



Introduction to Cloud Managed Networking

Cisco Meraki solution overview



About Cisco cloud-managed networking

Cisco Meraki: a complete cloud-managed networking solution

- Wireless, switching, security, WAN optimization, and MDM, centrally managed over the web
- Built from the ground up for cloud management
- Integrated hardware, software, and cloud services

Leader in cloud-managed networking

- Among Cisco's fastest-growing portfolios: over 100% annual growth
- Tens of millions of devices connected worldwide

Recognized for innovation

- Gartner Magic Quadrant, InfoWorld Technology of the Year, CRN Coolest Technologies

Trusted by thousands of customers worldwide:



Why cloud managed networking?

The cloud increases IT efficiency



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

Cisco Meraki: Bringing the cloud to enterprise networks



Meraki MR
Wireless LAN



Meraki MS
Ethernet Switches



Meraki MX
Security Appliances



Meraki SM
Mobile Device
Management

An integrated solution for new IT challenges



1 billion iOS & Android devices



Integrated mobile device management



HD video and rich media



Layer 7 application shaping



New business opportunities

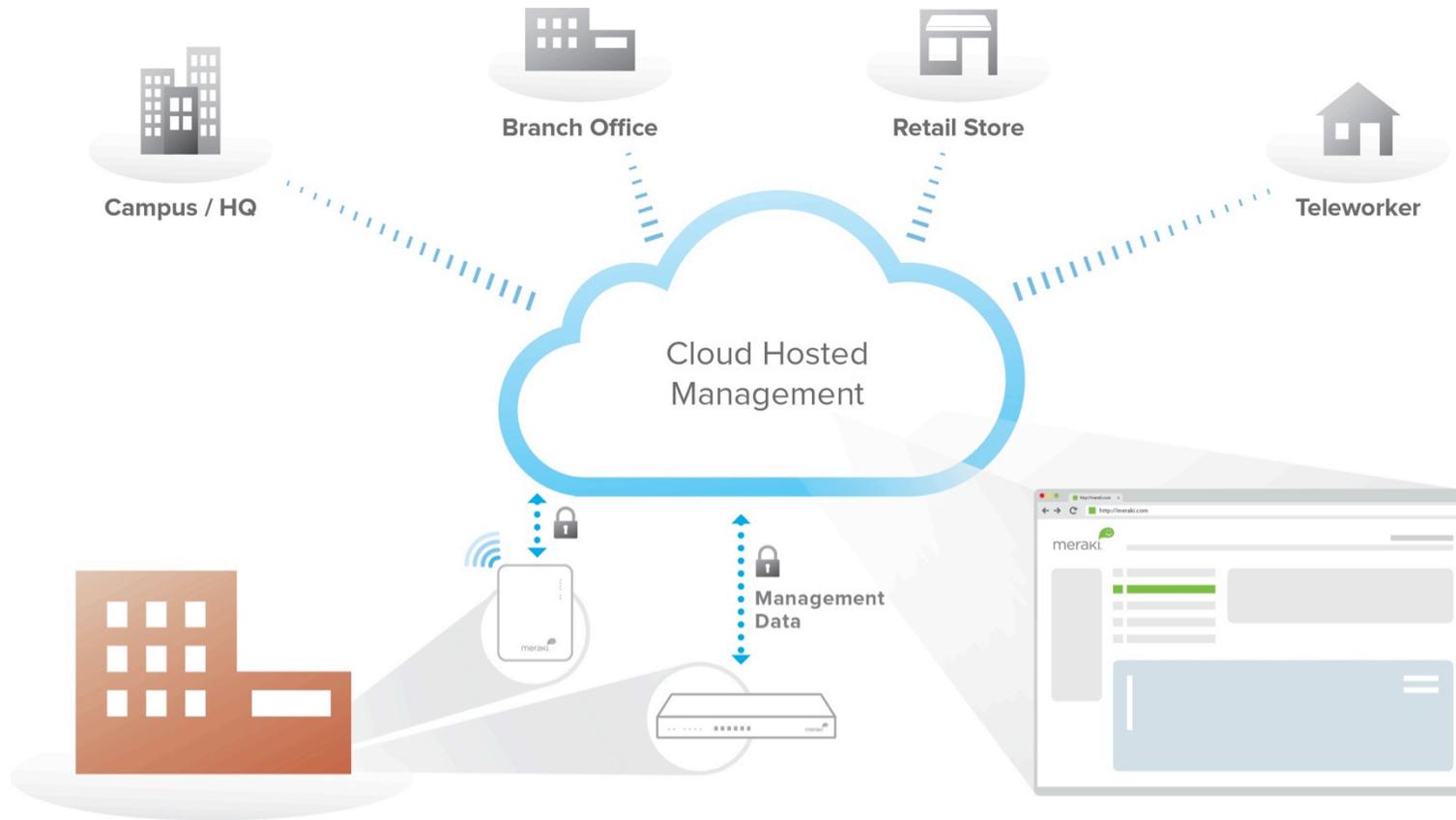


Analytics and user engagement

A complete solution out of the-box:
No extra hardware, software, or complexity

Cloud architecture

Cloud-managed networking architecture

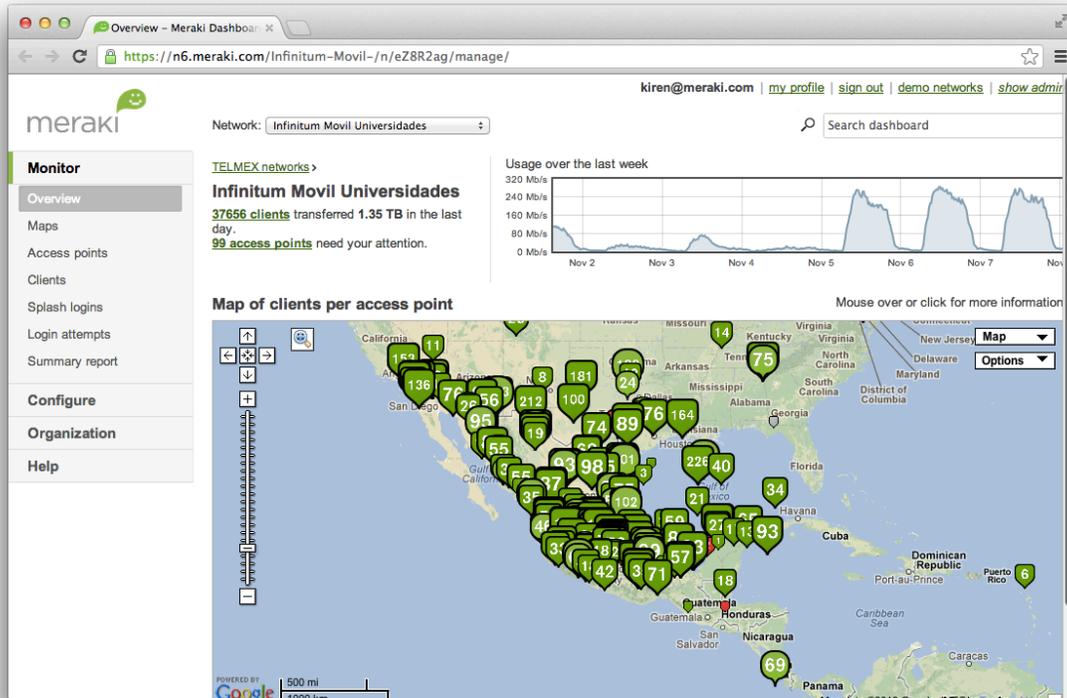


Network endpoints securely connected to the cloud

Cloud-hosted centralized management platform

Intuitive browser-based dashboard

Scalable cloud infrastructure



Telmex

Nationwide hotspot and 3G offload network



Dress Barn

Nation-wide deployment spanning hundreds of retail stores



Motel 6

70,000 hotel room deployment



Jeffco School District 80,000 student district with 100+ schools

Proven in 10,000+ endpoint deployments

Intuitive web-based dashboard

Wired + wireless

Client fingerprints

Application QoS

The screenshot displays the Meraki dashboard interface for a specific client. The browser address bar shows the URL: `https://n7.meraki.com/Meraki-Corp-Wire/n/B4WUfb/manage/usage/list?timespan=604800#c=k506c1c`. The Meraki logo is visible in the top left. A navigation menu on the left includes sections for Monitor, Configure, Organization, and Help. The main content area is titled 'Clients > cmedranos-iPad' and contains the following information:

- Details:** Edit details, MAC address: a4:67:06:77:e4:9f, IP: 10.80.108.28, Hostname: cmedranos-iPad (Bonjour, DHCP), Network access: normal, Connection: wireless, Capabilities: 802.11n, 2.4 and 5 GHz, Manufacturer: Apple, Operating system: Apple iPad, History: Event log, Packet capture: Run packet capture on this client, Systems mgmt: Not installed.
- Status:** Currently connected (with a green status icon), Signal strength: 30 dB (with a green progress bar), Duration: 43 minutes, Access point: 4th FL Lobby, SSID: Meraki-Guest, Splash Authorization: SSID: Meraki-Guest (with a warning: about 6 hours ago, user authenticated with Clickthrough splash. Authorization will expire in about 18 hours. (revoke authorization)), Channel: 157 - 5.785 GHz (11n, 20MHz channel), Packets: 2042 sent, 777 received, Data: 144.2 KB sent, 404.5 KB received.
- Usage:** 347.5 MB (339.2 MB received, 8.3 MB sent). A graph shows usage over time from Apr 6 to Apr 12, with a peak on Apr 12.
- Live tools:** Ping client.
- Approximate location:** Based on data from 4 APs between Apr 12 10:32 and Apr 12 16:42. Excluded data from 1 unplaced AP. A map shows the client's location on the 4th floor of a building.
- Warnings:** A warning states: 'WARNING: This client's location may be less accurate because some of the related APs are not placed on this map. You can place APs on maps and floorplans here.'
- Bottom section:** Four pie charts labeled Applications, Ports, HTTP content, and Custom Pie Chart.

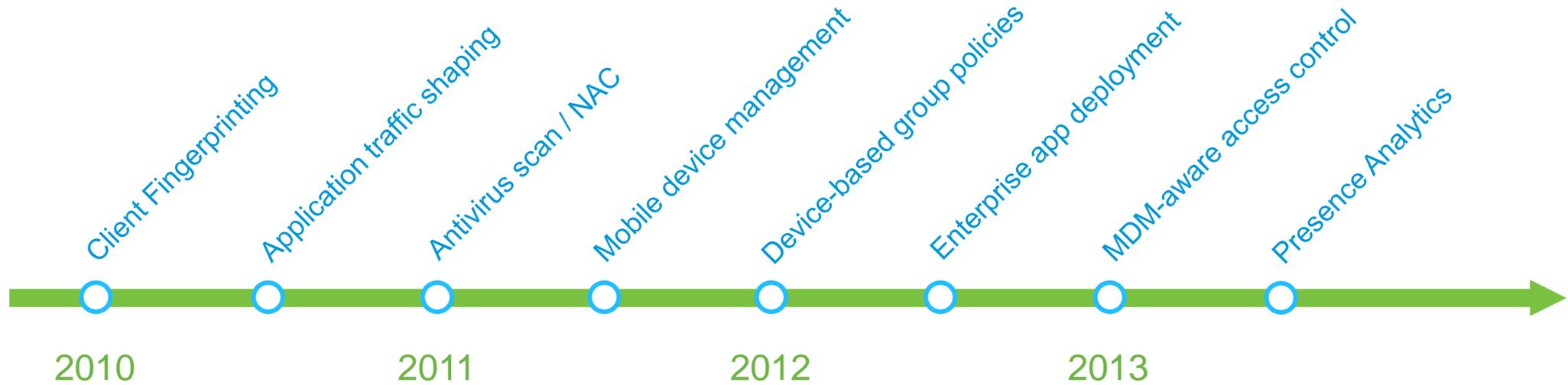
Instant search

Location analytics

Real-time control

SaaS feature delivery

BYOD feature velocity, past 36 months:



Feature updates seamlessly delivered from the cloud (user-scheduled)

Adapts to new devices, applications, and business opportunities

Solution highlights

Distributed networks

The screenshot displays a centralized cloud management interface. On the left, a sidebar menu includes sections for Monitor, Configure, and Organization, with sub-items like Overview, Change log, Settings, Configuration sync, License info, and Help. The main area features a map of the United States with numerous location pins, some green and some red, representing network sites. On the right, a table titled 'Expand' shows a search bar and a list of 930 networks. The table has columns for Name, Usage, and Clients. The data in the table is as follows:

Name	Usage	Clients
MAU1851 - Bossier City LA	none	0
DB0792 - Detroit MI	none	0
DB0339 - Matthews NC	none	0
DB0342 - Oceanside NY	none	0
MAU1581 - Papillion NE	none	0
DB0672 - Destin FL	none	0
DB0421 - Exton PA	none	0
MAU LAB EVDO	none	0
DB0440 - Champaign IL	none	0
MAU1660 - Hanford CA	none	0
DB0916 - Tulsa OK	none	0
DB0609 - Turnersville NJ	none	0

Centralized cloud management scales to thousands of sites

Multi-site visibility and control

Map-based dashboard; configuration sync; remote diagnostics; automatic monitoring and alerts

