SOLUTION BRIEF

Securing WLANs for PCI Compliance

Using Fortinet's Secure WLAN Solutions to Meet and Exceed PCI DSS Regulatory Requirements

Executive Summary

Retail Wi-Fi networks are a prime target for cyber-attacks due to the highly sensitive personal and financial data passing over them. Yet protecting them, and ensuring compliance with Payment Card Industry Data Security Standard (PCI DSS) is a challenge as retailers expand their own use of wireless technologies and encourage customer engagement via free Wi-Fi access.

Bricks and mortar retailers have little choice these days but to embrace Wi-Fi. Not only is it a powerful enabling technology for better customer service and improved efficiency, in many sectors from department stores to restaurants, free Wi-Fi is almost expected by consumers.

At the same time, many retailers are eager to leverage their Wi-Fi investment to garner customer intelligence and loyalty, and the most advanced are using it for real-time targeted marketing to their connected shoppers and patrons.

However, allowing unvetted mobile devices, social login, and new types of fixed and mobile Wi-Fi terminals on your network carries new risks. Retailers must be ever vigilant, as PCI DSS compliance and other security policies can quickly unravel. They must also recognize that PCI DSS alone is not sufficient for complete protection.

This paper is intended for Retail industry CIOs and CISOs. It discusses the threats and challenges for retailers, and explains how Fortinet enforces PCI DSS compliance and other security measures across its portfolio of wireless LAN solutions.

Retail is an IoT Poster Child

No doubt you have heard of the Internet of Things (IoT). Most likely though, you have earmarked it as something that applies to Smart Grids or the manufacturing supply chain.

Think again. Consider the variety of employee and consumer mobile devices coming onto your network, alongside a mix of proprietary systems for surveillance, inventory management, payment processing, and in-store marketing. Bricks and mortar retailers are fast becoming a poster child for the IoT.

WLAN PCI Compliance

Retail Wi-Fi networks that carry credit card data must comply with PCI DSS regulatory requirements.

Fortinet's consolidated approach to WLAN security enables consistent policies to be applied across both wired and wireless networks, simplifying management and PCI DSS compliance reporting.

- On-wire and off-wire Rogue AP detection and mitigation
- Integrated Wireless Intrusion Detection System (WIDS)
- Unified management interface for wired and wireless security
- Complete protection for mPOS and other embedded systems
- Network-wide PCI compliance reports generated automatically
- Kept secure through regular signature updates from FortiGuard

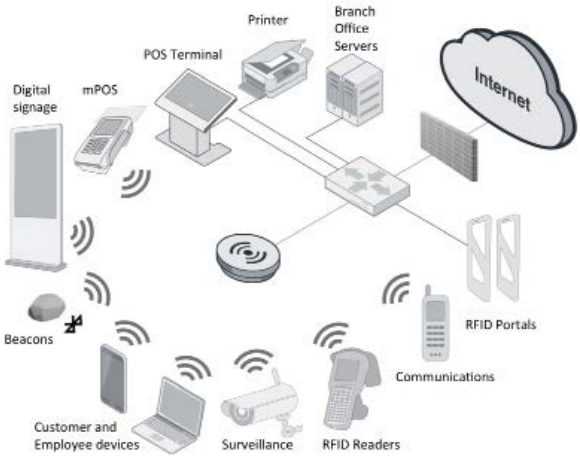

Figure 1: IoT components in today's Retail networks.

Retail Wi-Fi Trends

Savvy retailers want to monetize their Wi-Fi investment by making it available to their customers, and by doing more with it themselves. Common applications for Wi-Fi already include guest access, presence analytics, digital signage, kiosks, and mobile Point of Sale (mPOS), to name a few. And retailers know the more they use it, the better the ROI.

A 2014 Retail survey by Devicescape showed that taking even the most basic step of offering free Wi-Fi and nothing more, bears fruit, with over 50% of those surveyed claiming their customers on average spent more time and, most importantly, more money once Wi-Fi was available.

Guest access is the tip of the iceberg – What about inventory and customer service applications such as mPOS? From beacons to digital signage to mPOS terminals, retailers are seeing an explosion in both the number and types of devices in use. All the emerging applications and the plethora of different types of devices have implications for PCI DSS compliance.

Guest Wi-Fi

The most obvious security concern with allowing guests to access your network is ensuring that payment information is kept separate and secured from guests and other users. On a shared wireless infrastructure, this is easily accomplished by isolating payment transactions on their own SSID, and having guest and non-financial business traffic on different SSIDs.

