



# Wireless Security and Guest Access

Cisco Meraki Webinars Series





# Agenda

Introduction

Live demo

Cisco Meraki architecture

Case studies

Key design considerations

Cisco Meraki product line

Q&A

# Free APs for IT Professionals



Meraki 802.11n AP with 3-year  
cloud management license

[Click on this link to attend any Cisco Meraki live webinar and Cisco will send qualified attendees a free Meraki Wi-Fi Access Point \(AP\) with a 3-year cloud management license - a \\$699 MSRP value free.](#)

... or [click on this personalized referral link](#) for the current schedule for all the live webinars and recorded sessions.

# About Cisco Meraki

# Company Information

Leader in cloud networking: 20,000+ customer networks deployed

- Founded in 2006 at MIT - tradition of innovation and R&D
- 330 employees worldwide

Cloud-managed edge and branch networking portfolio

- Complete line of wireless, switching, security, WAN optimization, and mobile device management products

Cisco acquired Meraki for \$1.2 billion, form Cloud Networking Group

- Increase investment in Meraki technology (grow team, R&D)
- Utilize Cisco's reach to bring Meraki to new markets
- No changes planned to pricing, licenses, product roadmap, etc.

Trusted by thousands of customers worldwide:



# Recognized for Innovation

**Gartner**

Visionary, Magic Quadrant for Wired and Wireless LAN



2012 Technology of the Year



25 Coolest Emerging Vendors for 2012  
Top 100 Executives – CEO Sanjit Biswas



Mobility / Wireless Product of the Year

# Why cloud managed WiFi?

# Cloud increases IT efficiency



Manageability



Scalability



Cost Savings

- Turnkey installation and management
- Integrated, always up to date features
- Scales from small branches to the campus
- Reduces operational costs