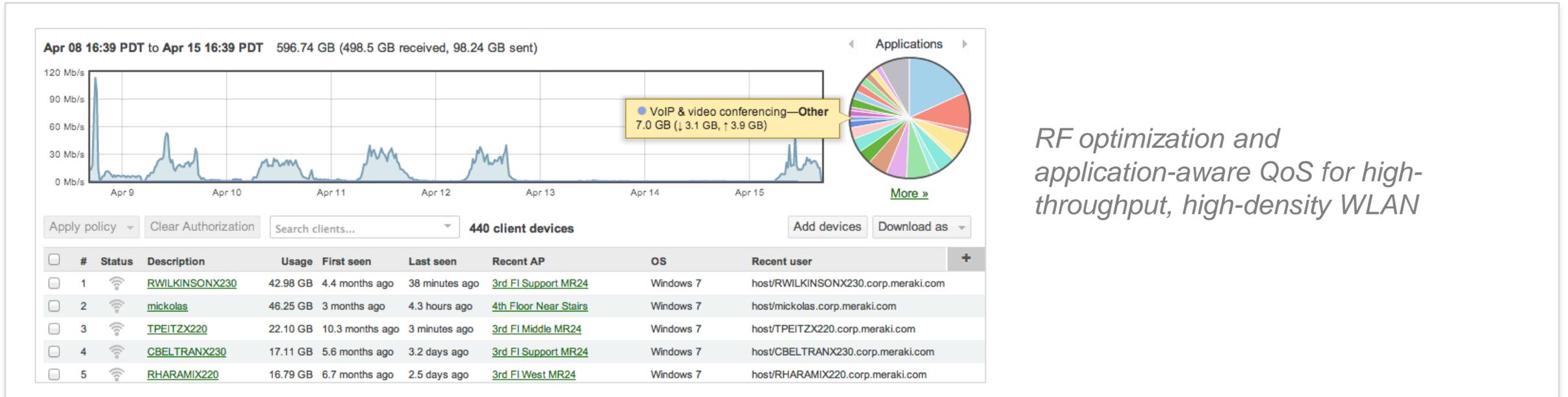
Zero-touch provisioning

Devices automatically provision from the cloud, no staging required; self-configuring site-to-site VPN

Traffic acceleration

WAN optimization and web caching accelerates and de-duplicates network traffic; application-aware QoS prioritizes productivity apps

High capacity edge networks



RF optimization and application-aware QoS for high-throughput, high-density WLAN

Layer 7 application traffic shaping

Throttle, block, or prioritize application traffic with DPI-based fingerprinting; set user and group-based shaping rules

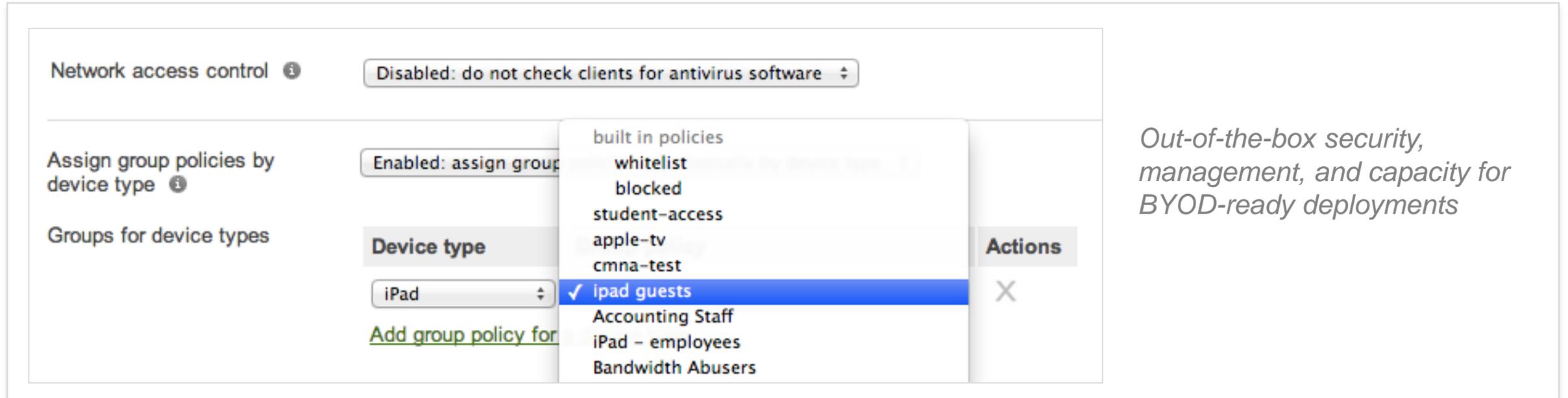
Cloud-base RF optimization

Dynamically avoid interference, optimizing channel selection and power levels

Density-optimized WLAN

RF platform tuned for airtime fairness and performance in dense performance-critical environments

Bring your own device (BYOD)



The screenshot shows a network management interface with the following elements:

- Network access control**: Disabled: do not check clients for antivirus software
- Assign group policies by device type**: Enabled: assign group
- Groups for device types**: iPad (selected)
- Device type**: iPad (selected)
- Policy list**:
 - built in policies
 - whitelist
 - blocked
 - student-access
 - apple-tv
 - cmna-test
 - ✓ ipad guests (highlighted)
 - Accounting Staff
 - iPad – employees
 - Bandwidth Abusers
- Actions**: X

Out-of-the-box security, management, and capacity for BYOD-ready deployments

Device-aware security

Device-aware firewall and access control; Antivirus scan; LAN isolation; Bonjour Gateway; Content and security filtering

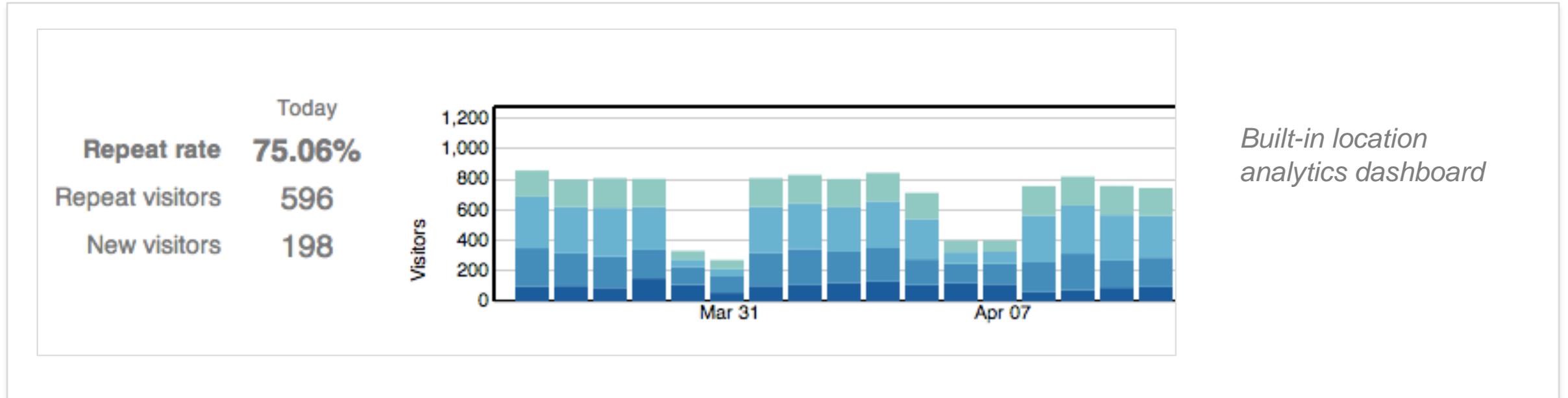
Integrated MDM

Enforce encryption, passcodes, and device restrictions; Deploy enterprise applications; Remotely lock or wipe devices

Simplified onboarding

Flexible authentication with AD integration, SMS authentication, hosted splash pages, and automatic MDM enrollment

User analytics and engagement



Optimize marketing and business operations

Analyze capture rate, dwell time, and new / repeat visitors to measure advertising, promotions, site utilization, etc.

Built-in analytics

Integrated into WLAN, no extra sensors, appliances, or software

Extensible API

Integrate location data with CRM, loyalty programs, and custom applications for targeted real-time offers

Flexible authentication and access control

- Click-through
Users must view and acknowledge your splash page before being allowed on the network
- Sign-on with
Require users to check in to your Facebook Page before gaining access to your network ⓘ
Configure Facebook settings [here](#).
- Sign-on with SMS Authentication **BETA**
Users enter a mobile phone number and receive an authorization code via SMS.

Flexible built-in authentication mechanisms

Flexible authentication

Secure 802.1x and Active Directory authentication; Facebook Authentication for branding and targeted social marketing; SMS self-service authentication, Lobby Ambassador, and hosted sign-on splash pages

Dynamic access control

Assign clients layer 3-7 firewall rules, VLANs, and application-aware quality of service by identity, group, location, or device type

Simplified enterprise security

Air Marshal

Scanning APs ④ **4 APs** in dedicated Air Marshal mode.

LAN containment ④ **Don't contain APs seen on the LAN**

Keyword containment ④
One keyword per line.

Off-channel scans ④ **Opportunistic and mandatory scans**

Mandatory scan schedule **4:00 AM**

or .



