WHITE PAPER

PCI Wireless Compliance Demystified

Best Practices for Retail

PCI Wireless Compliance Demystified

The introduction of wireless technologies in retail has created a new avenue for data breaches, circumventing traditional security architectures. Several recently publicized data breaches in the retail industry have exploited wireless vulnerabilities. Attackers have been able to access sensitive information such as credit/debit cards resulting in brand damage, financial/regulatory liabilities and retail business disruption. The Payment Card Industry (PCI) is now mandating stricter wireless security measures, and the cost of non-compliance is significant. This white paper discusses the new PCI Data Security Standard (DSS) wireless requirements and provides an executive summary of Motorola's Enterprise Wireless LAN solutions designed to provide out-of-the-box PCI compliance, robust wireless security and cost-effective compliance validation.

Retail Wireless Risks

Retailers have used wireless technology to drive business efficiencies for over twenty years. Sophisticated thieves recognize these wireless deployments offer the perfect entry point into the network to access and steal valuable customer information.

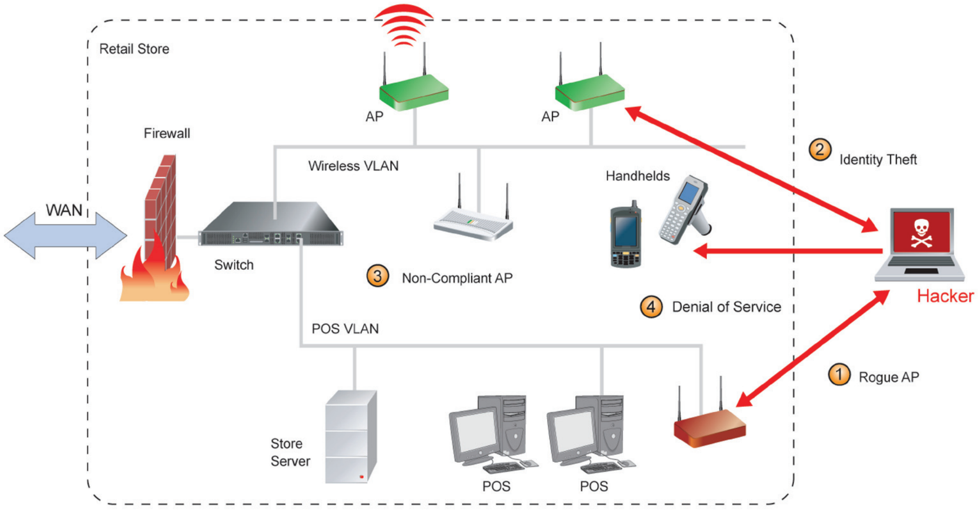


Figure 1: Typical retail store network and wireless vulnerabilities

Figure 1 illustrates a typical retail store network. The store network may include one or more of the following components – (i) Point of Sale (POS) terminals, (ii) Line of business server(s), (iii) Wireless Access Points (AP), (iv) Wireless devices (e.g., mobile terminals, barcode readers, printers, etc.), (v) Wired switches, WAN circuits and firewalls. Security conscious retailers have started segmenting their wireless and wired networks using Virtual LAN (VLAN) technology, and have also incorporated store firewalls or Access Control Lists (ACLs). Many retailers have WLANs deployed in stores for inventory management, mobile POS, wireless printing, etc. With the proliferation of low cost standards based WLAN, retailers have the following new security issues to consider.

Rogue Access Points

A rogue AP is an unauthorized wireless AP connected to the wired retail network. A rogue AP can be installed by an employee/contractor or a malicious attacker. It is important to realize rogues can show up on any network segment and even in stores that have no WLAN deployed.

- Rogue APs provide attackers with unrestricted access. They allow the attacker access to internal networks/computers just as if they were connected to an internal Ethernet port.
- Rogue APs can be installed on any network, including POS networks that have been intentionally segmented from wireless networks.
- Rogue APs can be installed in networks that specifically prohibit wireless devices.

Identity Theft

A hacker can masquerade as an authorized wireless device and connect to an authorized AP. Once on the network, all the rogue AP scenarios previously discussed are applicable.

- MAC address based ACLs are ineffective, since wireless MAC addresses are broadcast and hackers can easily change the MAC address of their device to match an authorized device.
- Wired Equivalent Privacy (WEP), the legacy WLAN encryption standard widely deployed in retail, can be cracked in a few minutes. Once hackers have the WEP key they have unrestricted access to the network allowing them to attack internal servers and applications.
- Wi-Fi Protected Access (WPA) Pre-Shared Key (PSK) is easy to implement and does not have the vulnerabilities of WEP; however, one common key is used between many devices. Hackers have been known to steal portable data terminals or use social engineering to obtain the pre-shared key. Dictionary based passwords can be cracked with relative ease. Once the PSK is compromised, the entire network is vulnerable until administrators change the key at every AP and every portable data terminal.

Non-Compliant APs

Wireless APs are frequently misconfigured. According to Gartner, the majority of all wireless security incidents happen as a result of misconfigured devices. Misconfigurations happen for a variety of reasons including human error and bugs in the AP's management software.

- A misconfigured AP in a store or distribution center can be detected and exploited by a hacker to gain access to the network.
- WLAN APs and infrastructure contain well-known vulnerabilities that can result in information disclosure, privilege escalation, and unauthorized access through fixed authentication credentials.

Denial of Service (DoS)

Hackers can easily perform wireless DoS attacks preventing devices from operating properly and stopping critical business operations.

- Wireless DoS attacks can cripple a distribution center or store despite the best security standards being deployed.
- Hackers can insert malicious multicast or broadcast frames via wireless APs that can wreak havoc on the internal wired network.

Cost of a Data Breach

In 2007, the Ponemon Institute published a study that examined the costs incurred by 35 companies after experiencing a data breach [1]. The cost of a data breach averaged $197 per compromised customer record in 2007, up from $182 per compromised record in 2006. Lost business opportunities, including losses resulting from brand damage and customer churn represented the most significant cost increase, rising from $98 in 2006 to $128 in 2007.

Retail Wireless Exposure

Several recent high profile data breaches have occurred as a direct result of wireless vulnerabilities. The most recent one at TJX was highly publicized and resulted in at least 45.7 million credit and debit card data being compromised. According to the Wall Street Journal [2], the TJX breach occurred as a direct result of weak wireless security. In August, 2008, the US Department of Justice announced [3] that "eleven perpetrators allegedly involved in the hacking of nine major U.S. retailers and the theft and sale of more than 40 million credit and debit card numbers have been charged with numerous crimes, including conspiracy, computer intrusion, fraud and identity theft." The indictments alleged that during the course of the sophisticated conspiracy, the perpetrators obtained the credit and debit card numbers by "wardriving" and hacking into the wireless computer networks of major retailers — including TJX Companies, BJ's Wholesale Club, OfficeMax, Boston Market, Barnes & Noble, Sports Authority, Forever 21 and DSW. Once inside the networks, they installed "sniffer" programs that would capture card numbers, as well as password and account information, as they moved through the retailers' credit and debit processing networks.