# Bringing the cloud to enterprise networks



Cisco Meraki MR  
Wireless LAN



Cisco Meraki MX  
Security  
Appliances

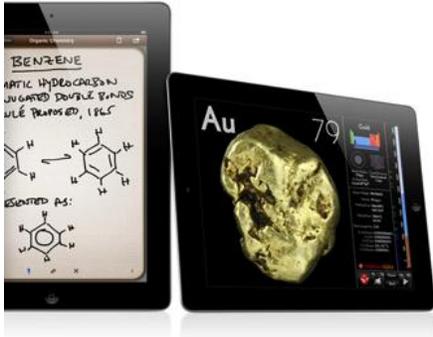


Cisco Meraki MS  
Ethernet  
Switches



Cisco Meraki SM  
Mobile Device  
Management

# Solving new IT challenges



350 million iOS devices



Integrated Device Management



New business applications



Turnkey Security and Guest Access



Video and rich media

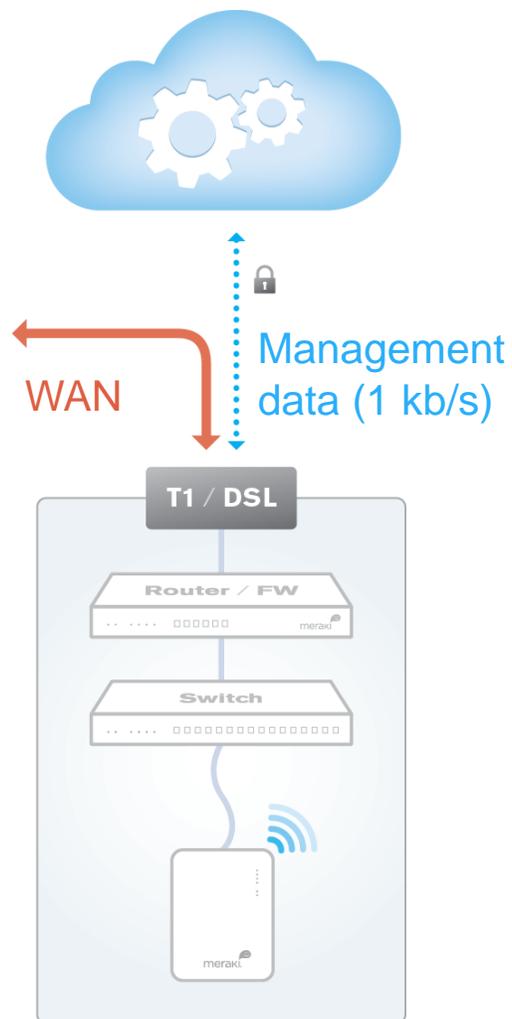


Layer 7 Application QoS

# Live Demo

# Cloud Networking Architecture

# Cisco Meraki's out-of-band control plane



## Scalable

- Unlimited throughput, no bottlenecks
- Add devices or sites in minutes

## Reliable

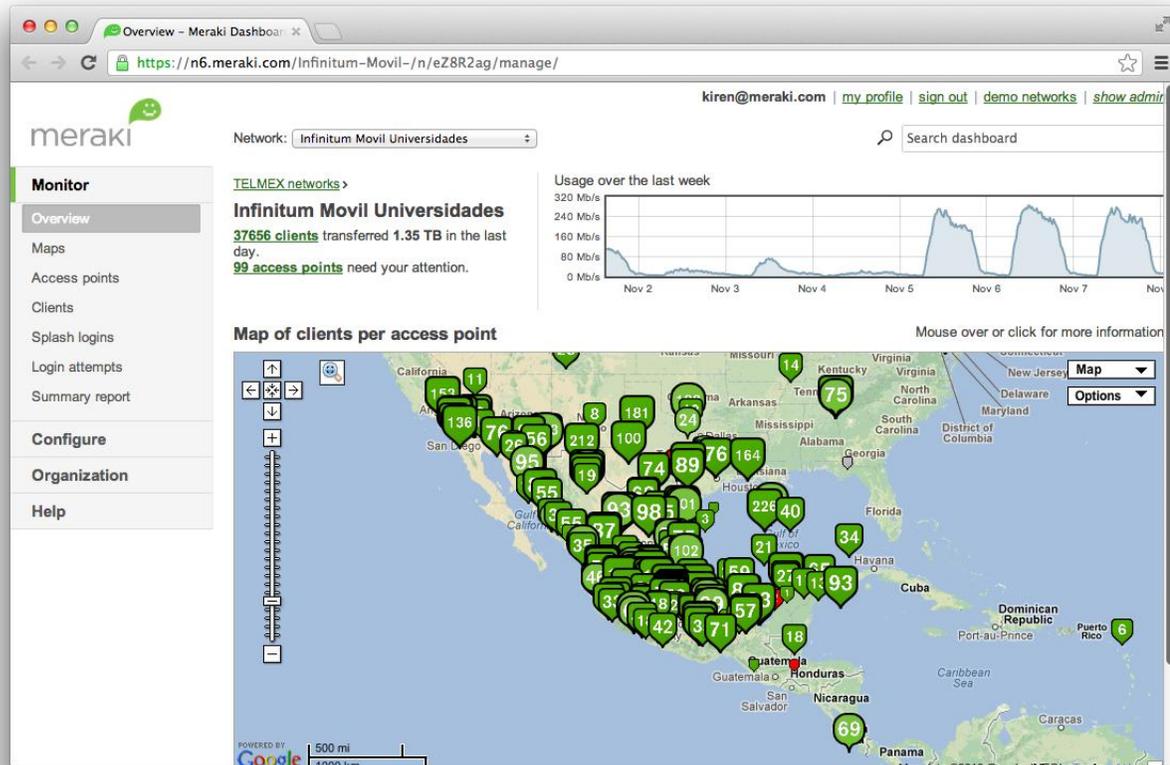
- Highly available cloud with multiple datacenters
- Network functions even if connection to cloud is interrupted
- 99.99% uptime SLA

## Secure

- No user traffic passes through cloud
- Fully HIPAA / PCI compliant (level 1 certified)
- 3<sup>rd</sup> party security audits, daily penetration test

*Reliability and security information at [meraki.com/trust](http://meraki.com/trust)*

