



Meraki Cloud Managed Networking

Cisco Meraki solution Overview & Demo



Why cloud managed networking?

The cloud increases IT efficiency



Manageability



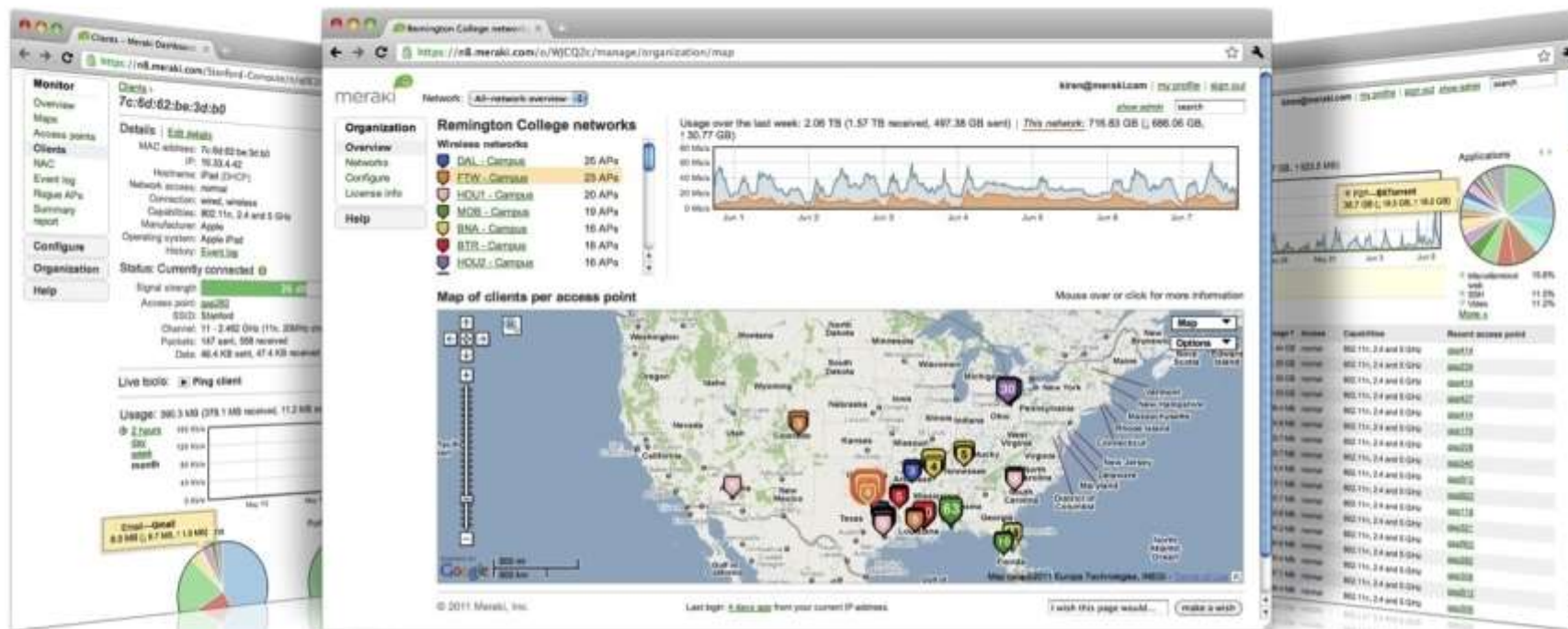
Scalability



Cost Savings

- 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 MC
Communication



Meraki MV
Security Cameras



Meraki SM
Mobile Device
Management

Solution highlights

Distributed networks



The screenshot displays a network management interface. On the left, a sidebar menu includes sections for 'Monitor', 'Configure', and 'Organization', with 'Overview' selected. The main area features a map of the United States with numerous location pins, some green and some red. On the right, a panel titled 'Expand' shows a search bar and a table of 930 networks. The table has columns for 'Name', 'Usage', and 'Clients'. Below is a list of network entries:

Name	Usage	Clients
MAU1851 - Bossier City LA	none	0
DB0782 - Detroit MI	none	0
DB0339 - Matthews NC	none	0
DB0342 - Oceanside NY	none	0
MAU1581 - Papillon NE	none	0
DB0672 - Destin FL	none	0
DB0421 - Exton PA	none	0
MAU LAB EVD0	none	0
DB0440 - Champaign IL	none	0
MAU1880 - Hanford CA	none	0
DB0918 - Tulsa OK	none	0
DB0809 - 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

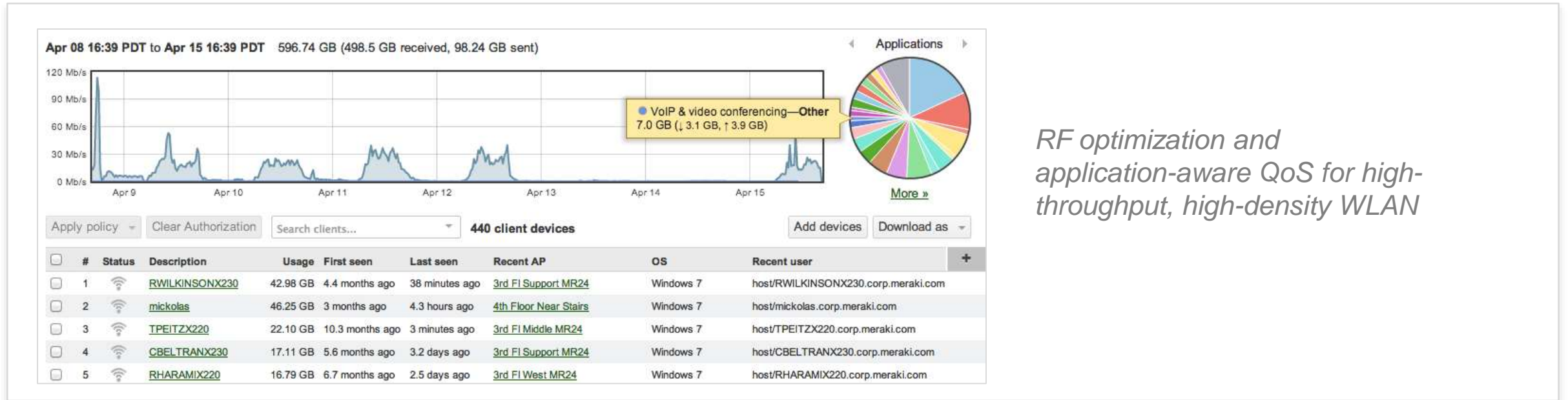
Zero-touch provisioning

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

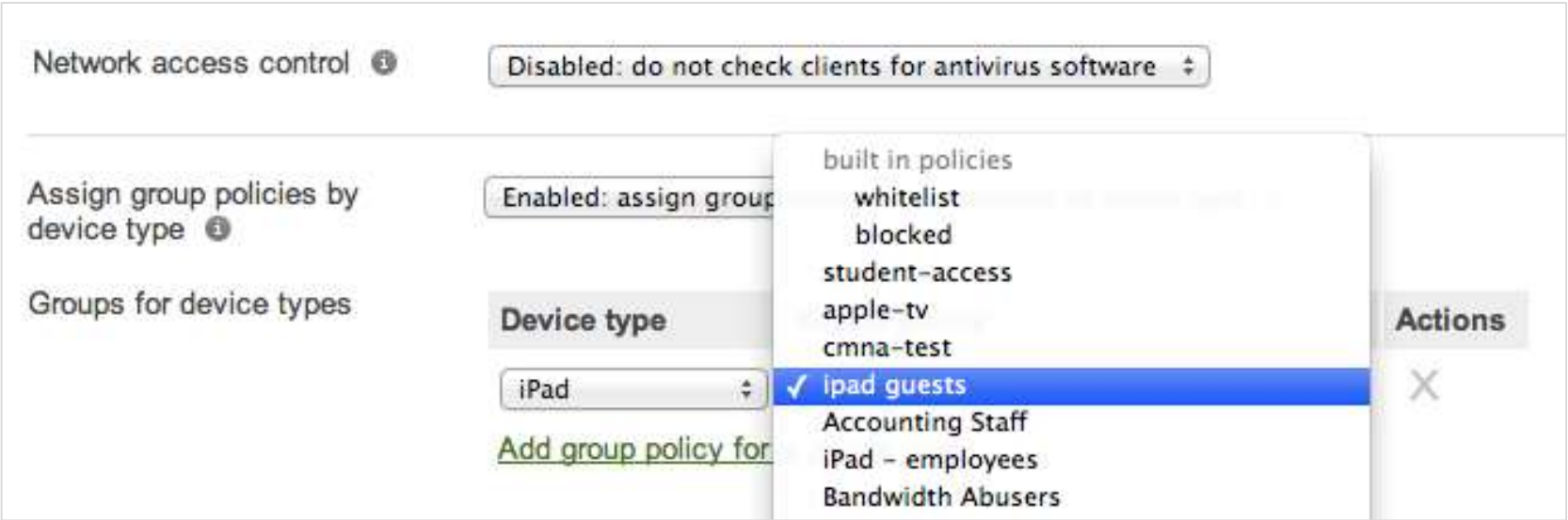
Cloud-base RF optimization

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**: A dropdown menu is open, showing options: "Disabled: do not check clients for antivirus software", "Enabled: assign group policies by device type", "built in policies", "whitelist", "blocked", "student-access", "apple-tv", "cmna-test", "✓ ipad guests" (highlighted), "Accounting Staff", "iPad - employees", and "Bandwidth Abusers".
- Assign group policies by device type**: A dropdown menu is open, showing "iPad" selected.
- Groups for device types**: A section with a link "Add group policy for" and an "Actions" button with a close icon (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

