

[DEPLOYMENT STORIES \(/CUSTOMERS\)](#)
[DEMO \(/LP/FREE-DEMO\)](#)

[PRODUCTS \(/PRODUCTS\)](#)

[TECHNOLOGIES \(/TECHNOLOGIES\)](#)

[PARTNERS \(/PARTNERS\)](#)

[See Other Enterprise Stories \(https://meraki.cisco.com/customers/enterprise\)](https://meraki.cisco.com/customers/enterprise)

Penn Mutual



HIGHLIGHTS

Three network admins oversee wireless, switching, and security across 42 locations

Secure solution segments wireless access for corporate users vs. guests

Auto-provisioning site-to-site VPN enables 40% savings in connectivity costs

WEBINARS & EVENTS

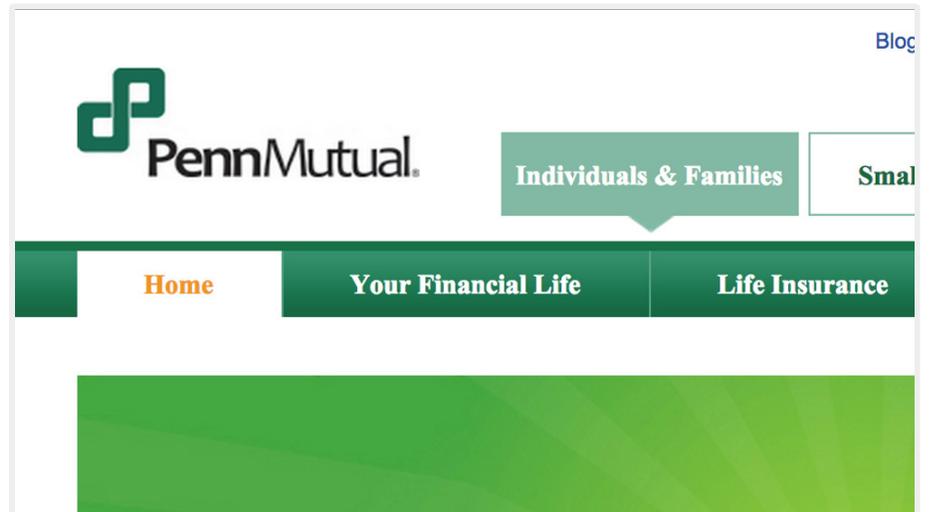
[1:1 and BYOD for K-12 \(https://meraki.cisco.com/webinars/signup/1269/11-and-byod-for-k-12/\)](https://meraki.cisco.com/webinars/signup/1269/11-and-byod-for-k-12/)

READ MORE

[Meraki Helps Mills & Reeve Achieve Total Customer Satisfaction \(http://www.responsesource.com/news/74109/meraki-helps-mills-reeve-achieve-total-customer-satisfaction\)](http://www.responsesource.com/news/74109/meraki-helps-mills-reeve-achieve-total-customer-satisfaction)

[Active Directory Integration Whitepaper \(https://meraki.cisco.com/lib/pdf/meraki_whitepaper_active_directory_integration.pdf\)](https://meraki.cisco.com/lib/pdf/meraki_whitepaper_active_directory_integration.pdf)

[Network Security Whitepaper \(https://meraki.cisco.com/lib/pdf/meraki_whitepaper_network_security.pdf\)](https://meraki.cisco.com/lib/pdf/meraki_whitepaper_network_security.pdf)



With 41 branch locations and over 1800 associates scattered across the United States, Andrew McInerney, Data Network and Voice Manager at Penn Mutual, oversees a challenging network. Previously, the mutual life insurance company used a traditional hub-and-spoke VPN service through a telecom carrier to support their distributed network. Over time, however, associates at the mutual life insurance company increasingly relied on Internet-hosted applications for everyday tasks, and this slowed the network down.

“There was a lot of latency,” McInerney explained. “The growing use of cloud-based applications in the financial industry meant our network needed to get up to speed.” Low speeds and high costs, as well as the bandwidth implications of having all data go through headquarters, soon outweighed the benefit of having a fully managed service. McInerney and his team began looking for alternative networking solutions that they could manage in-house.

McInerney sought a networking solution with a split-tunnel VPN model to reduce strain on bandwidth at the home office. In addition, he hoped to connect the previously wired-only field offices using a wireless solution, while maintaining network visibility.

With a staff of only three network administrators at the home office in Horsham, PA, he needed proven security to protect Penn Mutual’s confidential data, while providing an easy to manage interface for his lean IT team. “It goes without saying that security, in terms of controlling assets and controlling access to wired and wireless networks, is critical no matter what vertical you are in, but especially in the financial industry,” McInerney said.

When McInerney first learned about cloud networking, he realized that the Cisco Meraki web-based dashboard would allow his team to manage all 42 sites from the home office, without requiring extensive training or time spent on either deployment or management. “I looked into it and saw that Cisco Meraki captured everything we were trying to do,” he said. He quickly set up a test lab with one Cisco Meraki MX security appliance, one MS switch, and two MR access points. The trial worked flawlessly. “We had to pinch ourselves: ‘Is this really that simple?’”

