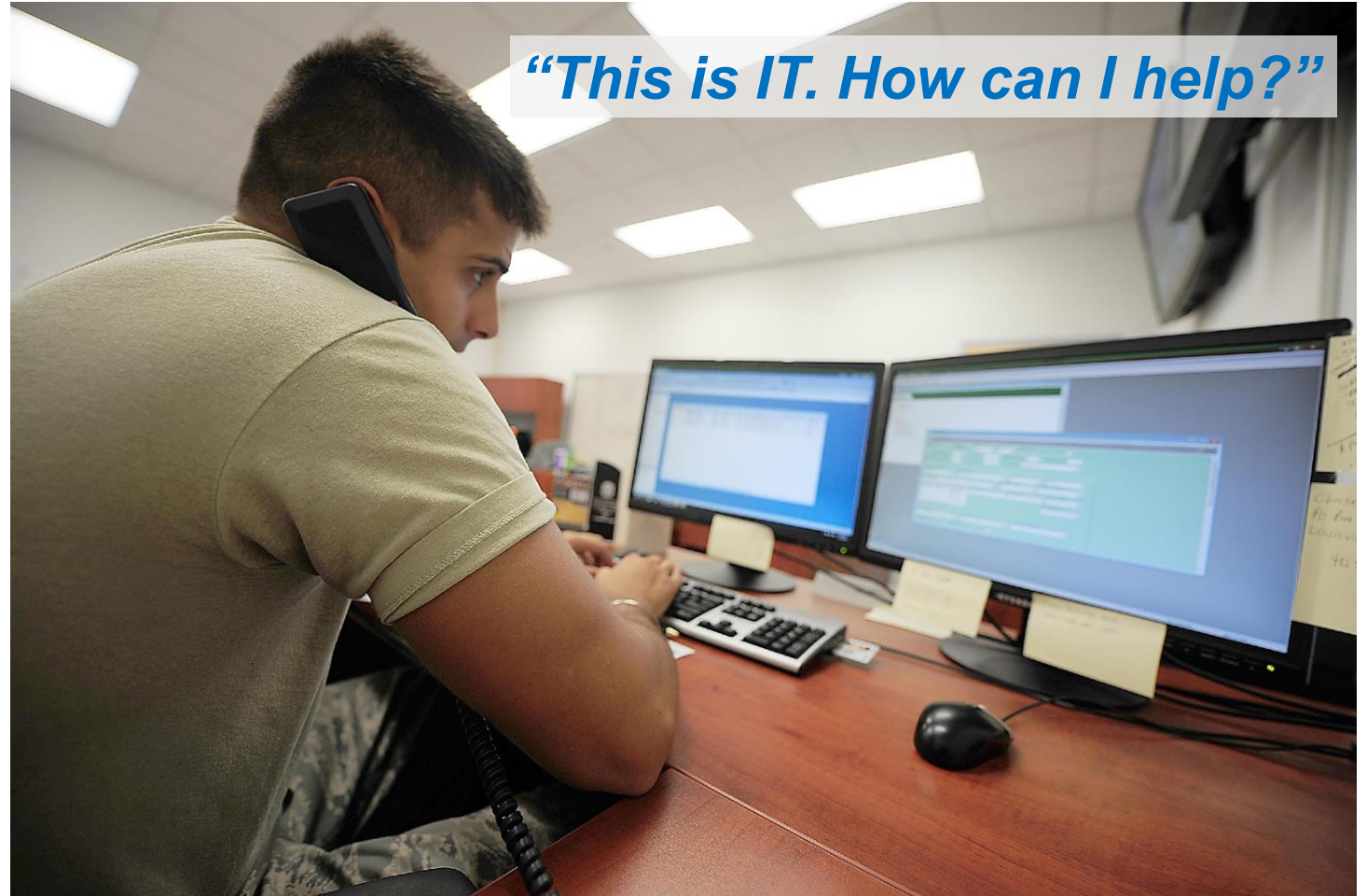


Sound familiar?

“The network’s slow”

“My Wi-Fi is broken”

“My Internet is down”



“This is IT. How can I help?”