[1] 2007 Annual Study: Cost of a Data Breach, http://www.ponemon.org/press/PR_Ponemon_2007-COB_071126_F.pdf

[2] How Credit-Card Data Went Out Wireless Door - Biggest Known Theft Came from Retailer With Old, Weak Security, By Joseph Pereira, Wall Street Journal, May 4, 2007; Page A1

[3] Retail Hacking Ring Charged for Stealing and Distributing Credit and Debit Card Numbers from Major U.S. Retailers - More Than 40 Million Credit and Debit Card Numbers Stolen, http://www.usdoj.gov/opa/pr/2008/August/08-ag-689.html

PCI Wireless Compliance Overview

The alarming increase in credit/debit card numbers and identity theft in retail has led to the creation and enforcement of stricter information security standards. Wireless specific requirements have also become stricter and retailers often find wireless as the "Achilles' heel" from a security and compliance perspective.

> ***"Merchants that have implemented or are considering using wireless technology must develop and deploy a comprehensive strategy to secure their systems from intrusion. … It has come to Visa's attention that some entities are not properly securing their wireless networks, which increasingly leads to the compromise of cardholder data, brand damage, and other concerns — both financial and regulatory."***
>
> Visa, August 2006

The PCI Security Standards Council is an open global forum, founded by American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International, for the ongoing development, enhancement, storage, dissemination and implementation of security standards for account data protection.

PCI released an updated version of their Data Security Standard (DSS) that went into effect starting October 1st, 2008. PCI DSS [4] version 1.2 is the global standard adopted by the card brands for all organizations that process, store or transmit cardholder data. It consists of steps that mirror security best practices.

PCI DSS Goals & Broad Requirements	
Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored data 4. Encrypt transmission of cardholder data and sensitive information across public networks
Maintain a Vulnerability Mgmt Program	5. Use and regularly update anti-virus software 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to data using a "need-to-know" methodology 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security

[4] https://www.pcisecuritystandards.org/

PCI DSS[5] version 1.2 places special emphasis on WLAN security. It requires Cardholder Data Environments (CDE) change wireless defaults (passwords, SSIDs, keys, etc.), use strong encryption, eliminate rogue/unauthorized wireless devices, restrict physical access to wireless devices, log wireless activity, define wireless usage policies, etc., as shown in the following table. PCI DSS wireless requirements can be broken down into the following two primary categories.

1. Universally applicable wireless requirements:
   These are requirements all companies should have in place to protect their wired networks from attacks via rogue or unknown wireless access points and clients. They apply to companies regardless of their use of wireless technology. As a result, they are universally applicable to companies wishing to comply with the PCI DSS.

2. Requirements applicable for in-scope wireless networks:
   These are requirements all companies who rely on wireless technology should have in place to protect those systems. They are specific to the usage of wireless technology in-scope for PCI DSS compliance. These requirements apply in addition to the universally applicable set of requirements.

PCI DSS 1.2 Wireless Requirements

Scope	Section	Requirement
Universally Applicable Requirements	11.1	Identify rogue and unauthorized wireless devices
	12.9	Responding to unauthorized wireless
Scoping	1.2.3	Firewall wireless from card holder network
Requirements for In-Scope Wireless Networks	2.1.1	Changing default wireless settings
	4.1.1	Encryption in wireless networ ks
	9.1.3	Physically secure wireless devices
	10.5.4	Audit logging of wireless activity
	11.4	Intrusion prevention (IPS) for wireless traffic
	12.3	Usage policies and procedures for wireless

Figure 2 shows a step by step flowchart for becoming compliant with PCI DSS from a wireless LAN perspective.

[5] https://www.pcisecuritystandards.org/security_standards/pci_dss_download.html