# Scalable cloud infrastructure



## Telmex

Nationwide hotspot and 3G offload network

## Next Retail

550 retail stores across the UK

## Motel 6

70,000 hotel room deployment

## Jeffco School District

80,000 student district with 100+ schools

Proven in 10,000+ device deployments

# SaaS feature delivery, quarterly updates

Search:   [Advanced search >](#) [Help](#)

951 client devices Select: **All**, None  [Columns...](#) [Download as XML](#)

Status	Description	Manufacturer	Open
<input type="checkbox"/>	1  Gregg	Intel	Win
<input type="checkbox"/>	2  Jenny-PC	Intel	Win
<input type="checkbox"/>	3  GOD	AzureWave	Oth
<input type="checkbox"/>	4  MacBook	Apple	Mac
<input type="checkbox"/>	6  kstephens Mac	Apple	Mac

**User/device fingerprinting**

LDAP membership:

Blocked web content:

Teachers:

**Content filtering**

Client details [Edit details](#) [Refresh details](#)

System name: Meraki Marketing iPad  
 Operating system: iOS 5.0.1  
 System model: iPad  
 BIOS: 9A405  
 Serial: V5048RTXZ38  
 Warranty: Apple  
 Capacity: 16GB  
 Free space:

Tags:

Battery charge:

Recent locations

**Mobile application deployment**

Applications

VoIP & video conferencing—Skype  
114.9 GB (↓ 51.9 GB, ↑ 63.0 GB)

Video 38.1%  
Miscellaneous 21.0%

**Application firewall**

Date	Scan result	AV	Running	Client IP
May 15 17:34	Passed	Norton Internet Security	Yes	10.254.92.19
May 30 18:24	Passed	Norton Internet Security	Yes	10.254.92.19
May 27 09:07	Passed	McAfee VirusScan	Yes	10.74.112.40
May 27 09:07	Passed	McAfee VirusScan	Yes	10.74.112.40
May 27 09:07	Passed	McAfee VirusScan	Yes	10.74.112.40
May 16 09:03	Passed	McAfee VirusScan	Yes	10.247.49.95
May 16 09:03	Passed	McAfee VirusScan	Yes	10.247.49.95
May 12 10:58	Passed	Microsoft Security Essentials - 2.1.6805.0	Yes	10.123.104.174

**Network access control**

Link compression: Enabled  
 Application accelerators: HTTP, CIFS, and FTP accelerators enabled.  
 Byte-level object cache: Using memory and disk. This device currently has 1.12 GB of data cached for traffic optimization.

32 Mb/s  
24 Mb/s  
16 Mb/s  
8 Mb/s  
0 Mb/s

12:54 12:56

Client bandwidth 281.0 MB  
Uplink bandwidth 5.8 MB

**WAN optimization**

# Case studies

# PCI compliant WiFi for shoppers and staff



UNITED COLORS  
OF BENETTON.

