Motorola AirDefense Retail Solutions

Wireless Security Solutions For Retail

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.

The PCI Security Standards Council released an updated version of their Data Security Standard (DSS) that went into effect on October 1st, 2008. PCI DSS version 1.2 is the global standard adopted by the card brands for all organizations that process, store or transmit cardholder data.

Wireless Risks in Retail

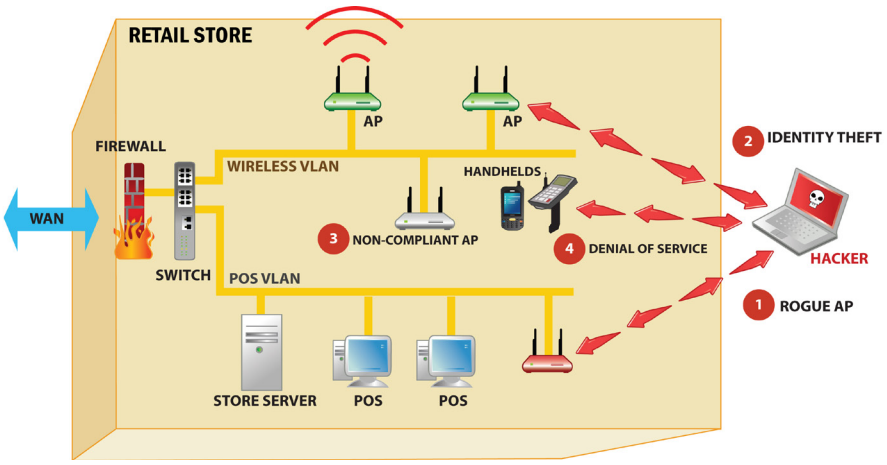
The introduction of wireless technologies in retail has created a new avenue for data breaches, circumventing traditional security architectures. Several recently publicized data breaches in the retail industry have exploited wireless vulnerabilities. Attackers have been able to access sensitive information such as credit/debit cards that have resulted in brand damage, financial/regulatory liabilities and disruption of business for retailers. Wireless introduces the following vulnerabilities that traditional security solutions cannot mitigate.

Rogue Wireless Devices

A rogue wireless Access Point (AP) is an unauthorized AP physically connected to the wired retail network. Rogue APs provide attackers with unrestricted access, bypassing firewalls and VPNs, to internal servers just as if they were connected to an internal wired port. Rogue APs can be installed on any network, including networks with no official wireless deployments and Point of Sale (POS) networks that have been segmented from regular wireless networks.

Identity Thefts

A hacker can masquerade as an authorized wireless device and connect to an authorized AP. MAC address based Access Control Lists (ACL) are useless since wireless MAC addresses are broadcast and hackers can easily change the MAC address of their device. WEP encryption can be cracked in a few minutes. WPA Pre- Shared Key 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 preshared key. Once the key is stolen, the entire network is vulnerable until administrators manually change the key at every AP and every portable data terminal.



In July 2009, the PCI Security Standards Council released the PCI DSS Wireless Guideline, as a supplement to DSS 1.2, to help organizations understand how PCI DSS applies to wireless environments, how to limit the PCI DSS scope as it pertains to wireless, and practical methods and concepts for deployment of secure wireless in payment card transaction environments.

Non-Compliant APs

Wireless APs are frequently misconfigured. According to Gartner, a majority of all wireless security incidents will happen as a result of misconfigured devices. Misconfigurations happen for a variety of reasons including human error and bugs in wireless 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 allowing them to attack internal servers and applications.

Denial of Service Attacks

Hackers can easily perform wireless denial of service (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 like WPA2. Hackers can insert malicious multicast or broadcast frames via wireless APs that can wreak havoc on the internal wired infrastructure of retail network.

PCI Wireless Requirements

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.

The Payment Card Industry (PCI) is now mandating stricter wireless security measures and the cost of non-compliance is significant.

PCI DSS version 1.2 places special emphasis on WLAN security. It requires all organizations with Cardholder Data Environments (CDE) to change wireless defaults (passwords, SSIDs, keys, etc.), use strong encryption, eliminate rogue/unauthorized wireless devices, restrict physical access to wireless devices, log wireless activity, and define wireless usage policies. Recently, the PCI Security Standards Council officially released the PCI Wireless Guidelines Document to help organizations understand how PCI DSS applies to wireless environments, how to limit the PCI DSS scope as it pertains to wireless, and practical methods and concepts for deployment of secure wireless in payment card transaction environments. Both of these documents consists of steps that mirror security best practices.