This also requires a variety of technologies including encryption, granular device- and user-based policy enforcement to ensure that the payment network is accessible to only specific users and devices and that the data is protected. Additionally, wireless bandwidth management and QoS is needed to prioritize financial transactions and ensure the SSID has adequate capacity.

Guest access is usually implemented by way of a captive portal accessible via a separate guest SSID. The captive portal keeps users in a walled garden until the user has been authenticated.

While this is not a PCI DSS concern per se, an infection through an in-store wireless connection that steals personal data could become a public relations nightmare for a retailer. For this reason, it is prudent to also implement IPS and Antivirus scanning for all connected devices.

Mobile Point of Sale

Once retailers have pervasive Wi-Fi at their facilities, adopting mPOS is a natural evolution toward improving the customer experience and streamlining operations. Breaking out an mPOS terminal allows retailers to line-bust at busy times, or simply speed up taking the money and turning over a table at a restaurant. There are numerous sales operations use cases. Airlines, for example, use mPOS to eliminate cash transactions, without significantly slowing down the beverage service.

From rugged handheld terminals to a card reader on a tablet or smartphone, mPOS equipment sales will enjoy a 40% CAGR through 2018, and it is projected that by 2018 the installed base of mPOS terminals will be larger than that of fixed terminals worldwide, according to the latest report from Smart Insights.

The adoption of mPOS by many industry leaders may lead you to assume that these solutions are secure and have been validated by the applicable Payment Card Industry (PCI) or Payment Application (PA) Data Security Standards. The short answer is that the PCI Council has not introduced any new standards specifically relating to mPOS, except for a new best practice introduced in November 2013 (PCI DSS 3.0, requirement 9.9) to prevent tampering and substitution of devices with card-reader capabilities, which only became mandatory July 1, 2015.

The fact is mPOS systems are less secure than fixed POS terminals. Lessons learned from desktop computers and servers are yet to be applied to embedded systems that make up the majority of mPOS terminals today. iOS- and Androidbased tablets are not immune to viruses either. According to F-Secure Labs, approximately 250 to 300 new threat families are discovered every quarter for Android (the majority) and iOS devices.

Mobile Payments

The emergence of mobile payments gives cyber criminals yet another reason to target Retail networks. A compromised NFC reader could potentially reveal credit card or mobile wallet information, while a compromised mobile device could allow a hacker to harvest account and identity information. It is early days for mobile payments; watch this space and beware.

Embedded Systems

Embedded systems such as mPOS terminals and mobile RFID and barcode readers, which have a very restricted UI, are hard to manage and maintain. Headless systems such as IP video cameras and fixed RFID readers are even harder, having no physical UI through which to review a device's firmware vintage and status.

Most embedded devices are based on Linux or Windows Embedded operating systems, and have only the most rudimentary access security, which is easily penetrated. Furthermore, because of their proprietary nature, and limited UI, the embedded OS is rarely updated, making the device itself a good target for network intrusion attacks such as worms and other malware.

Without appropriate IPS and Antivirus capabilities in the Wi-Fi network, an infected embedded system can go undetected for a long time, infecting other devices and potentially harvesting critical corporate or consumer data.

Even digital signage, innocuous as it may seem, poses a threat. Digital signs are nothing more than Android-, Windows-, or Linux-based computers with a big screen. They are typically Wi-Fi enabled to facilitate portability, often equipped with USB and peripheral ports which make them easy to tamper with.

Bluetooth beacons too are easy targets. Although they are mostly not Wi-Fi enabled, some are, and this is likely the trend going forward, as it enables rapid updating of messages and firmware, which is extremely tedious for stand-alone devices today. The trouble is, Bluetooth is easily hacked, giving cyber criminals access to the operating system.

Disregarding worms and viruses for a moment, once compromised, any one of the devices mentioned above could easily be turned into a rogue AP, through which cyber criminals could piggyback secure access to other systems. Or it could be an "evil twin" mimicking a legitimate AP, in order to carry out man-in-the-middle attacks on unsuspecting connected users.

The Scope of PCI DSS Requirements

PCI DSS is a global security standard provided by the Payment Card Industry Security Standards Council (PCI SSC) which requires certifiable support by any organization accepting credit and debit cards issued by the main brands such as Visa, MasterCard, or American Express. It calls out 12 broad requirements (see Table 1) for security management, policies, procedures, network architecture, software design, and other critical protective measures for data.

With PCI DSS being the core regulatory requirement for Retail networks, it is important to understand the standard and how PCI DSS defines sensitive information. But it is equally important to recognize that PCI DSS really has a very limited scope; namely, to protect financial transactions and personal data. What about the integrity of your network, the devices you use to run your business, and the devices of your customers?