WiFi in Corporate HQ and Flagship Stores

*"The dashboard is fantastic, including its analytics"*

Mark Bishop, IT Manager

## PCI Compliant Wireless LAN

Built-in stateful firewall isolates corporate traffic from guests

Cloud-hosted splash pages create marketing opportunities in retail

## Application-Level QoS

Prevents bandwidth-intensive applications from compromising network experience

Business apps prioritized

Video, gaming, P2P traffic throttled

# Secure employee and guest access



FOSTER PEPPER FLLC

Secure WLAN for attorneys and clients

*"It was plug and play, and there were no new complex systems to learn"*

Lucas Clara, IT Director

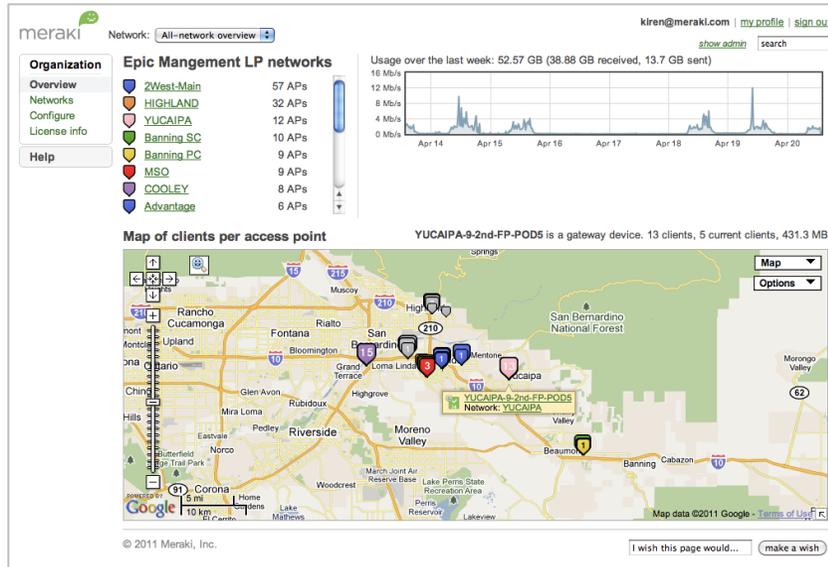
## 802.1X/RADIUS employee access

Industry-standard encryption and access control for attorney-client data  
Supports laptops and iPads

## Internet-only guest access

LAN isolated/protected from guests  
Custom splash page provides Ts and Cs

# HIPAA-compliant medical and patient access



Centrally managed wireless LAN across 22 distributed hospitals and clinics

*“With Meraki, we can take the equipment to a new facility and get the site up and running overnight.”*

Michael Crabtree, IT Manager

HIPAA-compliant security for doctors and patients

Virtual guest network provides Internet access for patients

WPA2-Enterprise secured wireless LAN for medical carts and tablets

Distributed sites centrally managed from the cloud

Network-wide visibility and control

Built-in monitoring and alerts

# Design Considerations

# Security design considerations

## Account protection

### Wireless security

Encryption and admission control

User and content-aware firewall

Guest access

NAC

Rogue AP detection and prevention

## BYOD networks

# Account Protection

# Account security protections

The image shows a Meraki account security interface. At the top left is the Meraki logo. Below it, the heading "Enter verification code" is followed by instructions: "A text message (SMS) has been sent to your phone number ending in 25. To verify your identity on this computer, check your phone and enter the code provided." There is a text input field for the code and a "Verify" button. Below the input field is a checked checkbox for "Remember verification for this computer for 30 days." A link "Didn't receive the text message? Get a new verification code" is also present. To the right, a "Security" settings panel is shown with the following options:

Security	
Password expiration	<input checked="" type="checkbox"/> Force users to change their password every <input type="text" value="60"/> days
Used passwords	<input checked="" type="checkbox"/> Force users to choose passwords different from their past <input type="text" value="5"/> passwords
Strong passwords	<input checked="" type="checkbox"/> Force users to choose strong passwords for their accounts <a href="#">What is this?</a>
Two-factor authentication	<input checked="" type="checkbox"/> Force users to set up and use two-factor authentication <a href="#">What is this?</a>

- Two-factor authentication
  - Protection from compromised passwords
  - SMS / Google Auth design eliminates RSA tokens
- Enforce password strength

# Change management features

meraki Network: All-network overview kiren@meraki.com | my profile | sign out show admin search

Organization  
Overview  
Networks  
Configure  
Change log  
License info  
Help