Here are the top 5 steps retailers can take to secure wireless.

1. Monitor the retail airspace 24x7 to eliminate rogue devices and block unauthorized wireless access. PCI compliance requires quarterly scanning for rogue devices at the very least. Using laptop based sniffers at each location quickly becomes an expensive and untenable solution for large retailers and can leave networks vulnerable for months.
2. Install a stateful wireless firewall between wireless networks and the card holder environment to restrict wireless traffic.
3. Prevent wireless attacks and intrusions by using a specialized Wireless Intrusion Prevention System (WIPS) that can detect and prevent identity theft and denial of service attacks.
4. Maintain detail forensic records of wireless activity for all stores, distribution centers

and headquarters with the ability to generate compliance reports and provide an auditable trail of wireless events.
5. Upgrade to WPA based wireless security.

The Motorola AirDefense Solution

Wireless Intrusion Prevention Systems (WIPS) thwart wireless attacks and provide the most cost effective solution to meet PCI wireless security requirements. The Motorola AirDefense Enterprise wireless security solution is based on patented technology that incorporates distributed smart IEEE 802.11a/b/g/n sensors reporting to a central server appliance. The remote sensors are deployed in stores, distributions centers and the retail headquarters. Sensors are vendor agnostic 24x7 WLAN radios available as standalone units or can be embedded in Motorola APs to reduce deployment costs. They monitor all WLAN activities 24x7 in the local airspace and communicate with the Motorola 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 their computer. The Motorola AirDefense solution addresses three key areas for retailers:

Comprehensive Wireless Security

Motorola AirDefense Enterprise provides the industry leading solution for rogue wireless detection and containment and 24x7 wireless intrusion prevention. Motorola AirDefense Enterprise can accurately distinguish neighboring devices from rogue devices that are connected to the retail network and can be setup to automatically terminate a rogue device over the air. Alternatively, the device can be blocked on the wired side using the Motorola AirDefense switch port suppression feature.

To find the location of the rogue device, Motorola AirDefense provides accurate map based location tracking using signal strength triangulation.

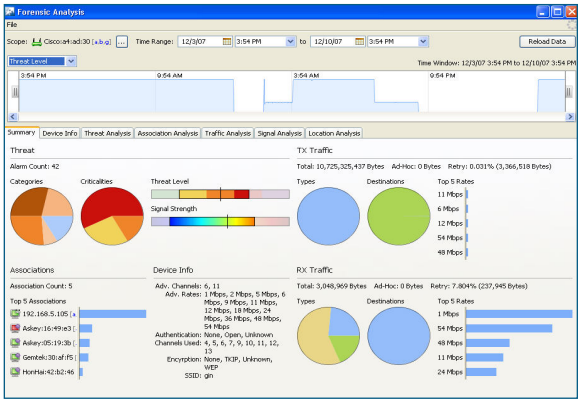
Motorola AirDefense Enterprise has the largest wireless attack library with over 200 alarms that can detect a range of attacks such as reconnaissance activity, identity theft, session hijacking or Man-in-the-Middle (MITM) attacks, multiple DoS attacks, wired side leakage, dictionary based attacks, etc. Motorola AirDefense reduces false positives by correlating wireless and wired side information in conjunction with rich historical context maintained in its forensic database instead of just looking at the present snapshot. Motorola AirDefense recognizes documented and undocumented (day-zero) attacks, because it does not rely solely on attack signatures but also on advanced anomalous behavior analysis. Once an accurate assessment of an intrusion is made, Motorola AirDefense Enterprise provides wireless and wired termination capabilities to mitigate the threat in real-time.

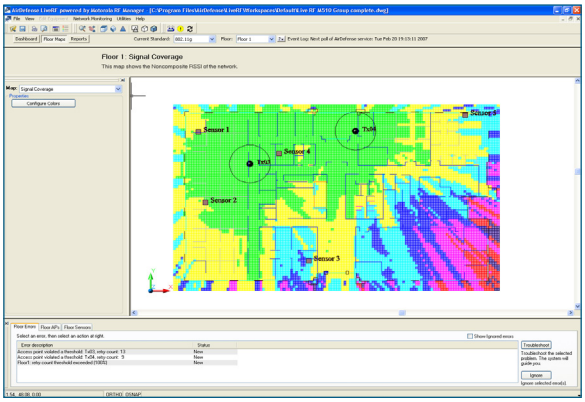
Motorola wireless APs and switches include a built-in layer 2-7 wireless firewall, capable of blocking several attacks (e.g. DHCP spoofing or ARP cache poisoning) that cannot be detected by traditional layer 3 firewalls, right at the edge of the WLAN. The Motorola wireless firewall contains sophisticated, distributed, stateful packet inspection technology, protecting users as they roam across the enterprise, while avoiding performance bottlenecks that arise when all traffic is funneled to a central choke point for inspection. The Motorola wireless firewall can effectively segregate WLAN traffic from the card holder environment and integrates with leading enterprise authentication systems, including LDAP and Active Directory, and can leverage a built-in location tracking engine to enforce user identity, role and location based security policies.