Upon deploying Cisco Meraki to the rest of the offices, McInerney's team simply cloned the test lab device configurations to the new devices from the dashboard. "We set everything up ourselves, though the Cisco Meraki support team helped us get started," he explained. "Cisco Meraki offers an incredible support channel; it's refreshing. As an IT manager, it's usually painful to get help, but in this case, it's not painful: it's just a quick phone call away. That's very important to me."

McInerney chose a staggered deployment to facilitate the company's transition away from the telecom carrier. Today, about halfway through their deployment, Penn Mutual has 22 MX security appliances: two MX400s at HQ and one MX80 or MX90 at each field location. The company also has several MS42/P switches and MR24 access points at each office. McInerney noted that cloud networking makes it easy to deploy as many devices as needed in a scalable way, while the zero-touch configuration, plug-and-play hardware increased deployment flexibility for the Penn Mutual team. "Now it's like clockwork; everything is working together perfectly," he said. "We've been having a tremendous amount of success."

In particular, McInerney praises the MX Security Appliance, which – with auto-provisioning site-to-site VPN – securely connects Penn Mutual's HQ and branch offices without manual VPN configuration. This site-to-site VPN solution also facilitated massive savings in connectivity costs, as Penn Mutual moved from an expensive T1 VPB hub and spoke model to using 50Mbps DSL broadband where available.

The MXs at each branch also provide Layer 7 visibility, allowing McInerney to isolate and identify unauthorized platforms for remediation. Layer 3 firewall rules ensure VLAN separation, while Layer 7 firewall rules deny access to specific applications. "The MX gives us visibility into our field networks that we never had before," McInerney said. Content filtering in the MX blocks categories including nudity and SPAM sources, and he is also easily able to limit uplink configuration and per-device and per-SSID bandwidth. Additionally, specific URLs are blocked (e.g. xfinitytv.net) and whitelisted (e.g. pennmutual.com).

"We came from an environment where our field offices had legacy layer 2 switches with minimal visibility. Having layer 7 visibility is incredible. It's clear to anyone who is viewing the dashboard what is going on at each port. "

—Andrew McInerney, Data Network and Voice Manager

Whereas associates were previously limited to wired connections, the Cisco Meraki APs now provide WiFi at all offices and thus greater mobility to Penn Mutual associates. With just a few clicks in the dashboard, McInerney configured two SSIDs across all locations. The corporate SSID is always available and securely connects clients to the LAN via WPA2-PSK authentication. The guest network, primarily intended for office visitors, utilizes a customized click-through splash page and pushes all guest clients to a specific VLAN, isolating them from connecting directly to the LAN. Furthermore, the guest SSID is only available during office hours, Monday-Friday from 8am to 6pm.

The Cisco Meraki MS switches in each branch further secure Penn Mutual's network. Penn Mutual uses enterprise security features that are easy to deploy at scale such as 802.1X port security. The MS switches also simplify network management: device fingerprinting ensures the IT team can find and identify specific clients irrespective of which switch or port they are connected to, while virtual stacking allows the IT team to configure ports across multiple sites with just a few clicks, search by tag or by port, configure trunk vs. access port types, set up native VLANs, and more: "We came from an environment where our field offices had legacy layer 2 switches with minimal visibility. Having layer 7 visibility is incredible. It's clear to anyone who is viewing the dashboard what is going on at each port," McInerney explained.

Today, Penn Mutual has a secure network with reliable access for associates and guests. McInerney and his team also boast increased network speeds via traffic shaping, bandwidth and filtering rules, and WAN optimization. They have complete visibility into clients, devices, and applications on the network. "The reporting feature for management is very insightful and detailed. With the dashboard, you literally have the ability to see your entire network at

Projected Costs for Legacy 3 year WAN Run rate

Internet Connectivity (3 Years)	\$2,016,000
Traditional T1 VPB hub and spoke model x 45 sites (1.544-4.632 Mbps Ethernet)	\$582,000/yr
WAN at HQ & DR (45Mbps x2)	\$90,000/yr
Content Management (3 Years)	\$153,000
Content Filtering Software	\$51,000/yr
Maintenance	\$24,750
Hardware security appliance	\$8,250/yr
3 Year Spend	\$2,193,750

Projected 3 Year Cost with Meraki (including rip and replace)

Internet Connectivity (3 Years)	\$673,495
HQ + 37 Branch (50Mbps DSL Broadband)	\$212,040/yr
WAN Mgmt Vendor (One Time setup)	\$37,375
Meraki Hardware & Licensing	\$599,141
MX, MS and MR x 41 Branch	\$382,896
MX, MS and MR License	\$72,081/yr
Content Management	Included
Wireless Installation (one time)	\$62,257
26 Branch Offices wired for MR	
3 Year Spend	\$1,334,893