Meraki Network Ops change log

Search: Bret Hull Go Help

Time	Admin	Network	SSID	Page	Label	Old value	New value
Jun 30 14:34	<a href="#">Tom Miller</a>	<a href="#">Tom Miller Home</a>		Overview	Tom ShoreTel enabled	disabled	enabled
Jun 30 14:34	<a href="#">Tom Miller</a>	<a href="#">Tom Miller Home</a>		Overview	Tom Meraki-Corp enabled	disabled	enabled
Jun 24 19:54	<a href="#">Chris Hilsenbeck</a>	<a href="#">Jeeta Home</a>		Overview	SSID name	personall	personal
Jun 24 19:54	<a href="#">Chris Hilsenbeck</a>	<a href="#">Jeeta Home</a>	personall	Access Control	WPA Passphrase		
Jun 24 19:48	<a href="#">Chris Hilsenbeck</a>	<a href="#">Jeeta Home</a>		Overview	SSID name	Chris Meraki-Corp	Jeeta Meraki-Corp
Jun 24 19:48	<a href="#">Chris Hilsenbeck</a>	<a href="#">Jeeta Home</a>		Overview	SSID name	Chris ShoreTel	Jeeta ShoreTel
Jun 24 19:48	<a href="#">Chris Hilsenbeck</a>	<a href="#">Jeeta Home</a>		Overview	SSID name	backcountry	personall
Jun 23 14:39	<a href="#">Chris Hilsenbeck</a>	<a href="#">E Williams Home</a>	personal	Access Control	WPA Passphrase		
Jun 23 14:39	<a href="#">Chris Hilsenbeck</a>	<a href="#">E Williams Home</a>		Overview	SSID name	backcountry	personal
Jun 23 14:39	<a href="#">Chris Hilsenbeck</a>	<a href="#">E Williams Home</a>		Overview	SSID name	Chris Meraki-Corp	Eric Meraki-Corp
Jun 23 14:39	<a href="#">Chris Hilsenbeck</a>	<a href="#">E Williams Home</a>		Overview	SSID name	Chris ShoreTel	Eric ShoreTel
Jun 21 21:30	<a href="#">Chris Hilsenbeck</a>	<a href="#">Cheeon Home</a>	personal	Access Control	WPA Passphrase		
Jun 21 21:30	<a href="#">Chris Hilsenbeck</a>	<a href="#">Cheeon Home</a>		Overview	SSID name	Thomer Meraki-Corp	Cheeon Meraki-Corp
Jun 21 21:30	<a href="#">Chris Hilsenbeck</a>	<a href="#">Cheeon Home</a>		Overview	SSID name	Thomer ShoreTel	Cheeon ShoreTel
Jun 17 18:29	<a href="#">Bret Hull</a>	<a href="#">Systems Manager</a>			Enabled alerts	- any -	test
Jun 17 15:58	<a href="#">Tom Miller</a>	<a href="#">Tom Miller Home</a>	strangelove2	Access Control	WPA Passphrase		
Jun 17 15:57	<a href="#">Tom Miller</a>	<a href="#">Tom Miller Home</a>		Overview	Tom Meraki-Corp enabled	enabled	disabled
Jun 17 15:57	<a href="#">Tom Miller</a>	<a href="#">Tom Miller Home</a>		Overview	Tom ShoreTel enabled	enabled	disabled
Jun 17 15:57	<a href="#">Tom Miller</a>	<a href="#">Tom Miller Home</a>		Overview	SSID name	Tom Personal	strangelove2

- Audit configuration changes
- Delegate and control privileges (role-based administration)
- Email alerts on configuration changes

# Wireless Security

# OTA encryption



# Admission control: who can join the network?

## WPA2 PSK

- Easy to deploy, no integration
- Best for small networks (does not scale)

## WPA2 Enterprise/802.1X

- Scalable, fine-grained
- RADIUS integration: Active Directory, LDAP, etc

## Native Active Directory/LDAP integration

- Scalable
- Easy to deploy: no RADIUS configuration
- Requires splash page

# Access control: what can they access?

NAT mode with LAN isolation: Internet only

Bridge mode: access LAN or VLAN

- VLAN tagging: tie SSID to a VLAN
- Firewall rules: restrict IP ranges
- Policy firewall: identity, device-based firewall rules



Example policy firewall rules:

**Students:** Internet only, via content filter

**Teachers:** Internet only, bypass content filter

**Staff:** Internet and internal servers

# Layer 3-7 stateful firewall

**Firewall & traffic shaping**

SSID:

**Firewall**

Layer 3 firewall rules

#	Policy	Protocol	Destination	Port	Comment	Actions
1	Deny	Any	Local LAN	Any		
2	Allow	Any	Any	Any		

[Add a layer 3 firewall rule](#)

Layer 7 firewall rules

#	Policy	Application
1	Deny	Peer-to-peer (P2P) BitTorrent

[Add a layer 7 firewall rule](#)

**Rule #2**

**Definition**  
This rule will be enforced on traffic matching any of these expressions.

**Bandwidth limit**  
135 Kbps [details](#)

**PCP / DSCP tagging**  
Do not set PCP tag / Do not set DSCP tag

[Add a new shaping rule](#)

Social web & photo sharing  **All Social web & photo sharing**

- Picasa
- Flickr
- smugmug
- imgur.com
- photobucket.com
- ImageShack
- MySpace
- Facebook
- Twitter
- Yelp

or [cancel](#)

User and content aware firewall in every access point

# Guest Access

# Critical requirement: protect local network

## **3 implementation options**

---

Separate network: APs, switches, WAN

- White House Situation Room

Cisco Meraki LAN isolation

- Unique to Meraki
- Secure, deploys in 1 click

VLAN tagging, firewall rules

- More complex, but flexible

Block access to LAN resources (file shares, etc)  
Prevent spread of viruses

# Other options

## Admission Control

- Open, WPA2-PSK, Guest Ambassador

## Click through splash pages

- Show logo, terms of use

## Bandwidth and content restrictions

- Application traffic shaping (limit P2P)
- Adult content filtering

## Time-based SSIDs

# NAC

# Cisco Meraki's built-in NAC

---

Network access control \*

Check clients for antivirus software

Remediation \*

- ✓ Show default NAC failure page
  - Show custom URL
-

# Wireless Intrusion Prevention

# Cisco Meraki Wireless Intrusion Prevention System

Detect and classify APs using multiple heuristics (captured probes, active scans, spectral scans)

- Identify other nearby APs within the network
- Interfering APs from nearby networks

Most importantly: identify rogue spoofing and attacking

- Detect other APs accidentally exposing your wired LAN
- Detect other APs spoofing your SSID
- Detect attacks, such as malicious broadcasts and floods

Rogue containment

- De-authenticate clients, rendering rogue APs ineffective

Prioritized alerts: automatically notify individual or group of admins

# BYOD Networks

# Key Cisco Meraki BYOD technologies

Layer 7 device fingerprinting

Group policy firewall

Guest isolation firewall

NAC with anti-virus scan

Device-based policies

# Flexible, fine-grained policies

## Flexible, fine-grained controls

- Identity, device, location, application

## Complete, integrated solution

- No external appliances, NAC software, etc

## Example policies:

- Retail: block YouTube for company-owned iPads
- Corporate: CEO's iPad on VLAN 20
- Guests: Allow visitor access from any iOS/Android device, but only allow Windows laptops with AntiVirus software
- Teleworker: Allow NetFlix from home but not in branch office