PCI Wireless Compliance

Motorola AirDefense Enterprise provides the most cost-effective mechanism to comply with PCI DSS wireless requirements. Complying with the PCI wireless requirements is tedious and expensive for most retailers. PCI DSS Section 11.1 requires that retailers use a wireless analyzer at least every quarter to identify all wireless devices in use. Note that this is required regardless of WLAN deployment status, the intent being to neutralize rogue wireless devices that can show up even if WLANs have not been deployed.

Scanning a few stores and assuming that the rest are similar is not sufficient. The PCI Wireless Guideline clearly specifies that wireless scanning has to be done for all locations, regardless of wireless deployment status and that the scan results should clearly classify authorized, neighboring and rogue wireless devices at each location. Further, relying on wired-side scanning alone will not meet the requirement since wireless devices not actively connected to the wired infrastructure or on isolated network segments may not show up on a wired-side scan. Motorola AirDefense Enterprise sensors perform wireless scans 24x7 above and beyond the quarterly PCI requirement. Every device is centrally logged in the server's forensic database and PCI compliance reports can be scheduled and automatically generated by the system. Motorola AirDefense Enterprise updates and maintains around 300 different statistics for every wireless device, every minute, and is capable of storing this data for months. The forensic data is mined to produce detailed PCI compliance reports.





Remote Wireless Network Assurance

The Motorola AirDefense solution offers a unique set of tools for vendor agnostic, remote WLAN performance management. Motorola AirDefense can significantly reduce the management cost of store and distribution center wireless networks by providing powerful tools for optimizing network performance and remote troubleshooting. Motorola analyzes traffic flow to interpret WLAN performance and identify usage characteristics, interference from neighboring WLANs, channel overlap, and performance degradation. The innovative add-on modules integrated into the Motorola performance management and troubleshooting suite include Motorola AirDefense Advance Troubleshooting, Motorola AirDefense Spectrum Analysis, Motorola AirDefense LiveRF, and Motorola AirDefense Advanced Forensics. These tools provide a real-time view of all WLAN traffic, enabling network administrators to remotely troubleshoot problems, identify and respond to network mis-configurations, and monitor the networks availability. The net result is a system that provides retailers the ability to maximize the availability of their WLAN while simultaneously reducing operational expenses.

About Motorola AirDefense

Motorola offers a comprehensive portfolio of wireless LAN (WLAN) infrastructure solutions designed to enable the truly wireless enterprise, regardless of the size of your business — from large enterprises with locations all over the world to branch offices and small businesses. As the market leader and innovator of 24x7 monitoring solutions, Motorola AirDefense provides a complete suite of wireless security and operation support solutions to enable risk-free wireless LANs. Motorola AirDefense provides the most advanced solutions for vendor agnostic rogue wireless detection, network performance management, remote troubleshooting, policy enforcement and intrusion prevention. Only Motorola delivers wireless agility inside the enterprise, between locations and out to end-user devices. With time-proven resiliency, security and performance equal to or greater than that of a wired network, Motorola's solutions substantially reduce network deployment and maintenance costs, and ensure the availability of cost-effective wireless connectivity in every corner of the enterprise.

Motorola AirDefense Solutions belong to the broader One Point Wireless Suite, a set of powerful and innovative software solutions that reflect Motorola's holistic approach to network design, management, security and network assurance. Motorola delivers both an unrivaled indoor/outdoor wireless portfolio and the software tools you need to build and operate a trusted high-performance wireless network.

For more information on Motorola AirDefense Solutions, please visit us on the web at motorola.com/airdefensesolutions.


Quick Sale
Cash Count
Inventory
Work Order
End of Day
Configuration
Work In Progress
End of Week
Data Manager
Pick Up
Hours Worked
Reports
Refund
Punch In/Out

MOTOROLA

motorola.com