PCI DSS is not the end game; comprehensive protection against all manner of cyber-threats, in existence now or in the future, is the end game! This requires security measures beyond the minimum requirements of PCI DSS. Don't forget, there have been numerous high-profile reports of Retail networks that were at the time fully PCI DSS compliant, yet still suffered severe breaches through the Wi-Fi network.

PCI DSS affects both wired and wireless networks. However, wireless networks and the emerging IoT present many additional challenges for meeting the standard and addressing the plethora of threat vectors Retail networks may be exposed to. Since the trends discussed above all revolve around wireless networks, additional technology and security measures are needed to ensure compliance while also protecting the network, devices, and applications running on that network.

PCI DSS 3.1 Requirements

1	Install and maintain a firewall configuration to protect cardholder data.
2	Do not use vendor-supplied defaults for system passwords and other security parameters.
3	Protect stored cardholder data.
4	Encrypt transmission of cardholder data across open, public networks.
5	Protect all systems against malware and regularly update anti-virus software or programs.
6	Develop and maintain secure systems and applications.
7	Restrict access to cardholder data by business need to know.
8	Identify and authenticate access to system components.
9	Restrict physical access to cardholder data.
10	Track and monitor all access to network resources and cardholder data.
11	Regularly test security systems and processes.
12	Maintain a policy that addresses information security for all personnel.

Table 1: PCI DSS 3.1 (April 2015) requirements.

WLAN PCI DSS Compliance Challenges

In their Global State of Information Security Survey 2015, PwC found that the 9,700 companies surveyed, had detected nearly 43 million security incidents in 2014. That represents a 66% CAGR in incidents since 2009. As retailers become more reliant on Wi-Fi, a greater percentage of attacks are originating from mobile devices.

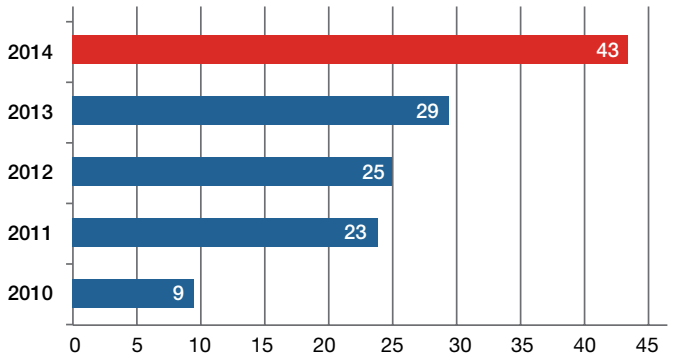

Figure 2: Security incidents detected by surveyed companies.

Meanwhile, Verizon's 2015 Data Breach Report shows that 20% of companies failed to sustain the security procedures put in place, fairing least well in Wi-Fi-related security areas.

In the 2014 assessment, average compliance rose for 11 of the 12 PCI DSS requirements, with the exception being Requirement 5 (Protect all systems against malware and regularly update anti-virus software or programs) which fell from 96% to 92%. They also noted that PCI DSS Requirement 11 had the lowest average compliance at only 80% and that full compliance had dropped from 40% to 33%. Requirement 11 relates to Rogue AP detection and reporting, vulnerability scanning, and penetration testing.

When addressing compliance mandates like PCI DSS, retailers must realize that security is a continual process—a quarterly snapshot (which is all that PCI DSS demands in many cases) is generally inadequate. Furthermore, any security measures that rely on humans initiating some action tend to break down quickly. Therefore, wherever security policies and procedures can be automatically enforced by the network, this is the most favorable strategy.

Some of the key considerations for successful PCI DSS compliance on wireless LANs are discussed below:

Network Segmentation

Retailers must be cognizant of the differences between wired and wireless networks and take special care to segment and secure the different types of networks that may be carrying cardholder data. As long as cardholder data never traverses the WLAN, the WLAN is considered out of scope as far as PCI DSS is concerned. However, whenever a wireless network is used to transmit cardholder data, it must be firewalled and monitored.

When employee, guest, and mPOS data is all sharing the same physical infrastructure, proper segmentation of the network and separation of the data requires the network to be able to identify data, applications, and traffic regardless of source.

Scanning for Unauthorized Devices

PCI DSS mandates periodic monitoring to keep unauthorized or rogue wireless devices from compromising the security of the Cardholder Data Environment (CDE). That means all networks containing a CDE must check for the presence of rogue APs and devices and take necessary measures.