Contributors to bad end user experience

Internal

LAN congestion

Rogue actors

Network design

Network capacity limits

External

WAN congestion

Application errors

Application server processing time

Authentication / DNS server response time

Contributors to bad end user experience

LAN congestion

Deploy Meraki tools (Traffic shaping, QoS, Air Marshal)

Rogue actors

Network design

Network capacity limits

WAN congestion

Application errors

Application server processing time

Authentication / DNS server response time

Contributors to bad end user experience

LAN congestion

Rogue actors

Network design

Network capacity limits

Address with training, more infrastructure

WAN congestion

Application errors

Application server processing time

Authentication / DNS server response time

Contributors to bad end user experience

LAN congestion

Rogue actors

Network design

Network capacity limits

WAN congestion

Application errors

Application server processing time

Authentication / DNS server response time

Apply Meraki Insight

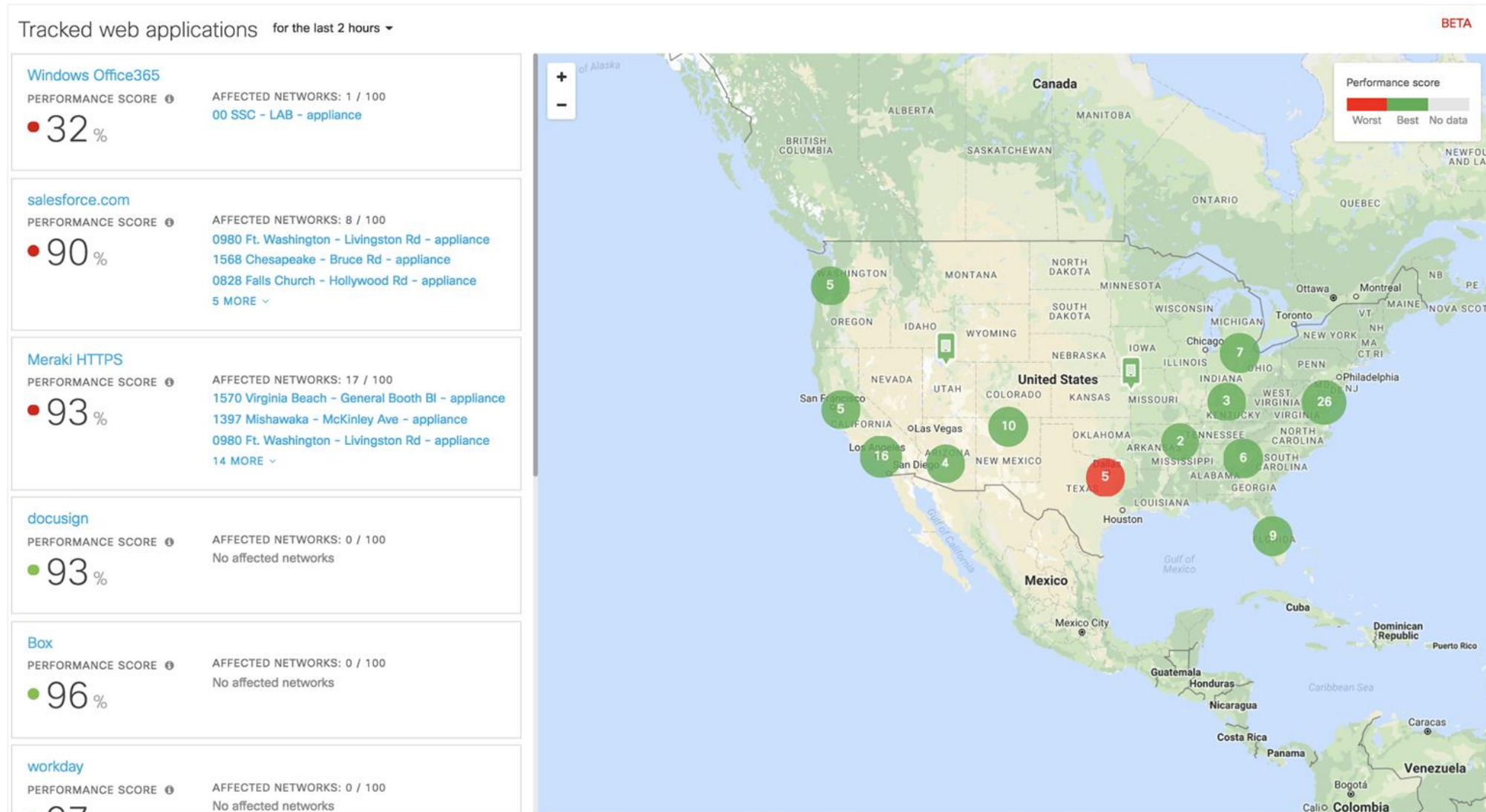
Meraki Insight

Provides end-to-end visibility into how your end-users are experiencing their **SaaS applications**

Assists with application performance management and troubleshooting

How does this differ from what is built in? This offers **data for external factors**, including the entire Wide Area Network, ISPs and SaaS applications like Office 365, Salesforce.com, etc...