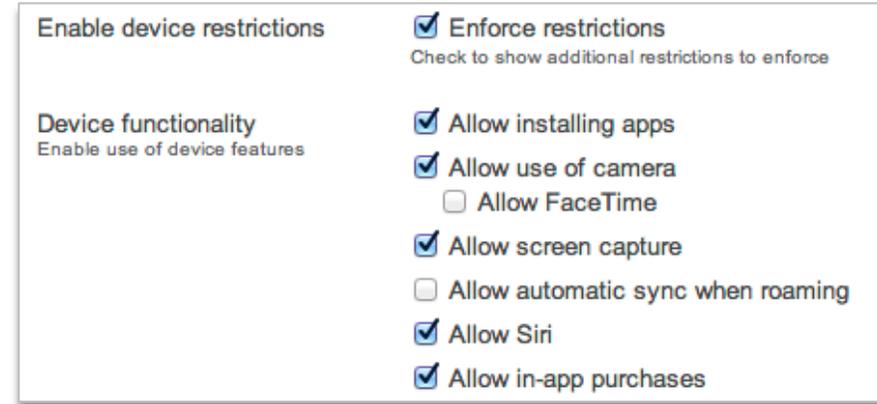
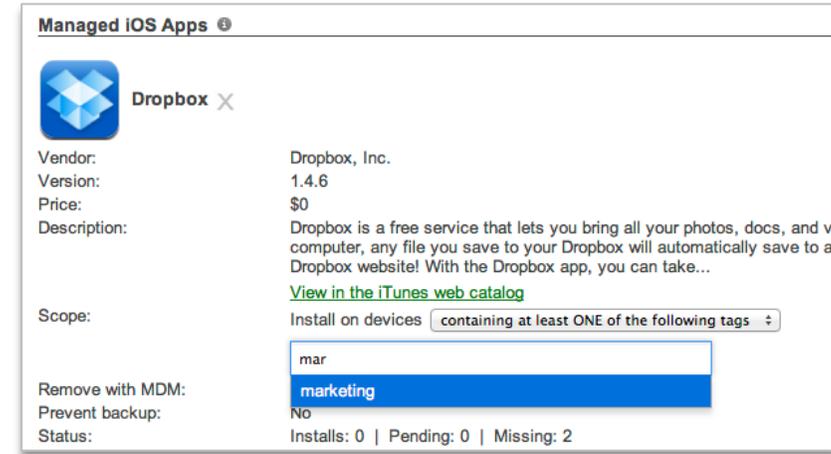
# Control company owned devices

Manage hardware and software inventory

Troubleshoot with remote desktop

iOS and Android management

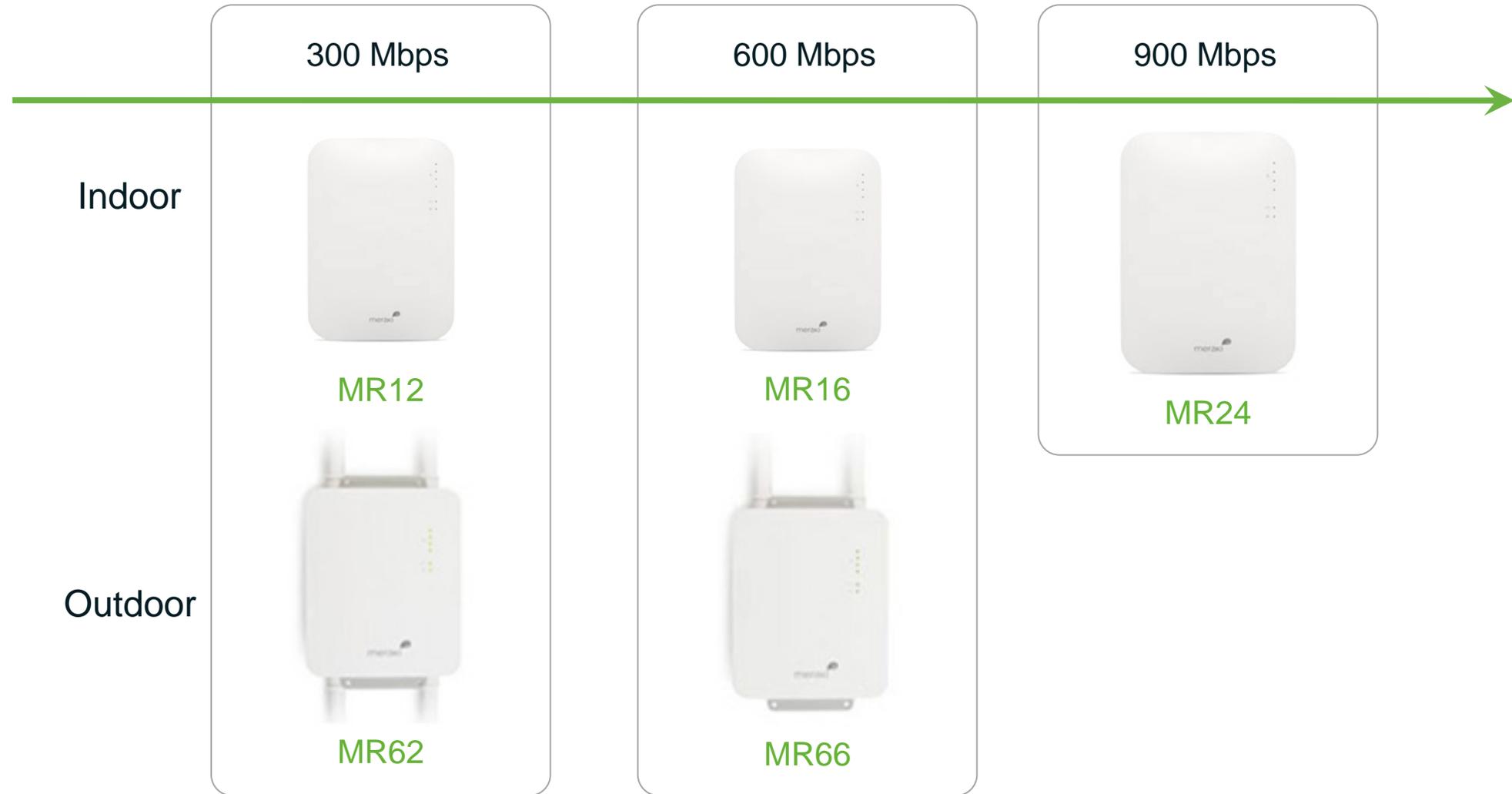
- Deploy apps across thousands of devices
- Set security policies and profiles
- Remote wipe, lock device, etc.