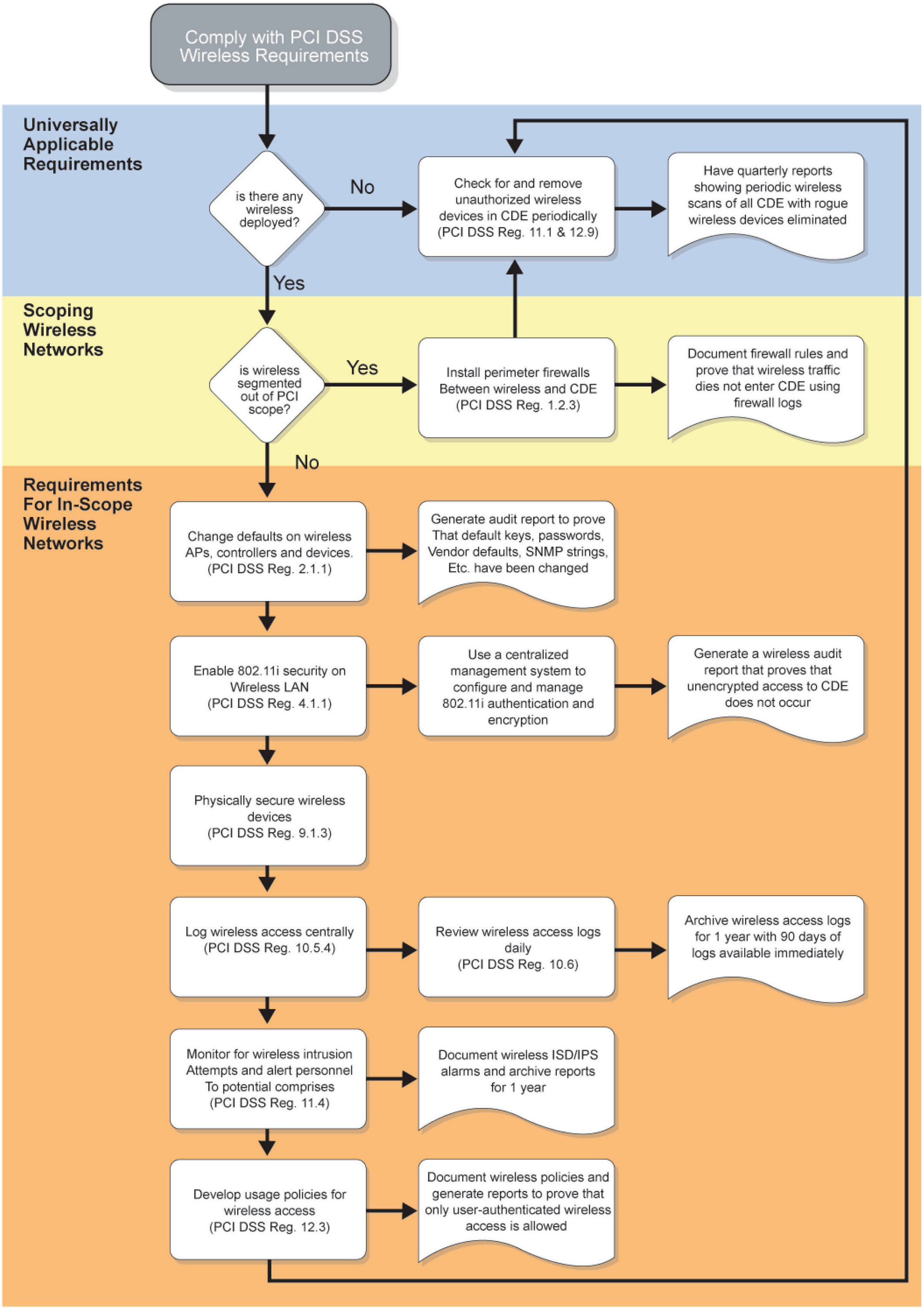

Comply with PCI DSS Wireless Requirements
Universally Applicable Requirements
is there any wireless deployed?
No
Yes
Check for and remove unauthorized wireless devices in CDE periodically (PCI DSS Reg. 11.1 & 12.9)
Have quarterly reports showing periodic wireless scans of all CDE with rogue wireless devices eliminated
Scoping Wireless Networks
is wireless segmented out of PCI scope?
Yes
No
Install perimeter firewalls Between wireless and CDE (PCI DSS Reg. 1.2.3)
Document firewall rules and prove that wireless traffic dies not enter CDE using firewall logs
Requirements For In-Scope Wireless Networks
Change defaults on wireless APs, controllers and devices. (PCI DSS Reg. 2.1.1)
Generate audit report to prove That default keys, passwords, Vendor defaults, SNMP strings, Etc. have been changed
Enable 802.11i security on Wireless LAN (PCI DSS Reg. 4.1.1)
Use a centralized management system to configure and manage 802.11i authentication and encryption
Generate a wireless audit report that proves that unencrypted access to CDE does not occur
Physically secure wireless devices (PCI DSS Reg. 9.1.3)
Log wireless access centrally (PCI DSS Reg. 10.5.4)
Review wireless access logs daily (PCI DSS Reg. 10.6)
Archive wireless access logs for 1 year with 90 days of logs available immediately
Monitor for wireless intrusion Attempts and alert personnel To potential comprises (PCI DSS Reg. 11.4)
Document wireless ISD/IPS alarms and archive reports for 1 year
Develop usage policies for wireless access (PCI DSS Reg. 12.3)
Document wireless policies and generate reports to prove that only user-authenticated wireless access is allowed

Figure 2: Complying with PCI DSS wireless requirements

Universally Applicable PCI Wireless Requirements

Although PCI DSS outlines requirements for securing existing wireless technologies, there are validation requirements that extend beyond the known wireless devices and require monitoring of unknown and potentially dangerous "rogue" devices. A rogue wireless device is an unauthorized wireless device that can allow access to the CDE.

Wireless networks can be out of PCI scope if (i) no wireless is deployed or (ii) if wireless has been deployed and segmented away from the CDE. If no wireless is deployed, periodic monitoring is needed to keep unauthorized or rogue wireless devices from compromising the security of the CDE. Segmenting wireless networks out of PCI scope typically requires a firewall between the wireless network and the CDE.

PCI DSS Requirement	*Testing Procedure*
11.1 Test for the presence of wireless access points by using a wireless analyzer at least quarterly or deploying a wireless IDS/IPS to identify all wireless devices in use.	Verify that a wireless analyzer is used at least quarterly, or that a wireless IDS/IPS is implemented and configured to identify all wireless devices. If a wireless IDS/IPS is implemented, verify the configuration will generate alerts to personnel. Verify the organization's Incident Response Plan (Requirement 12.9) includes a response in the event unauthorized wireless devices are detected.
12.9.3 Designate specific personnel to be available on a 24/7 basis to respond to alerts.	Verify through observation and review of policies, that there is 24/7 incident response and monitoring coverage for any evidence of unauthorized activity, detection of unauthorized wireless access points, critical IDS alerts, and/or reports of unauthorized critical system or content file changes.

Wireless Scanning

The purpose of requirement 11.1 is to ensure unauthorized or rogue wireless device cannot access the CDE. The intent is to prevent an attacker from using rogue wireless devices to negatively impact the security of cardholder data. It is acceptable to use wireless analyzer or a preventative control such as a Wireless Intrusion Detection/ Prevention System (IDS/IPS) as defined by the standard.

Since a rogue device can potentially show up in any location, it is important all locations are either scanned regularly or wireless IDS/IPS systems are implemented in all locations. An organization may not choose to select a sample of sites for compliance. Organizations must ensure they scan all sites quarterly to comply with the standard. The organization's responsibility is to ensure the CDE is compliant at all times. During a PCI DSS assessment, the organization or their assessor may choose to validate compliance with requirement 11.1 by choosing a sample of all locations. The PCI SSC leaves sampling, for the purposes of validation, at the discretion of the organization or their assessor. As part of the validation, the assessor should check that the organization has the appropriate process and technology in place to comply at all locations.

The PCI DSS requirement clearly specifies the use of a wireless analyzer or a wireless IDS/IPS system for scanning. Relying on wired side scanning tools (tools that scan suspicious hardware MAC addresses on switches) may identify some unauthorized wireless devices. However, they tend to have very high false positive/negative detection rates. Wired network scanning tools often miss cleverly hidden and disguised rogue wireless devices or devices connected to isolated network segments. Wired scanning also fails to detect many instances of rogue wireless clients. A rogue wireless client is a device whose wireless connection is not intended within the environment. Although insufficient on their own, wired analysis tools can be valuable when used in conjunction with wireless analyzers to improve the quality of the scan results.