Unfortunately, intrusion detection in wireless LANs is more complicated than for a wired LAN, given lack of physical control over devices and the shared medium characteristics of wireless. Since separation of trusted and untrusted networks is critical in running a secure retail operation, it is imperative that the WLAN security technology can detect and disable unauthorized wireless devices connected directly or indirectly to the CDE.

Rogue access points may be introduced in various ways:

- Mobile hotspots on laptops, smartphones, and tablets.
- Connecting a WLAN adapter to a file/application server.
- Attaching a WLAN router to the wired LAN.

For example, numerous PC applications, the Windows OS itself, and most smartphones and tablets allow users to create a virtual AP on the device. This type of rogue AP enables downstream clients to piggyback on the host device's secure network connection, and gets around typical NAC controls such as 802.1X. Therefore, detecting rogue access points and attacks from wherever they occur requires technology capable of recognizing unauthorized devices on both the wired and wireless network.

Wireless Intrusion Detection

While detecting Rogue access points and unauthorized devices is all-important, there are other types of intrusion attempts that must be safeguarded against as well.

As noted earlier, Retail networks are seeing rapid growth in the number of headless embedded systems. These are highly vulnerable to attacks that take advantage of OS vulnerabilities and unpatched systems. Worms and viruses on one infected mobile device can infect other Wi-Fi attached devices, even without either of them accessing the Internet, and they can spread rapidly, quickly compromising a fleet of cameras, mPOS terminals, or RFID readers.

Wireless Intrusion Detection Systems are needed to protect critical business applications and devices from both external and internal attacks. Such systems can detect denial-ofservice attacks, eavesdropping, keylogging, AP MAC spoofing, Honeypot attacks, and many more common network-level wireless attack types.

Enforcing Usage Policies Network-aide

PCI DSS mandates the need for acceptable usage policies and procedures, which include those for wireless devices. This means that organizations must define how wireless is to be used within their environment, how it is to be secured and deployed, and how they will address incidents as they occur.

Any usage policy should address how employees can and should use their authorized wireless devices. Just specifying a policy is not enough; technical controls must be in place to enforce it, thereby preventing sensitive data loss.

Take the case of sending credit card information in email. It is naive and unreasonable to expect all employees to appreciate the implications of putting such information in emails that might be seen by another employee not authorized to see such data, or worse, someone outside the company. No amount of security education can eliminate this risk. However, Data Loss Prevention technologies can detect and prevent it from happening, and escalate awareness that a potential violation occurred.

Strong Authentication and Encryption

Wi-Fi is considered an open, public network. PCI DSS mandates the use of strong wireless authentication and encryption to ensure that card data is transferred in an encrypted format.

This requires that Retail networks not only support a wide variety of authentication and encryption options, but that they can enforce the application of policy related to the appropriate encryption standard.

In their April 2015 update to PCI DSS v.3.1, the PCI Council states SSL and early TLS implementations are no longer considered sufficiently strong cryptography and cannot be used as a security control after June 30, 2016. Instead, TLS, IPSEC, and SSH should be used to safeguard sensitive cardholder data during transmission over open, public networks.

Continuous Malware Protection

It is not enough to put Antivirus software on devices. Many devices in Retail networks are proprietary embedded systems that do not support Antivirus software applications. Plus, you have no control over the devices belonging to your patrons.

The only reliable strategy for scanning malware is to look at the packets in every communication flow, looking for known signatures identified as malware. This type of deep packet inspection requires a lot of horsepower, along with up-to-date attack signature databases. Usually this requires specialized security appliances.

Fortinet PCI DSS Compliance and Beyond

As a recognized leader in network security, Fortinet has taken a consolidated approach to implementing wired and wireless LAN security, which sets it apart from all other vendors, and goes far beyond PCI DSS compliance.

In our controller-managed secure WLAN solution based on the award-winning FortiGate and coordinated FortiAP access points, WLAN control is tightly integrated with Firewall, VPN services, Network IPS, DLP, Antivirus scanning, Web Filtering and Application Control, on the FortiGate platform.

This approach has several compelling advantages over the typical alternative of using separate security appliances for different functions: first, it dramatically cuts the complexity and total cost of ownership of enforcing comprehensive threat protection; second, it provides far greater visibility of user behavior, device and application utilization, and threat activity; and third, it allows superior governance over bandwidth and application priorities.

These advantages are easily illustrated by understanding the fundamental difference in the way security is implemented and processed by Fortinet's consolidated architecture, versus the multiple appliance approach from other vendors.