26 Rogue SSIDs | [439 Other SSIDs](#) | [5 Spoofs](#) | [0 Malicious broadcasts](#) | [212 Packet floods](#)

Containment	SSID	Last seen	First seen	# APs	Rogue because	Seen by	Broadcast MACs
uncontained	63 hidden SSIDs	Apr 16 18:22	Aug 24 05:57	63	Seen on LAN	4th FL Sales1 (74 dB) 21 more >	12:18:0a:31:87:50 62 more >
uncontained	SG3 FoxFi	Apr 10 00:04	Mar 20 07:09	1	Seen on LAN	4th Floor Near Stairs (34 dB) 1 more >	5c:0a:5b:5f:a4:0f
uncontained	Daghan Altas's iPhone	Apr 12 08:21	Apr 12 08:21	1	Seen on LAN	Air Marshal - 2nd Floor 1 more >	66:a3:cb:84:ad:bd

Enterprise-class security features for security-conscious environments

Air Marshal WIDS/WIPS

Detect wireless attacks; contain rogue APs; cloud-based alerting and diagnostics

User and device aware security

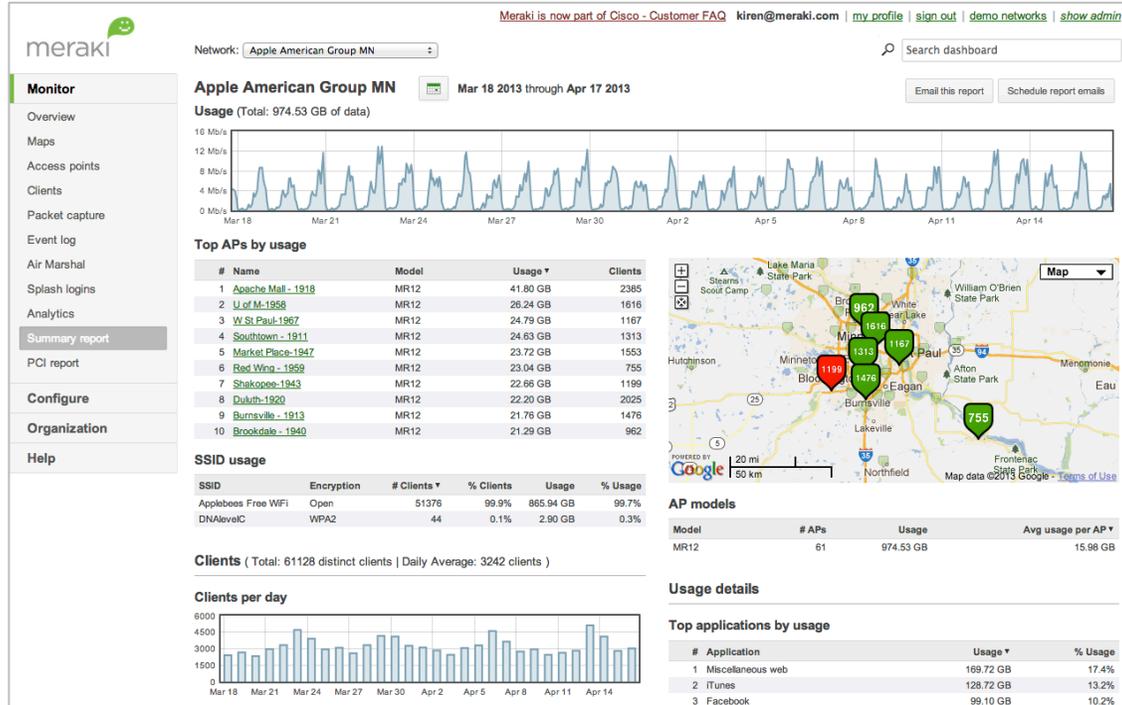
User, device, and group-based firewall rules (layer 3-7) with Active Directory integration

Complete NG firewall and content security

Application firewall; content filtering matching 1B+ URLs; antivirus / antimalware filtering; Google safe-search