Meraki Insight in the dashboard



Meraki Insight in the dashboard

Tracked web applications for the last 2 hours ▾

Windows Office365

⚙ EDIT

PERFORMANCE SCORE ⓘ

AFFECTED NETWORKS: 1 / 100

00 SSC - LAB - appliance

● 32%

Network: 98%
Application: 32%

Insight into both the network and application layers

00 SSC - LAB - appliance

PERFORMANCE SCORE ⓘ

CLIENTS BY NETWORK-LAYER SCORE

● 26%

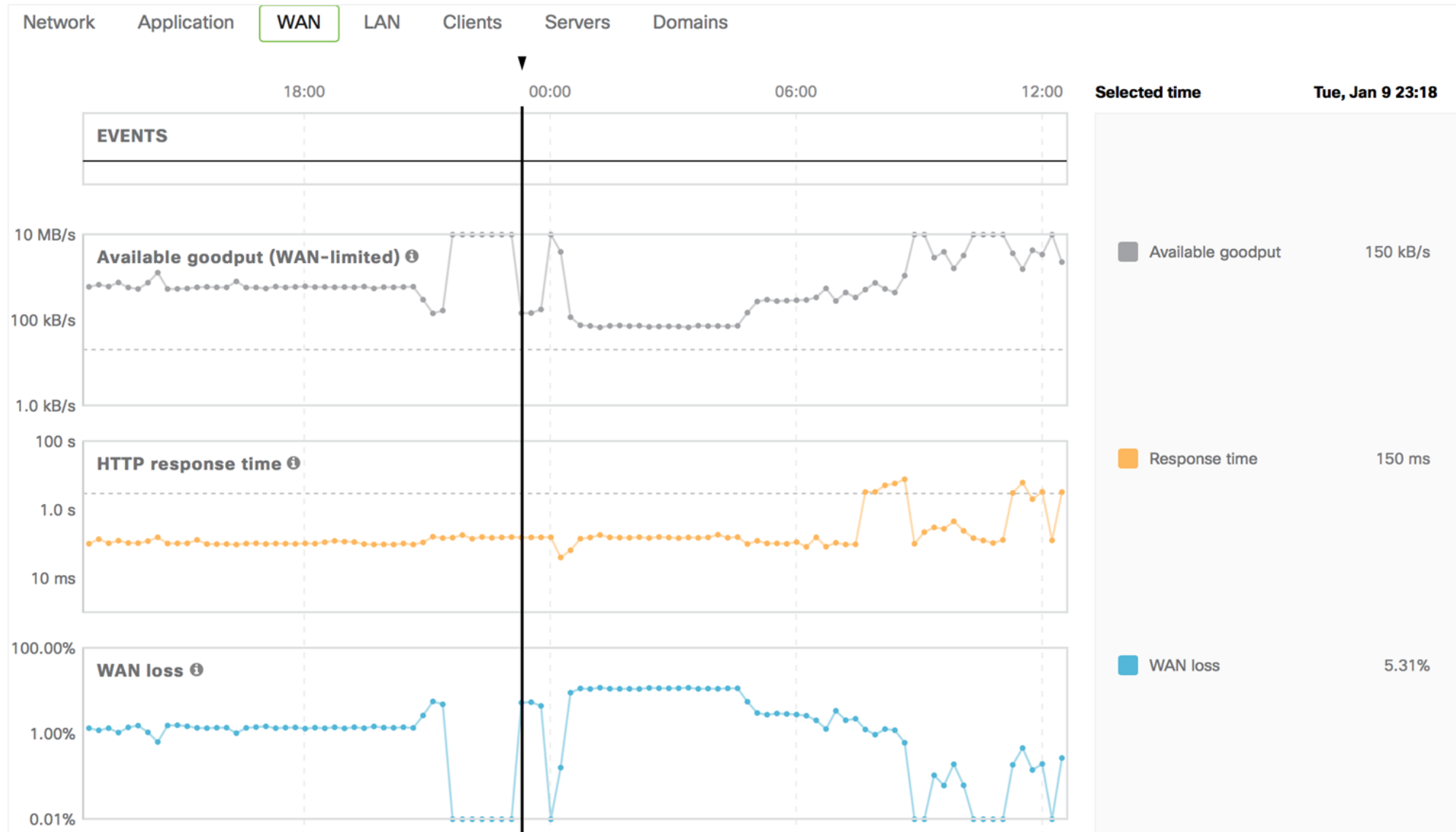


CLIENTS BY APPLICATION-LAYER SCORE



[VIEW TRENDS](#)