Fully integrated with Cisco Meraki dashboard

# Products

# 5 access point models



# Key features

## Enterprise security and guest access

- Air Marshal™ wireless intrusion prevention
- Secure guest access
- 802.1x / Active Directory integration

## Automatic RF optimization

- AutoRF™ cloud-based performance tuning
- High performance mesh routing

## BYOD control

- User and device-based policies
- Built in MDM
- Automatic device fingerprints

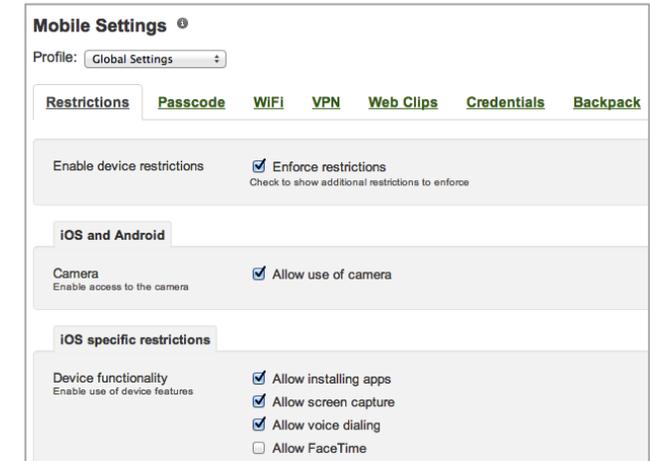
# Other Cisco Meraki product families



MX Security  
Appliances



MS Ethernet  
Switches



SM Mobile Device  
Management

Complete edge and branch hardware portfolio  
Integrated under single cloud-based management dashboard

# Other Cisco Meraki product families



- Multi-site management
- Zero-touch device provisioning
- Seamless firmware upgrades (user-scheduled)
- Summary reports
- PCI compliant
- 99.99% SLA



Networks that simply work

For more information and discount pricing quotations for your project,  
contact 1 PC Network, your authorized Cisco Meraki Elevate Partner.

**[Click here to Register Your New Meraki Projects.](#)**  
**[Qualify for Important Extra Cisco Discounts.](#)**

**[1 PC Network Inc.](#)**

*3675 S. Rainbow Blvd #107-374  
Las Vegas, NV 89103-1059*

*Phone: +1-800-965-8499  
+1-702-949-6077*

*Toll Free, USA  
Las Vegas, NV, USA*