Case studies

Case study: Applebee's

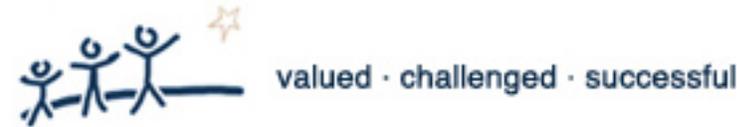
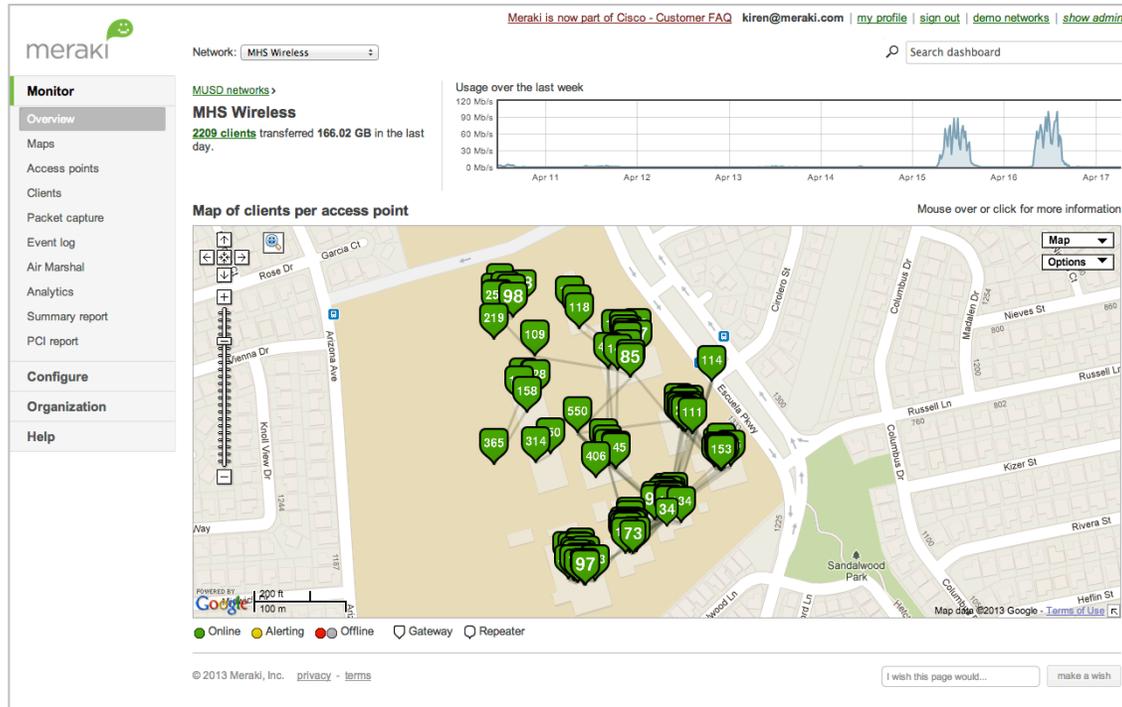


- Wireless LAN spanning over 270 restaurants nationwide
- Customer engagement through guest access, coupons, promotions
- PCI-compliant solution enables mobile POS
- Restaurants centrally managed over the web
- Deployed without pre-staging or on-site IT

“The Meraki Dashboard makes it easy to manage the WiFi across all the restaurants, and we have the visibility we wanted.”