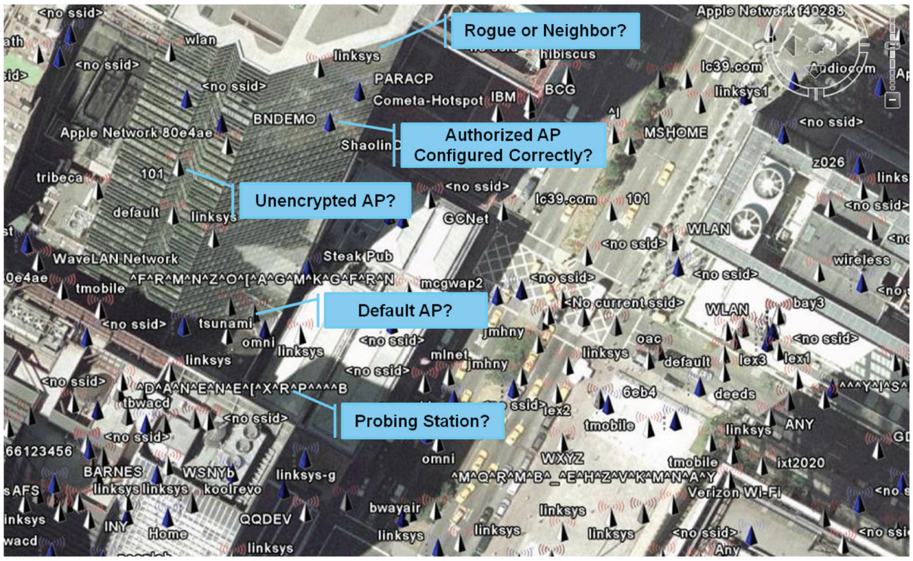


Figure 3: Wireless scanning challenges – wireless devices around 5th Avenue, New York, (Source: Google Earth, Wigle.net)

Organizations can use freely available tools such as NetStumbler or Kismet as wireless analyzers running on a laptop. Using this method, a technician or auditor can walk around each site and detect wireless devices. They can then manually investigate each device to determine if it allows access to the CDE and classify them as rogues or just friendly neighboring wireless devices. Although this method is technically acceptable, it is often times operationally tedious, error prone, and costly. Figure 3 shows a scan of wireless devices present within a few blocks around 5th Avenue in New York City. A wireless store scan would detect multiple devices and the process of separating neighboring devices from true rogues on the network is tedious and error-prone if done manually. It is recommended wireless scanning be automated, with wireless IDS/IPS systems capable of automatically and accurately classifying rogue devices co-existing within the shared wireless medium.

Although the PCI DSS standard does not directly state what the output of wireless analysis should be, it does imply it should be created, reviewed, and used to mitigate the risk of unauthorized or rogue wireless devices. At a minimum, the list of wireless devices should clearly identify all rogue devices connected to the network. To comply with the intent of requirement 11.1, companies should immediately remediate the rogue threat in accordance with requirement 12.9 and rescan the environment at the earliest possible opportunity. This is similar to other verification requirements within the PCI DSS. Manual scanning and mitigation can be tedious and it is recommended the process be automated using a centrally managed wireless IDS/IPS.

Segmenting Wireless Networks

PCI compliance mandates a firewall be installed between any wireless networks capable of accessing the CDE and the CDE. Wireless networks that do not store, process or transmit card holder data should be isolated from the CDE. Robust firewalls are a well established method of isolating and containing network segments. The intent is to prevent unauthorized users from accessing the CDE via a wireless network for purposes other than credit card transactions. The wireless firewall should perform the following general functions: (i) Filter packets originating from wireless network segments, (ii) Perform stateful inspection of connections, (iii) Log traffic allowed and denied by the firewall.

PCI DSS Requirement	***Testing Procedure***
1.2.3 Install perimeter firewalls between any wireless networks and the cardholder data environment, and configure these firewalls to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.	Verify that there are perimeter firewalls installed between any wireless networks and systems that store cardholder data, and that these firewalls deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.

PCI DSS compliance requires all firewall and security policies be audited and verified every 6 months, at a minimum. If a firewall is shared between wireless and other protocols/applications, the default policy for handling inbound traffic should be to block all packets and connections into the CDE unless the traffic type and connections have been specifically permitted. This approach is more secure than another approach used often: permit all connections and traffic by default and then block specific traffic and connections. Traffic originating from networks that have wireless that are supposed to be out of the CDE should explicitly be blocked. Organizations should consider using outbound traffic filtering as a technique for further securing their networks and reducing the likelihood of internally based attacks. As a rule, any protocol and traffic not necessary in the CDE (not used or needed for credit card transactions), should be blocked. This will result in a reduced risk of attack and will create a CDE with less traffic and is easier to monitor.

Requirements Applicable for In-scope Wireless Networks

PCI DSS compliance for wireless networks that are in-scope requires (i) strong authentication and encryption; (ii) changing default passwords and settings on wireless devices; (iii) physical security of wireless devices (iv); logging of wireless access and intrusion prevention (v); development and enforcement of wireless usage policies.

Strong Authentication and Encryption

By 2001, a series of independent studies from various academic and commercial institutions had identified weaknesses in Wired Equivalent Privacy (WEP), the original security mechanism in the Institute of Electrical and Electronics Engineers (IEEE) 802.11 specification. These studies showed that, even with WEP enabled, an intruder equipped with the proper tools and a moderate amount of technical knowledge could gain unauthorized access to the wireless network via the WLAN.

In 2003, the Wi-Fi Alliance introduced Wi-Fi Protected Access (WPA™), as a strong, standards-based interoperable Wi-Fi security specification. WPA provides assurance data will remain protected and only authorized users may access their networks. WPA uses Temporal Key Integrity Protocol (TKIP) for data encryption to change the keys used for encryption on a per packet basis.

In 2004, the Wi-Fi Alliance introduced Wi-Fi Protected Access 2 (WPA2™), the second generation of WPA security. Like WPA, WPA2 provides Wi-Fi users with a high level of assurance that their data will remain protected and that only authorized users can access their wireless networks. WPA2 is based on the final IEEE 802.11i amendment to the 802.11 standard ratified in June 2004. WPA2 uses the Advanced Encryption Standard (AES) for data encryption and is eligible for FIPS (Federal Information Processing Standards) 140-2 compliance.

PCI DSS 1.2 compliance requires discontinuing WEP, and moving to the robust encryption and authentication provided by the IEEE 802.11i standard. The Wi-Fi Alliance certifies products as WPA or WPA2 compatible for interoperability based on the 802.11i standard.

PCI DSS Requirement	*Testing Procedure*
4.1.1 Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices (for example, IEEE 802.11i) to implement strong encryption for authentication and transmission. • For new wireless implementations, it is prohibited to implement WEP after March 31, 2009. • For current wireless implementations, it is prohibited to use WEP after June 30, 2010.	Verify the following regarding vendor default settings for wireless environments and ensure that all wireless networks implement strong encryption mechanisms (for example, AES): • Encryption keys were changed from default at installation, and are changed anytime anyone with knowledge of the keys leaves the company or changes positions • Default SNMP community strings on wireless devices were changed • Default passwords/passphrases on access points were changed • Firmware on wireless devices is updated to support strong encryption for authentication and transmission over wireless networks (for example WPA/WPA2) • Other security-related wireless vendor defaults, if applicable

There are two modes in WPA and WPA2 - Enterprise and Personal. Both provide an authentication and encryption solution.

