Meraki MX for Retail

Cloud Managed Security

The Meraki MX Security Appliance is optimized for distributed retail locations, protecting sites from attack while reducing network complexity.

- PCI L1 certified cloud architecture
- Secure branch locations
- Easy deployment and maintenance
- Branded, in-store customer connectivity
- Dynamic retail analytics (MX60W)
- Bandwidth hog containment

"What I like about Cisco Meraki is the ease of con guration and distribution. And the dashboard is fantastic."

—Mark Bishop, IT Manager, United Colors of Benetton UK

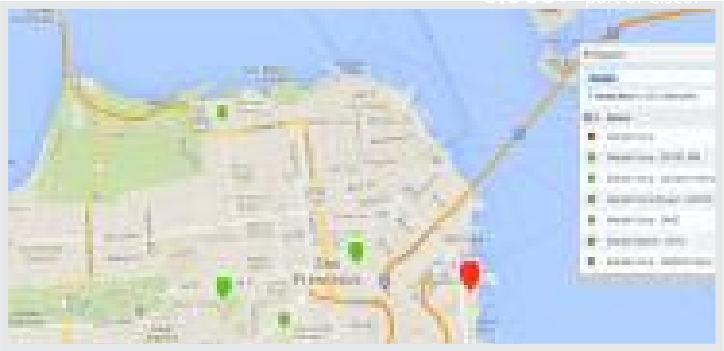
See for yourself! FREE evaluations available at **meraki.cisco.com/eval**

Cisco Meraki MX Customers:

UNITED COLORS OF BENETTON. Westfield RESTORATION HARDWARE CARTER & K. BLACK dressbarn Orchard REEDS

The new standard for security and centralized management

The MX lets retailers rapidly deploy branch locations, improve site productivity, and enhance in-store customer experience.



The Cisco Meraki dashboard lets you intuitively manage remote networks, devices, and clients.

Secure Branch Locations

- Securely connect remote sites in minutes with built-in Auto VPN
- Contain malicious activity with integrated Sourcefire intrusion prevention and malware scanning
- Easily propagate security settings across multiple sites using configuration templates
- Weed out unwanted content and prevent phishing attacks with best-in-class content filtering
- Control tra□c based on geography with Geo-IP ACLs

Sourcefire Intrusion Prevention secures branch sites from malicious attack.

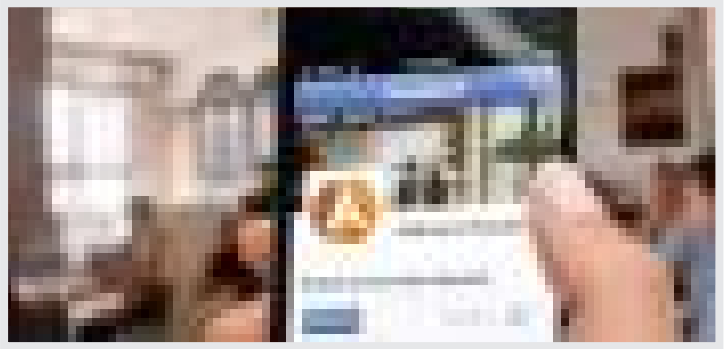
Reduce Network Complexity

- Enjoy established PCI L1 compliant cloud architecture
- Quickly deploy remote sites by preconfiguring Meraki devices from the cloud
- Centrally manage all networks, devices, and clients from any Internet-accessible location through a single, web-based dashboard
- Seamlessly pull updates from the cloud

Content filtering protects against phishing attacks while ensuring unwanted content is blocked.