Leslie McMasters, Network Administrator, Apple American Group

Case study: Milpitas Unified School District

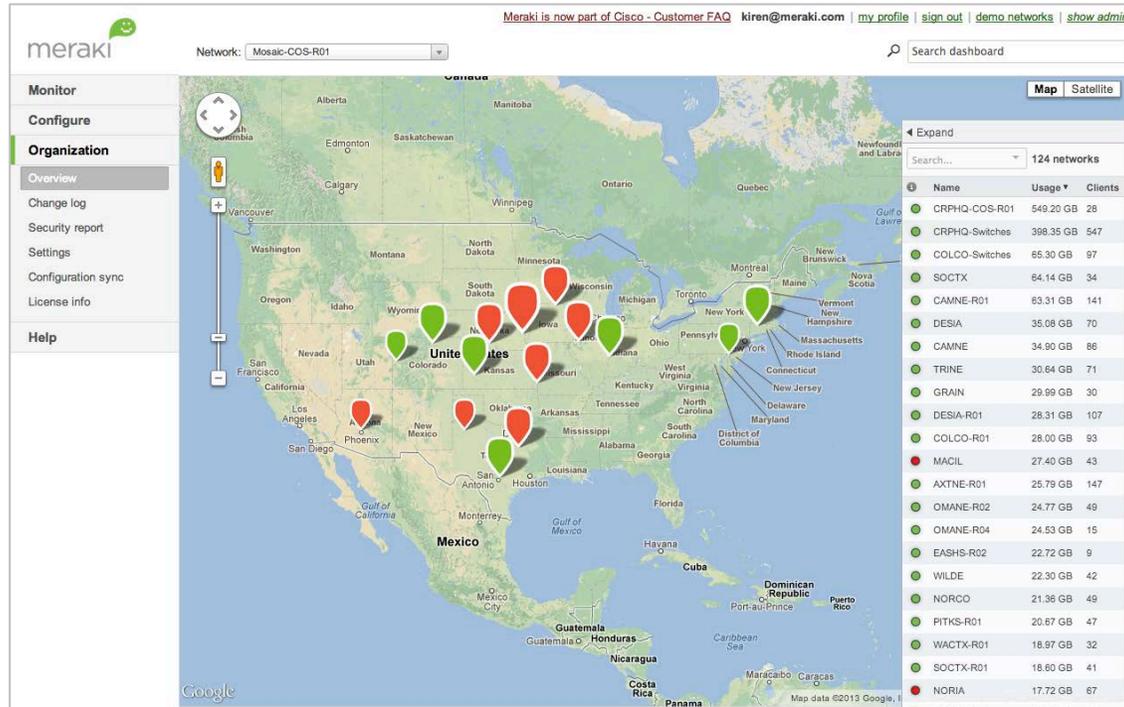


- California school district with 14 schools, 10,000 students
- Deployed cloud-managed firewall, 500 wireless APs (indoor + outdoor), and 100 Ethernet switches
- Enabled 1:1 Google Chromebook deployment and BYOD policy
- Application visibility and control optimizes bandwidth across 10k+ clients

“The Dashboard, the traffic shaping, and the MDM were real advantages. We can see the traffic and devices on the fly.”

Chin Song, Director of Technology, Milpitas Unified School District

Case study: Mosaic



- Healthcare and services provider with 5,000 employees, 40 facilities across 11 states
- Deployed 350 cloud-managed wireless APs, switches, and security appliances
- HIPAA-compliant WiFi for electronic medical records and guest access
- Centrally managed by small IT staff

“The Meraki solution has provided us with a secure, centrally managed distributed network.”

Daniel McDonald, Systems Integration Manager, Mosaic

Product Families

MR wireless access points



Feature highlights

BYOD policies

Application traffic shaping

Guest access

Enterprise security

WIDS / WIPS

Location analytics

6 models including indoor / outdoor, high performance(802.11ac) and value-priced

Enterprise-class silicon including RF optimization, PoE, voice / video support

Lifetime warranty on indoor APs

MX security appliances



Feature
highlights

Zero-touch site to site VPN

WAN optimization

NG firewall

Content filtering

WAN link bonding

Intrusion detection

6 models scaling from small branch to campus / datacenter

Complete networking and security in a single appliance

MS access & aggregation switches



Feature highlights

Voice and video QoS

Layer 7 app visibility

Virtual stacking

PoE / PoE + on all ports

Remote packet capture,
cable testing

Gigabit access switches in 8, 24, and 48 port configurations, PoE available on all ports

10 Gigabit SFP+ aggregation switches in 24 and 48 port configurations

Enterprise-class performance and reliability including non-blocking performance, voice/video QoS, and a lifetime warranty

Systems Manager mobile device management



Feature highlights

Centralized app deployment

Device security

Rapid provisioning

Backpack™ file sharing

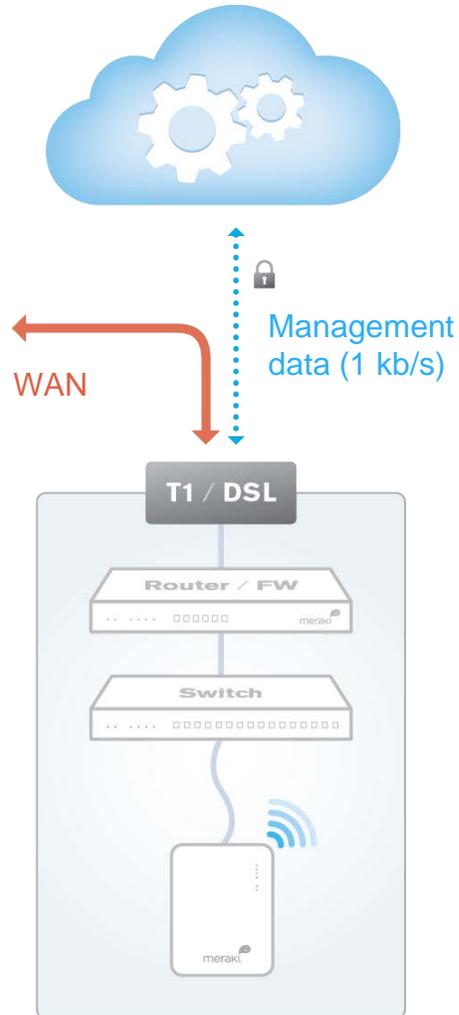
Asset management

Device Management controls iOS, Android, Mac, and Windows devices

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

100% free - available at no cost to any organization, sign up at meraki.cisco.com/sm

Out of band cloud management in every product



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)
- 3rd party security audits, daily penetration testing
- Automatic firmware and security updates (user-scheduled)

Reliability and security information at meraki.cisco.com/trust

Free evaluations available



Try Cisco Meraki with no risk or commitment

Complimentary technical assistance available

Start eval at meraki.cisco.com/eval

Thank you.