Mode	*WPA*	*WPA2*
Enterprise	Authentication: IEEE 802.1X/EAP Encryption: TKIP/MIC	Authentication: IEEE 802.1X/EAP Encryption: AES-CCMP
Personal	Authentication: PSK Encryption: TKIP/MIC	Authentication: PSK Encryption: AES-CCMP

Personal mode is generally designed for home and Small Office Home Office (SOHO) users who do not have authentication servers available. It operates in an unmanaged mode that uses a Pre-Shared Key (PSK) for authentication instead of IEEE 802.1X. This mode uses applied authentication in which a pass-phrase (the PSK) is manually entered on the access point to generate the encryption key. Consequently, it does not scale well in the enterprise. The PSK is typically shared among users. Weak passphrases are vulnerable to password cracking attacks. To protect against a brute force attack, a truly random passphrase of 13 or more characters (selected from the set of 95 permitted characters) is probably sufficient. Rainbow tables (pre-computed password hashes based on an exhaustive list of password character combinations) have been computed by the "Church of WiFi"[6] for popular SSIDs for a several different WPA/WPA2 passphrases. To further protect against intrusion, the WPA-PSK network's SSID should be unique.

[6] http://www.renderlab.net/projects/WPA-tables/

Enterprise mode meets the rigorous requirements of enterprise security. It leverages the IEEE 802.1X authentication framework using an Extensible Authentication Protocol (EAP) with an authentication server to provide strong mutual authentication between the client and authentication server (via the access point). Each user is assigned a unique key mechanism for access to the WLAN. This affords a high level of individual privacy. For WPA, TKIP encryption is used. TKIP employs an encryption cipher that issues encryption keys for each data packet communicated in each session of each user, making the encryption code extremely difficult to break. For WPA2, AES encryption is used. AES is stronger than TKIP, thus providing additional network protection.

Changing Default Settings

Changing default administrative passwords, encryption settings, reset functions, automatic network connection functions, factory default shared keys and Simple Network Management Protocol (SNMP) access helps eliminate many of the vulnerabilities impacting the security of the CDE.

PCI DSS Requirement	***Testing Procedure***
2.1.1 For wireless environments connected to the cardholder data environment or transmitting cardholder data, change wireless vendor defaults, including but not limited to default wireless encryption keys, passwords, and SNMP community strings. Ensure wireless device security settings are enabled for strong encryption technology for authentication and transmission.	Verify the following regarding vendor default settings for wireless environments and ensure that all wireless networks implement strong encryption mechanisms (for example, AES): • Encryption keys were changed from default at installation, and are changed anytime anyone with knowledge of the keys leaves the company or changes positions • Default SNMP community strings on wireless devices were changed • Default passwords/passphrases on access points were changed • Firmware on wireless devices is updated to support strong encryption for authentication and transmission over wireless networks (for example WPA/WPA2) • Other security-related wireless vendor defaults, if applicable

Often, WLAN devices ship with their own default settings, some of which inherently contain security vulnerabilities. An administrator password is a prime example. On some APs, the factory default configuration does not require a password (the password field is blank). Other APs might have simple and well-documented passwords ("password" or "admin"). Unauthorized users can easily gain access to the device's management console if default settings are left unchanged. Similarly, many wireless APs have a factory default setting that allows unencrypted wireless access. Some APs might be pre-configured for WEP access with simple keys like "111111".

Some wireless APs use SNMP agents, which allow network management software tools to monitor the status of wireless APs and clients. The first two versions of SNMP (SNMPv1 and SMPv2) support only trivial authentication based on plain-text community strings and, as a result, are fundamentally insecure. SNMPv3, which includes mechanisms to provide strong security, is highly recommended. If SNMP is not required on the network, the organization should simply disable SNMP altogether. It is common knowledge the default SNMP community string that SNMP agents commonly use is the word "public" with assigned "read" or "read and write" privileges. Leaving default strings unchanged makes devices vulnerable to attacks. Organizations that require SNMP should change the default community string, as often as needed, to a strong community string. Privileges should be set to "read only" if that is the only access a user/system requires.

All Wi-Fi APs have a Service Set ID (SSID). The SSID is an identifier that is sometimes referred to as the "network name" and is often a simple ASCII character string. The SSID is used to assign an identifier to the wireless network (service set). Clients that wish to join a network scan an area for available networks and join by providing the correct SSID. Disabling the broadcast SSID in the APs forces a client device to perform active scanning (probing with a specific SSID). The default SSID values used by many 802.11 wireless LAN vendors are published and well-known to would-be adversaries. Suppressing the SSID is not necessarily a security mechanism, as a hacker can sniff the SSID using fairly trivial techniques. However, broadcasting an SSID that advertises the organization's name or is easily identifiable with the organization is not recommended.

Physical Security of Wireless Devices

PCI DSS promotes the need for physical security surrounding wireless devices. The focus of this requirement is on securing publically accessible or risky devices. This does not imply organizations need to put a physical cage around every AP or chain down every handheld device. The intent is to reasonably secure those devices generally accessible to the public or at risk of being lost or stolen.

PCI DSS Requirement	***Testing Procedure***
9.1.3 Restrict physical access to wireless access points, gateways, and handheld devices.	Verify physical access to wireless access points, gateways, and handheld devices is appropriately restricted.

Although the requirements do not state how to secure such devices, there are many ways to implement physical security. For example, many consumer grade APs have a "factory reset" feature. The reset function poses a particular problem because it allows an individual to negate any security settings that administrators have configured in the AP. It does this by returning the AP to its default factory settings. The default settings generally do not require an administrative password and may disable encryption. An individual can reset the configuration to the default settings simply by inserting a pointed object such as a pen into the reset hole and pressing. If a malicious user gains physical access to the device, that individual can exploit the reset feature and cancel out any security settings on the device. Additionally, resets can be invoked remotely over the management interface or using a serial console interface on the AP. These require physical access and PCI recommends that adequate

Options for securing wireless devices may include physically restricting access (by mounting APs high up on the ceiling) and disabling the console interface and factory reset options by using a tamper-proof chassis. Many enterprise APs are equipped with special mounting brackets that prevent ready access to the Ethernet cable.

Securing handheld wireless devices and laptops is more difficult since physical access to these devices is required. Precautions such as avoiding PSKs and passwords printed on the device are recommended. Inventory management of wireless devices and being able to track and report missing devices is recommended.