Enhance in-store customer connectivity

- Customize shopper experience with branded splash pages
- Allow guest Internet access using Facebook login—and promote your business on customer News Feeds
- Access aggregate demographic data from Facebook check-ins to tailor shopper experience

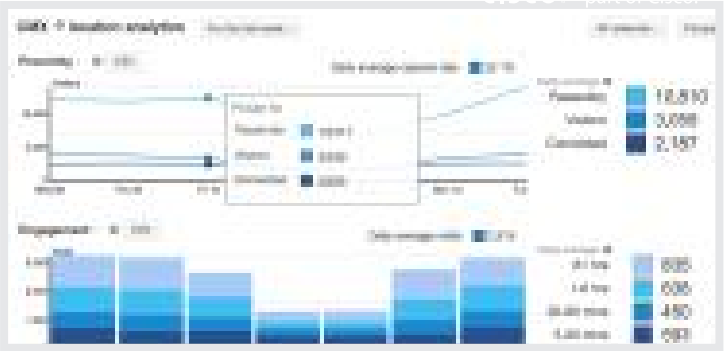


Wired splash pages with Facebook Login enable intuitive guest access while promoting your brand.

Cisco Systems, Inc. | 500 Terry A. Francois Blvd, San Francisco, CA 94158 | (415) 432-1000 | sales@meraki.com

Leverage Dynamic Retail Analytics

- Gain network insights from industry- leading application tra□c visibility and client fingerprinting
- Limit or optimize applications and websites with Layer 7 firewall and tra□c shaping rules



Location analytics built into the MX60W measures key customer statistics over time.

Identify & contain bandwidth hogs

- Measure presence by tracking the number and types of connected clients
- Increase foot tra□c and lengthen dwell time with in-store mobile customer engagement using Meraki's extensible APIs
- Identify shopping trends by analyzing user web tra□c

Deep visibility and control over network tra□c and Layer 7 consumption.

CUSTOMER HIGHLIGHT

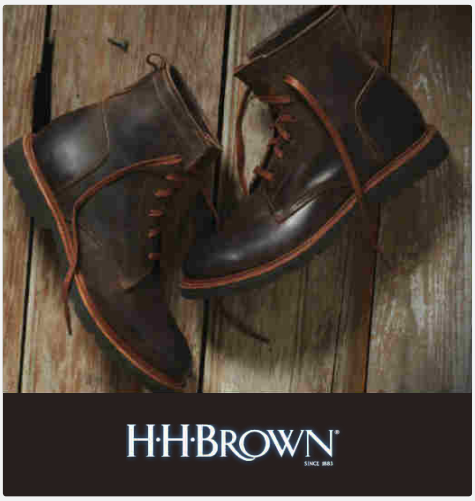
H.H. Brown

Quick Facts

- Wholly-owned Berkshire Hathaway subsidiary
- Oversees 19 shoe brands
- MXs deployed in 45 retail locations

Why HH Brown chose the Meraki MX

- Rapid, easy deployment of site-to-site Auto VPN
- MX is a feature-rich, single-box solution
- Free trial evaluation showed how intuitive and easy it is to manage sites, apps, and users with the MX



CASE STUDY

The Heartbleed Vulnerability

How MX customers contained Heartbleed in one day.

The disclosure of the dangerous (and widespread) Heartbleed vulnerability in April, 2014, propelled public awareness of exploitable threats. Intrusion prevention (IPS) plays a critical role in protecting networks from attacks such as this.

How IPS works on the Meraki MX

The Meraki MX security appliance integrates with industry-leading Sourcefire IPS to contain malicious activity at your network's perimeter. The MX performs intrusion prevention via rulesets: pre-defined security policies that determine the level of threat protection needed.

Sourcefire refreshes rulesets automatically (adding newly discovered vulnerabilities and purging older ones), so MX customers don't need to exert any e□ort in order to have a well- tended, constantly pruned baseline level of security. Even better, these rulesets are updated daily and pushed within an hour to MX customers from the cloud—no manual staging or patching needed.

In the case of Heartbleed, Sourcefire identified a vulnerability signature and refreshed its rulesets within 24 hours of disclosure—so all MX customers using IPS were protected automatically once they received that update.

IPS can be easily configured in 15 seconds in the Meraki dashboard, allowing IT admins to enjoy up-to-date, best-in-class intrusion prevention while averting the "pilot error" that often plagues complex, manual configuration and patching of IPS.

The Meraki MX's Intrusion Prevention secures branch sites from malicious attack; detailed security reporting provides deep visibility into threats.