mojo Networks

pinkberry

"This was one of the easiest technology projects I've ever instituted. There have been no issues and nothing but positive feedback."

"We've blown the doors off our expectations with the Pinkcard loyalty program."

– Tony DiCenzo, SVP of IT, Pinkberry

Highlights

- The premium yogurt retailer headquartered in Los Angeles, CA, and having more than 170 Pinkberry stores in operation worldwide.
- Deploying Wi-Fi guest access in stores in a secure manner that satisfied Payment Card Industry (PCI) security standards, was affordable and required minimal operational effort. Driving the Wi-Fi deployment was the launch of The Pinkcard, Pinkberry's new loyalty program and mobile app; as well as requests from store customers and owners for Wi-Fi access services.
- Mojo Cloud, which combines Mojo Wireless Manager and Mojo AirTight, providing PCI compliance scanning and reporting.

Benefits

- Swift rollout of Wi-Fi without the need to add any IT staff
- Success of the Pinkcard program beyond expectations
- Built-in automated security simplified PCI compliance

Pinkberry Serves Up Wi-Fi Guest Services with a Side of Rewards

When Pinkberry Inc. first received requests for Wi-Fi guest access the yogurt retailer wanted to ensure the best customer experience. The Company began to explore how to protect customer information and meet the wireless scanning requirements of the Payment Card Industry Data Security Standard (PCI DSS), which requires specific actions to protect customer information and also requires regular over-the-air security checks for unauthorized devices.

But then, Pinkberry launched The Pinkcard, a new loyalty program and mobile app. The five-year-old, Los Angeles-based Brand, best known for it's light and refreshing yogurt, felt strongly that offering Wi-Fi guest services would help drive the Pinkcard program's success.

So in April 2012, it began investigating how to securely enable Wi-Fi access in its 100-plus independently owned franchises in the United States. Pinkberry also has stores in South America, Europe, the Middle East and Asia.

Security First

"Top priorities in the Wi-Fi system were the ability to shut down any unauthorized Wi-Fi access points (APs) attempting to connect to the Pinkberry network and built-in support for PCI auditing compliance," says Tony DiCenzo, senior vice president of IT at Pinkberry.

Pinkberry also wanted a Wi-Fi system that required minimum maintenance and required little or no training or Wi-Fi experience on the part of the store – and all at a reasonable cost.

The solution was Mojo Cloud, a combination of Wi-Fi access (Mojo Wireless Manager), automated wireless intrusion prevention and PCI compliance scanning and reporting (Mojo AirTight). Pinkberry has standardized on cloud-managed Mojo for Wi-Fi throughout its stores.

Mojo APs are capable of providing high- speed 802.11n access, while monitoring the wireless airspace and protecting the network from wireless threats, including Rogue APs, thus fulfilling the PCI DSS wireless security requirements. Among these is PCI DSS Requirement 11.1, which calls for the regular testing for presence of unauthorized Wi-Fi devices in the cardholder data environment.

Getting There from Here

"The PCI component was a serious consideration. We looked at several companies. A lot of them were pretty expensive solutions with only rudimentary security capabilities that didn't guarantee PCI compliance beyond a checkmark," explains DiCenzo.

He says Pinkberry sought a top-down, centralized approach to deployment, management and security of in-store APs. The Company data center communicates with Pinkberry retail stores using Multiprotocol Label Switching (MPLS) virtual private network (VPN) WAN services.

But the Company didn't want to receive piles of alerts and security logs to interpret and then have to decide whether to act on them. And if alerts started gathering dust, that would have ultimately introduced a greater degree of risk into the network.

"The most important feature to us was the ability to automatically prevent breaches of the network. We didn't want to have to do it manually," DiCenzo says. He adds that the other Wi-Fi solutions he evaluated didn't offer automated disconnection of unauthorized APs attempting to join the network, which made the Mojo decision a slam dunk.

For example, any user running the Pinkberry mobile application is protected from associating with an AP that might be impersonating the Pinkberry network. It might do so by broadcasting a service set identifier (SSID), or network name, such as "Pinkberry" and attempting to gain user credentials when the user connects. Such phony APs, run by hackers, are often called an "evil twin" or a "honeypot."

Also, says DiCenzo, "Different suppliers interpret new PCI standards in different ways. We felt most comfortable with Mojo. We have many franchise partners, and one of our responsibilities was to find the best value and best service so that it would be easy for them to implement and use."

Adding a Franchise: No Extra Staff Required

DiCenzo says the Company didn't have to add any IT staff to roll out the Wi-Fi guest services. Each franchise wishing to participate in the Wi-Fi program gets one AP, which is pre-configured by Mojo and then shipped directly to the store. From there, the franchisee makes a call to Pinkberry's network manager, who explains how to simply plug in the AP to the proper port on the store's firewall.

Pinkberry takes it from there; the Company has standardized on its policy rules, which it enforces through a Web portal into the Mojo Cloud. The Mojo AP brings up a Pinkberry-branded splash page to guests connecting over Wi-Fi, who can use the Pinkcard app to avail offers and services beyond what's available in stores and to use prepaid monies on their card to conveniently purchase products.

"This was one of the easiest technology projects I've ever instituted," says DiCenzo. "There have been no issues and nothing but positive feedback."

Lessons Learned

Prior to the Mojo deployment, Pinkberry hadn't been running Wi-Fi in stores for internal or guest access. DiCenzo says that at first he didn't realize – but soon discovered – that some of the Company's existing security mechanisms got in customers' way. Since workers weren't using Wi-Fi at all in the stores, they weren't using the Company network to connect to the Apple App Store, Android Google Play and other public mobile app stores. So access to these sites had been blocked by the Company firewall.

"We were treating consumer access the same way as we were internal access, so iPhones couldn't go to the App Store," DiCenzo explains. That issue was quickly resolved by adjusting the firewall to partition Wi-Fi and internal LAN traffic with two sets of access policies residing on separate ports.

From a cost perspective, DiCenzo finds it advantageous to have the AP and monitoring (sensor) capabilities integrated. "What Mojo offers is one-stop-shop; the data forwarding hardware is fully integrated with the monitoring solution. When you are working with partners in the field with limited technical resources, the simpler the better," he says.

Overshooting it's goals

Fast-forward to today. "We've blown the doors off our expectations with the Pinkcard loyalty program," says DiCenzo. He says Pinkberry exceeded its three-month goals in just one month after launching the Pinkcard program in October 2012. DiCenzo acknowledges that the program would also likely have done well using 3G/4G cellular services only, but, "adding Wi-Fi made throughput that much faster and we think resulted in quicker and better experiences for our customers.