Wireless Intrusion Prevention and Access Logging

Intrusion detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents, which are violations or imminent threats of violation of computer security policies, acceptable use policies, or standard security practices. An Intrusion Detection System (IDS) is software that automates the intrusion detection process. An Intrusion Prevention System (IPS) is a system that has all the capabilities of an IDS and can also attempt to stop incidents

PCI DSS Requirement	*Testing Procedure*
11.4 Use intrusion-detection systems, and/or intrusion-prevention systems to monitor all traffic in the cardholder data environment and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines up-to-date.	Verify the use of intrusion-detection systems and/or intrusion-prevention systems and that all traffic in the cardholder data environment is monitored. Confirm IDS and/or IPS are configured to alert personnel of suspected compromises. Examine IDS/IPS configurations and confirm IDS/IPS devices are configured, maintained, and updated per vendor instructions to ensure optimal protection.

Wireless IDS/IPS provides several types of security capabilities. Because wireless IDS/IPS is a relatively new form of IDS/IPS, capabilities currently vary widely among products.

Most wireless IDS/IPS can create and maintain an inventory of observed WLAN devices, including APs, WLAN clients, and ad hoc (peer-to-peer) clients. The inventory is usually based on the SSIDs and MAC addresses of the devices' wireless network cards. Some systems can also use fingerprinting techniques on observed traffic to verify the vendor, instead of relying on MAC address information (which could be spoofed). The inventory can be used as a profile to identify new WLAN devices and the removal of existing devices. Administrators can then tag each entry as being an authorized WLAN, a benign neighboring WLAN (another organization in the same building), or a rogue WLAN. When evaluating solutions, it is recommended enterprises evaluate the automatic device classification capabilities of the wireless IDS/IPS.

A wireless IDS/IPS typically performs extensive logging of data related to detected events. This data can be used to confirm the validity of alerts, investigate incidents, and correlate events between the IDS/IPS and other logging sources. Data fields commonly logged by a wireless IDS/IPS include the following: (i) Timestamp (usually date and time), (ii) Event or alert type, (iii) Priority or severity rating, (iv) Source MAC address (the vendor is often identified from the address), (v) Channel number, and, (vi) Location of event or ID of the sensor observing the event.
A wireless IDS/IPS can detect attacks, misconfigurations, and policy violations at the WLAN protocol level, primarily examining IEEE 802.11 protocol communication. It typically does not examine communications at higher networking layers (IP addresses, application payloads etc.). Some products perform only simple signature-based detection, while others use a combination of signature-based detection, anomaly based detection and stateful protocol analysis techniques. Organizations should use wireless IDS/IPS products that use this combination of techniques to achieve broader and more accurate detection.

The types of events detected by wireless IDS/IPS include:

1. Unauthorized WLANs and WLAN devices: Through its information gathering capabilities, a wireless IDS/IPS can detect rogue APs, unauthorized STAs and unauthorized WLANs (both infrastructure mode and ad hoc mode).

2. Poorly secured WLAN devices: Most wireless IDS/IPSs can identify APs and STAs not using the proper security controls. This includes detecting misconfigurations and weak WLAN protocols. This is accomplished by identifying deviations from organization-specific policies for setting encryption, authentication, data rates, SSID names, and channels. For example, they could detect a wireless device is using WEP instead of WPA2.

3. Unusual usage patterns: Some wireless IDS/IPSs use anomaly-based detection methods to detect unusual WLAN usage patterns (e.g., a lot more clients than usual connected to a particular AP, or a higher than usual amount of network traffic between a client and an AP). In this instance, one of the devices might have been compromised, or unauthorized parties might be using the WLAN. Many systems can identify failed attempts to join the WLAN, such as alerting on several failed attempts in a short period of time, which could indicate an attempt to gain unauthorized access to the WLAN. Some systems can also alert if any WLAN activity is detected during off-hours periods.

4. Denial of service (DoS) attacks: DoS attacks include logical attacks such as flooding (which involves sending large numbers of messages to an AP at a high rate), spoofing (which involves sending fake messages that disrupt wireless connections) and physical attacks such as jamming (which involves emitting electromagnetic energy on the WLAN's frequencies to make the frequencies unusable by the WLAN). DoS attacks can often be detected through stateful protocol analysis and anomaly detection methods. These methods determine if the observed activity is consistent with the expected activity. Many denial of service attacks are detected by counting events during periods of time and alerting when threshold values are exceeded. For example, a large number of events involving the termination of wireless network sessions can indicate a DoS attack.

5. Impersonation and man-in-the-middle attacks: Some wireless IDS/IPSs can detect when a device is attempting to spoof the identity of another device. This is done by identifying differences in the characteristics of the activity, such as certain values in frames.

Wireless IDS/IPS can identify the physical location of a detected threat by using signal strength triangulation - estimating the threat's approximate distance from multiple sensors by the strength of the threat's signal received by each sensor, then calculating the physical location at which the threat would be the estimated distance from each sensor. This allows an organization to send physical security staff to the location to address the threat. Wireless IDS/IPS use building floor plans to determine if the threat is inside or outside a building, or if it is in a public area or secured area. This information is helpful not only in finding and stopping the threat, but also in prioritizing the response to the threat. Wireless IDS/IPS can set the priority of alerts based in part on the location of each threat. Laptop based IDS/IPS sniffers can also be used to pinpoint a threat's location, particularly if fixed sensors do not offer triangulation capabilities or if the threat is moving.

Development and Enforcement of Wireless Usage Policies

The PCI DSS mandates the need for acceptable usage policies and procedures, which include those for wireless devices. The importance here is that organizations understand how wireless is to be used within their environment, how it is to be secured and deployed, and how the organization will address incidents as they occur. Another important aspect the policy should address is how employees can, and should, use their authorized wireless devices. For example, if employees receive laptops, they need to understand the acceptable usage and responsibilities of wireless networking. If an employee receives a wireless inventory device, they need to understand how to properly protect, access, and store that device.

PCI DSS Requirement	***Testing Procedure***
12.3 Develop usage policies for critical employee-facing technologies (for example, remote-access technologies, wireless technologies, removable electronic media, laptops, personal data/digital assistants (PDAs), e-mail usage and Internet usage) to define proper use of these technologies for all employees and contractors.	**12.3** Obtain and examine the policy for critical employee-facing technologies.