Meraki Insight in the dashboard



Introducing our first probe for Meraki Insight

The MX Series



Available Spring 2018

SKU	Length of Term (Years)	Max Throughput	Minimum Hardware Spec
LIC-MI-S-1Y	1	200 Mbps	MX6x
LIC-MI-S-3Y	3	200 Mbps	MX6x
LIC-MI-S-5Y	5	200 Mbps	MX6x
LIC-MI-M-1Y	1	500 Mbps	MX84/100
LIC-MI-M-3Y	3	500 Mbps	MX84/100
LIC-MI-M-5Y	5	500 Mbps	MX84/100
LIC-MI-L-1Y	1	2 Gbps	MX250
LIC-MI-L-3Y	3	2 Gbps	MX250
LIC-MI-L-5Y	5	2 Gbps	MX250
LIC-MI-XL-1Y	1	>2 Gbps	MX450
LIC-MI-XL-3Y	3	>2 Gbps	MX450
LIC-MI-XL-5Y	5	>2 Gbps	MX450

Today's announcements give Cisco Meraki customers more options and pave the way to the exciting next phase of the Meraki journey – building a smarter network.

Smarter hardware: New security cameras and access points

Expanding software: New ways to measure client experience

The Meraki Full Stack



MR
Access Points



MX
Security Appliances



MS
Ethernet
Switches



Systems Manager
EMM



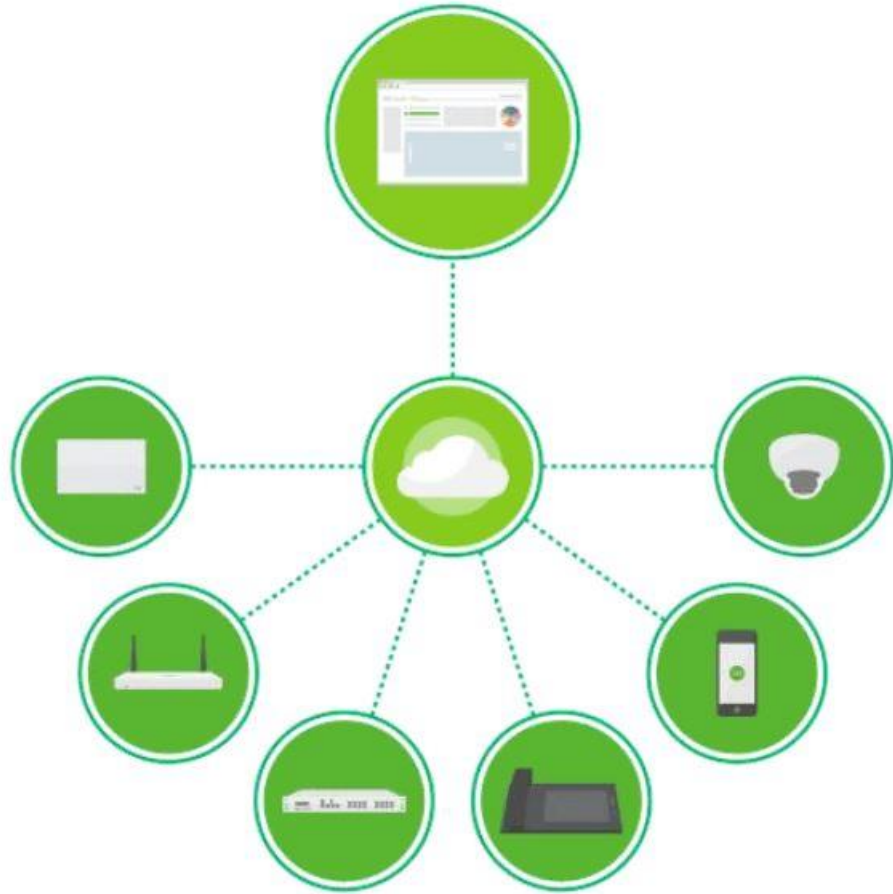
MC
Communications



MV
Security Cameras

A complete cloud managed IT portfolio
Single pane of glass management

Simplifying across IT with cloud management



Questions?

Thank you.