With Fortinet's consolidated security architecture, traffic is subjected to all enabled security measures in one pass, it doesn't need to get on and off the wire, or be copied in and out of each system's memory, as it does when security is implemented in multiple separate appliances. This means that traffic is processed at the session level, so you preserve total visibility of which user, on what device, is doing what. This is absolutely crucial when it comes to applying per-user or perdevice policies for any one of these security functions.

Fortinet PCI DSS Compliance Highlights

Unified Security Policies

Fortinet unifies wired and wireless security management under a single-pane-of-glass interface, allowing retailers to implement consistent security policies across wired and wireless networks spanning thousands of remote sites. Precise granularity and control lets them define policies at the user, device, or application level, and preserve end-to-end session visibility.

By accurately detecting and securing all devices touching the network, as well as scanning for and suppressing rogue access points, Fortinet allows retailers to rapidly adopt new retail technologies and tools while still adhering to PCI DSS.

Network-wide Reporting

A key component of Fortinet's management framework is FortiAnalyzer – a network security logging, analysis, and reporting appliance that aggregates log data from all Fortinetsecurity appliances. It provides a comprehensive suite of easily customable reports that allow you to quickly analyze and visualize network threats, inefficiencies, and usage. FortiAnalyzer provides valuable tools for network vulnerability scanning, which is a key requirement for PCI DSS compliance.

Among the standard reports are comprehensive auditor-friendly PCI compliance reports relating to Rogue AP and unauthorized device detection, which eases the pain of PCI DSS compliance reporting. FortiAnalyzer provides IT with enterprise-wide, dashboard-level statistics about the overall health of wireless networks at every location, and provides the ability to drill down to determine the root cause of any problems.

WIDS and Rogue AP Detection

PCI DSS mandates regular reporting on suspicious or unknown APs. The FortiGate Rogue AP detection engine automates the scanning process to provide continuous monitoring for Rogue APs, and provides a means to determine if unknown APs are on the network.

While dedicated or background air monitors scan for unknown APs and wireless client traffic, FortiGate uses various onwire correlation techniques to determine how and where the unknown AP is physically connected to the network. It can even detect virtual APs sharing the Wi-Fi radio of an authenticated client. The Rogue AP list shows last-seen and "on-wire" status, enabling administrators to rapidly classify trusted or untrusted devices, and take corrective action to locate and remove rogues.

Zero-day Threat Protection

Given the speed with which new attacks hit the streets, retailers need automated protection in place to guard against the very latest threats. FortiGuard provides this assurance and peace of mind.

Fortinet WLAN solutions are Secured by FortiGuard, meaning that they automatically receive continuous exploit, virus, and application signature updates, ensuring immediate protection from zero-day cyber-threats. FortiGuard Labs is a global team of over 200 threat researchers who continually research the latest attacks and figure out how to neutralize them. Their work results in regular security updates that are downloaded to Fortinet products as a FortiGuard subscription service, to provide your network with the latest protection against new and emerging threats.

Signatures are created not only to address specific exploits, but also potential attack permutations, protecting customers from zero-day threats. Fortinet deploys a variety of security filters for a variety of products including traffic anomaly filters, vulnerability-based filters, and signatures.

Integrated, Centralized Authentication

Integrated, centralized authentication with single sign-on and policy enforcement is critical to providing secure centralized access to the variety of systems that exist in Retail networks.

Administrators may be responsible for systems extending out from the core of the network to thousands of branches, and they need to provision consistent, secure access to those backend systems for specific users or devices at a remote location.

FortiAuthenticator provides a secure system that tightly integrates existing directory services and allows for the quick deployment of seamless identity and access control, while supporting advanced authentication protocols such as twofactor authentication. It enables an administrator at corporate to activate the correct authentication method and access controls for a tablet, mPOS terminal, RFID reader, etc., on any Wi-Fi network, without altering the controlling FortiGate configuration.

Summary

Today's bricks and mortar retailers are faced with the daunting task of having to add new technology to their networks in order to remain competitive, while keeping sensitive data flowing through those networks secure. PCI DSS requires a wide variety of mitigating controls be in place to protect cardholder data against accidental or intentional loss, and with the latest changes to the standard introduced in April 2015, compliance requirements have only become more stringent.

Fortinet's consolidated approach to security enables consistent policies to be applied across both wired and wireless networks, simplifying management and PCI DSS compliance reporting.

January 24, 2020 9:54 AM

485440-0-0-EN

D:\Fortinet\Minor Changes\Re-color existing assets\sb-red-FA-securing-wlans-for-pci-compliance-1242020