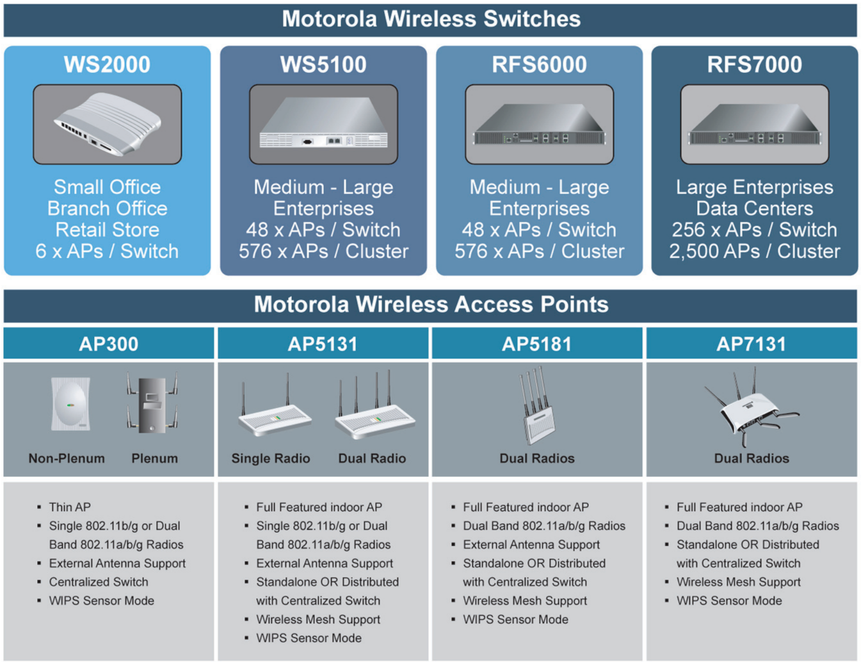
PCI compliance mandates organizations to verify that the usage policies require explicit management approval to use wireless networks in the CDE. Any unsanctioned wireless must be removed from the CDE. Usage policies require wireless access is authenticated with a user ID and password or other authentication item (for example, token). WPA Enterprise supports this requirement. If PSKs are used then they must be rotated whenever employees that have access to wireless devices leave the organization. In Enterprise mode, individual user access can be enabled/disabled centrally. PCI compliance further requires the organization to maintain a list of approved products. For example, if a wireless AP needs to be replaced, substituting it with a non-sanctioned AP is not acceptable.

PCI compliance requires automatic disconnect of wireless sessions after a specific period of inactivity. For example, a wireless POS terminal should automatically logout and disconnect from the CDE if left unattended.

PCI compliance also prohibits copying, moving, or storing of cardholder data onto local hard drives, and removable electronic media when accessing such data via wireless-access technologies. For example, if a wireless POS is being used card holder data should not be stored locally on the device, it should only be encrypted and transmitted.

Motorola WLAN Solution for PCI Compliance

Motorola offers a comprehensive portfolio of wireless LAN infrastructure solutions designed to enable the truly wireless enterprise, regardless of the size of its business - from large enterprises with locations all over the world to branch offices and small businesses. Motorola's Wireless Enterprise portfolio offers resiliency, security and performance equal to or greater than a wired network.



Motorola Wireless Switches

WS2000	WS5100	RFS6000	RFS7000
Small Office Branch Office Retail Store 6 x APs / Switch	Medium - Large Enterprises 48 x APs / Switch 576 x APs / Cluster	Medium - Large Enterprises 48 x APs / Switch 576 x APs / Cluster	Large Enterprises Data Centers 256 x APs / Switch 2,500 APs / Cluster

Motorola Wireless Access Points

AP300	AP5131	AP5181	AP7131
Non-Plenum Plenum	Single Radio Dual Radio	Dual Radios	Dual Radios
▪ Thin AP ▪ Single 802.11b/g or Dual Band 802.11a/b/g Radios ▪ External Antenna Support ▪ Centralized Switch ▪ WIPS Sensor Mode	▪ Full Featured indoor AP ▪ Single 802.11b/g or Dual Band 802.11a/b/g Radios ▪ External Antenna Support ▪ Standalone OR Distributed with Centralized Switch ▪ Wireless Mesh Support ▪ WIPS Sensor Mode	▪ Full Featured indoor AP ▪ Dual Band 802.11a/b/g Radios ▪ External Antenna Support ▪ Standalone OR Distributed with Centralized Switch ▪ Wireless Mesh Support ▪ WIPS Sensor Mode	▪ Full Featured indoor AP ▪ Dual Band 802.11a/b/g Radios ▪ Standalone OR Distributed with Centralized Switch ▪ Wireless Mesh Support ▪ WIPS Sensor Mode

Figure 4: Motorola wireless LAN infrastructure solution

Motorola's complete portfolio of wireless LAN infrastructure, as shown in Figure 4, is built on an integrated upgradeable platform, allowing organizations to cost-efficiently extend wireless networking from headquarters, to retail stores and distribution centers with ease of integration and manageability. The WS2000 Wireless Switch offers an easy to manage network-in-a-box solution for small enterprises and remote sites, including an integrated router, gateway, firewall, and Power-over-Ethernet (PoE). The RFS7000 provides robust, highly scalable support for enterprise mobility, offering enhanced roaming, security, quality of service and management features. Motorola's RF Management Suite (RFMS) is a powerful set of integrated applications that enable administrators to execute end-to-end design and management of wireless LANs — pre- and post-deployment. All Motorola APs are designed for enterprise class wireless security supporting IEEE 802.11i (WPA and WPA2 certified) and 3DES IPSec encryption.

Motorola Wireless IPS Solution

The Motorola AirDefense Solution is based on patented technology that incorporates distributed smart IEEE 802.11 sensors reporting to a central server appliance. Remote sensors are deployed in stores, distributions centers and the retail headquarters. Sensors are deployed with dedicated radios. On Motorola dual radio APs like the AP-5131 or the AP-7131, one radio can be dedicated for monitoring and the other for access. Sensors monitor all WLAN activities 24x7 in their local airspace and communicate with the AirDefense server, which correlates and analyzes the data to provide scalable, centralized management for security and operational support of the WLAN. Administrators access the system via management console software installed on the computer.

AirDefense recognizes all WLAN devices, including APs, WLAN user stations, "soft APs" where stations function as APs and specialty devices such as wireless bar code scanners and mobile terminals for shipping or inventory applications. AirDefense also identifies rogue behavior from ad-hoc or peer-to-peer networking between user stations and accidental associations from user stations connecting to neighboring networks. AirDefense Enterprise can accurate distinguish neighboring devices from rogue devices connected to the retail network. In a mall with several stores, one is likely to see many neighboring wireless devices. It is crucial a WIPS be able to accurately classify neighboring devices from actual rogue devices connected to the store network.