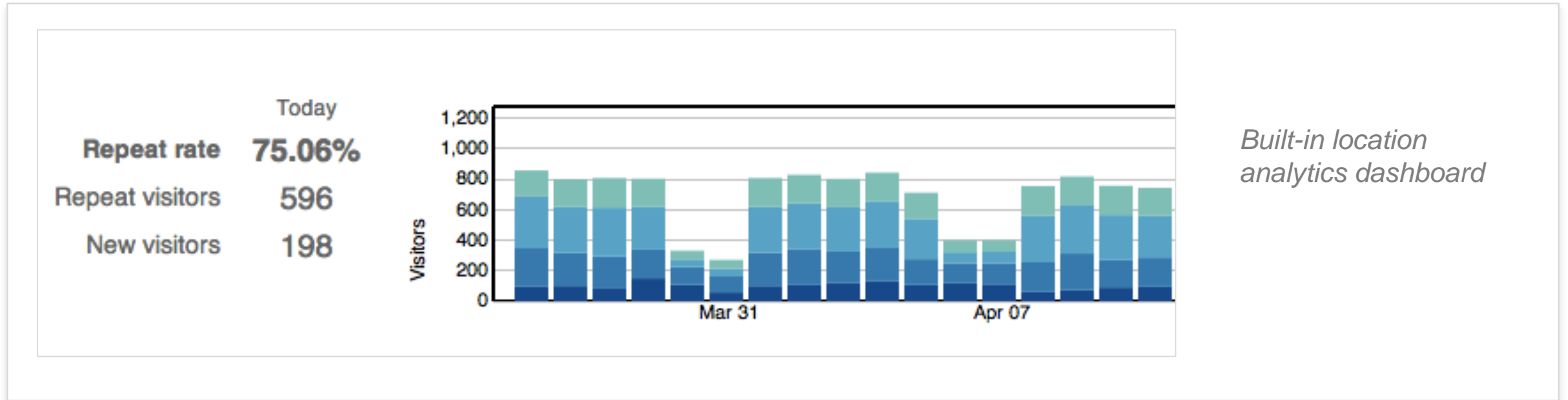
Integrated MDM

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

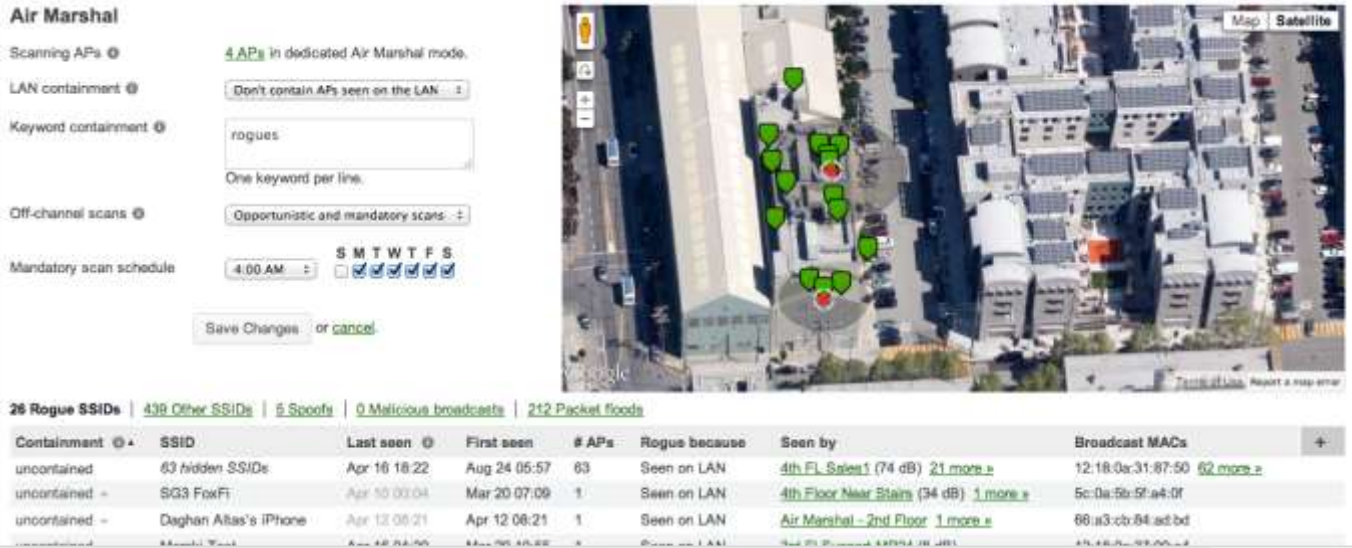
Flexible authentication

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



The screenshot displays the 'Air Marshal' configuration interface. On the left, there are settings for 'Scanning APs' (4 APs in dedicated mode), 'LAN containment' (Don't contain APs seen on the LAN), 'Keyword containment' (rogues), 'Off-channel scans' (Opportunistic and mandatory scans), and 'Mandatory scan schedule' (4:00 AM, SMTWTFS). A 'Save Changes' button is visible. On the right, a satellite map shows several green and red markers representing detected APs. Below the map, a summary bar shows: 26 Rogue SSIDs, 438 Other SSIDs, 6 Spoofs, 0 Malicious broadcasts, and 212 Packet floods. A table below lists detected SSIDs and their details.

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 03:04	Mar 20 07:09	1	Seen on LAN	4th Floor Near Stairs (34 dB) 1 more »	5c:0a:5b:5f:a4:d0
uncontained	Daghan Atlas's iPhone	Apr 12 08:21	Apr 12 08:21	1	Seen on LAN	Air Marshal - 2nd Floor 1 more »	68: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

Cisco Meraki: Bringing the cloud to enterprise networks



Meraki MR
Wireless LAN



Meraki MS
Ethernet Switches



Meraki MX
Security Appliances



Meraki MC
Communication



Meraki MV
Security Cameras



Meraki SM
Mobile Device
Management

Thank you.