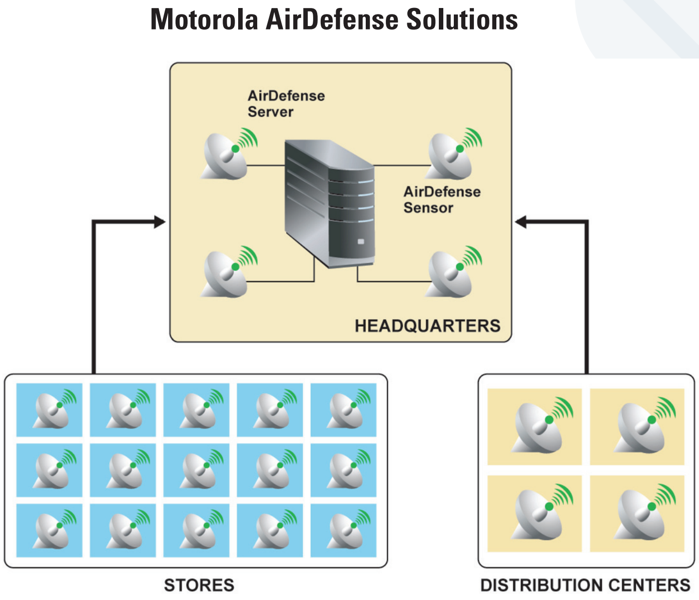


Figure 5: Motorola AirDefense Enterprise solution

AirDefense Enterprise can be setup to automatically terminate a rogue device over the air. Alternatively, the device can be blocked on the wired side using switch port suppression. To find the location of the rogue device, AirDefense provides accurate map based location tracking using signal strength triangulation. The system intelligently sorts through multiple floor plans and enables the IT administrator to locate and track rogue devices in real-time.

PCI Requirement		***Motorola Solution***
11.1	Identify rogue and unauthorized wireless devices	Motorola AirDefense wireless IPS provides • Accurate classification of rogues from neighboring wireless devices • Detection capabilities across segmented and firewalled networks • Vendor agnostic detection of WLAN devices • Location tracking of devices on a map • Minute-by-minute granular forensic information for any device • Scalability to thousands of distributed locations • Dual-radio Motorola APs for 24x7 monitoring and full-time AP function
12.9	Responding to unauthorized wireless	Motorola AirDefense wireless IPS provides • 24x7 wireless monitoring • Automatic rogue termination using wireless and wired techniques • Flexible reporting and alerting options with integration capabilities into various Security Information Management (SIM) systems • Ability to automatically create ACLs for suspicious devices
1.2.3	Firewall wireless from card holder network	• Motorola wireless switches supports stateful Layer 2 and role-based firewalls. Base the security policy on user, group, location, encryption strength, etc. • Follow a user as they move across different APs and switches • Provide a stateful firewall at Layer 2, without having to create Layer 3 subnets • Allow established sessions to continue uninterrupted after a mobile unit roams between an AP and a switch • Handle Layer 2 attacks, including ARP cache poisoning and ARP spoofing, DHCP rogue server attacks, DHCP starvation, broadcast storms, incomplete fragment attack checks, suspicious activity checks, several DoS attacks, etc. • Lock down the protocols a POS device can access; role based firewall allows separate firewall policies for laptops and POS equipment even if they are on the same WLAN • Block POS devices that are compromised and attempt non-standard operations
2.1.1	Changing default wireless settings	Motorola WLAN infrastructure is centrally managed and monitored to prevent default backdoors • Centrally configured and managed APs • 24x7 monitoring and alerting of misconfigured devices based on actual over the air analysis
4.1.1	Encryption in wireless networks	Motorola's WLAN infrastructure is fully compatible with IEEE 802.11i and supports • WPA-TKIP • WPA2-CCMP (AES) • WPA2 TKIP • 802.1X EAP-TLS and EAP-TTLS • Protected EAP (PEAP) • Kerberos • Integrated AAA/RADIUS Server Motorola provides legacy encryption protection solutions providing a secure and compliant upgrade path for legacy WEP networks • KeyGuard – Per packet WEP key rotation for devices that cannot be upgraded to WPA • WEP CloakingTM – WEP key protection for legacy networks without requiring hardware or software upgrades to the infrastructure • VPN capabilities on mobile devices for enc

9.1.3	Physically secure wireless devices	Motorola's wireless LAN APs and mobile clients support multiple features to mitigate risks due to physical access • APs with wall, ceiling and above-ceiling tile mounting options • Thin APs with no local sensitive data storage • Tamper resistant and tamper evident enclosures • Mobile units with encrypted passwords
10.5.4	Audit logging of wireless activity	Motorola AirDefense wireless IPS has the most detailed wireless forensic database available in the industry • Over 300 wireless statistics per device per minute logged • Ability to log wireless data for months • Instant analysis using the forensic wizard • Digitally signed and fully customizable reports
11.4	Intrusion prevention (IPS) for wireless traffic	Motorola AirDefense wireless IPS utilizes its 24x7, real-time monitoring of 802.11a/b/g networks for the most accurate intrusion detection of known and unknown attacks. • 200+ attacks and policy violations detected • Rogue device containment • Stateful monitoring of all WLAN activity based on attack signatures, protocol analysis, statistical anomaly and policy violations • Reconnaissance detection (e.g. NetStumbler, Wellenreiter, etc.) • Identity theft detection • Multiple forms of Denial-of-Service (DoS) attacks detected • Session hijacking or Man-in-the-Middle (MITM) attack detection • EAP attacks • Anomalous behavior alarms • Wireless termination of unauthorized connections • Wired side port suppression and access control lists
12.3	Usage policies and procedures for wireless	Motorola AirDefense Wireless IPS can be used to define and enforce wireless policies • Encryption and Authentication policies • Approved data rates, operating channels, traffic thresholds and usage times • WLAN device and roaming policies • Vendor policies • Ability to automatically notify policy violations • Ability to terminate wireless connections based on policies Motorola wireless switches support Network Access Control (NAC) • User and client authorization check for resources without a NAC agent. • Blocking or quarantining non-compliant devices from connecting to a WLAN • 802.1x based pre-admission control

Conclusions

Retail's wireless vulnerabilities have been recently exploited by hackers seeking lucrative data such as credit card numbers and customer personal information. Recent high profile data breaches have highlighted the need for wireless monitoring and intrusion prevention. The cost of a data breach is substantial - from immediate fines and business disruption to long term brand damage and legal liabilities. The Payment Card Industry has enforced new Data Security Standards with stricter wireless controls and audit procedures. Motorola offers out-of-the-box PCI compliant WLAN infrastructure solutions. In addition, Motorola's AirDefense Wireless IPS solution can lock down the retail airspace and provide the best wireless security available in the industry while facilitating cost-effective PCI compliance from a wireless perspective.

MOTOROLA

motorola.com