WHITE PAPER

SECURE MOBILITY SOLUTIONS FOR RETAIL TRANSACTIONS

PCI DSS 3.1 COMPLIANCE

aruba
a Hewlett Packard Enterprise company

TABLE OF CONTENTS

CYBERATTACKS AND RETAIL

As threats rise, retailers are rapidly transforming their networks to bring new efficiencies to inventory management and move to mobile point-of-sale systems.

At the same time, in-store mobile marketing and engagement strategies are helping retailers personalize shopping where digital signage helps bring up-to-the-minute promotions and relevant content to customers.

Retailers are also expanding their use of analytics to collect increasing amounts of data about shoppers and their habits. Information about time spent in a store, what products shoppers view and purchase and a variety of other pertinent data can now be collected by wireless networks and delivered to retailers.

Location-aware mobile apps and push-notifications are transforming the shopping experience, and delivering context-relevant information over the air based a user's location and personal communication preferences.

Many of these new requirements provide significant competitive advantages but inadvertently increase the complexity of retail networks. Merchants want to take advantage of the productivity and efficiency benefits of mobility, but above all else, they need to protect their networks and their customers' sensitive credit and debit card data in order to meet compliance demands and safeguard their brand.

PCI DSS: A PRIMER

The Payment Card Industry (PCI) Data Security Standard (DSS) debuted in December of 2004. It was largely heralded as a key milestone in the history of information security and compliance. PCI DSS is designed to encourage and enhance cardholder data security and facilitate the adoption of consistent data security measures around the world.

PCI DSS is one of a series of security standards from the PCI Security Standards Council that apply to manufacturers of payment devices, applications, infrastructure and users. The PCI Council was formed by the major payment card brands, including American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc.

PCI DSS applies to all system components included in or connected to the cardholder data environment (CDE), and includes special guidance for organizations that want to utilize Wi-Fi technology. It affects all entities in the payment card process, including merchants, processors, acquirers, issuers and service providers, as well as all other entities that store, process or transmit cardholder data and other sensitive authentication data.

WHO IS IMPACTED BY PCI DSS?

While PCI DSS is widely applicable to retail, it can also impact healthcare, service providers, education, hospitality and financial services organizations as well as any company that processes credit and debit card transactions.

The PCI DSS standard applies wherever account data – both cardholder and authentication data – is stored, processed or transmitted. The PCI Council refers to this as the cardholder data environment or CDE.

Cardholder data includes the primary account number (PAN), cardholder name, expiration date and service code. Sensitive account data includes full magnetic stripe data or equivalent on a chip, the card validation value and the PIN.

PCI DSS VERSION 3.1

PCI DSS provides a minimum set of requirements for protecting cardholder data and is designed to be enhanced over time to adapt security mechanisms to the evolving threat landscape.

Version 3.1 was issued in April 2015 and the changes introduced are designed to help organizations take a proactive approach to protecting cardholder data, focusing more on security than strictly compliance.

PCI DSS 3.1 places greater emphasis on education and awareness of the intent of requirements, increased flexibility on ways to meet the requirements, and helps organizations understand their responsibilities when working with different business partners to ensure cardholder data security.

The intent with the 3.1 update is to provide clarification to many of the requirements that have been viewed as somewhat ambiguous and to expressly forbid the use of weak Secure Sockets Layer (SSL) and Transport Layer Security (TLS) encryption protocols for securing cardholder data. Figure 1 shows the 12 requirements of PCI DSS which serves as the baseline of technical and operational requirements to protect cardholder data.

Goal	PCI DSS requirement
Build and maintain a secure network and systems	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.
Protect cardholder data	3. Protect stored cardholder data. 4. Encrypt transmission of cardholder data across open, public networks.
Maintain a vulnerability management program	5. Protect all systems against malware and regularly update anti-virus software or programs. 6. Develop and maintain secure systems and applications.
Implement strong access control measures	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.
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 for all personnel.

Figure 1: The 12 requirements of PCI DSS.

THE IMPORTANCE OF PCI DSS COMPLIANCE

Complying with the PCI DSS standard is mandatory for any organization that stores, processes or transmits credit card data. However, despite the increasing maturity of the standard and many organizations' understanding of the requirements, compliance remains a difficult task.

While significant progress is being made, there are several compelling reasons for any organization to fully comply with PCI DSS, including:

- **Protecting the merchant's brand** – A security breach negatively impacts a merchant's image and affects customer loyalty. Consumers expect merchants to adequately protect their private information and will actively avoid those perceived to have lax security standards.

  Research has shown that 12% of loyal customers who have been victims of identity fraud stop doing business with that merchant where the fraud occurred, and 36% will shop there less frequently.[1] Data breaches also have ripple effects that extend beyond customer revenue to affecting consumer trust and stock value.

- **Mitigate risks of security breaches** – While no security standards or technologies can completely eliminate all risks, merchants that implement security controls as part of PCI DSS compliance improve their chances of both avoiding a breach in the first place and of minimizing damage of a breach.

- **Fines for out-of-compliance merchants** – Card brands are enforcing PCI compliance more aggressively and retailers, payment terminal providers and payment processors can be subject to fines if they are out of compliance with PCI DSS.

  For example, Visa may levy fines of up to $500,000 per incident for any merchant or service provider that is compromised and not compliant at the time of the incident.

  If a Visa member does not notify the company's fraud control group of a suspected or confirmed loss or theft of any Visa transaction information, the member is subject to a $100,000 fine per incident. Similarly, MasterCard has been stepping up its enforcement practices as well.

- **Safe harbor for PCI-compliant merchants in the event of a breach** – If a merchant experiences loss of cardholder data due to a security breach but is compliant with PCI DSS at the time of the breach, the merchant is exempt from the charges relating to credit and debit card replacements.

  Replacement charges of $80-$320 per credit or debit card number lost can be levied upon non-compliant merchants.

- **Access to lower interchange per transaction rates for PCI-compliant merchants** – Merchants who demonstrate compliance with PCI DSS can qualify for lower tiers of per-transaction card brand fees.

[1] "Retail's Reality: Shopping Behavior After Security Breaches" Interactions Consumer Experience Marketing, July 2014 (http://www.interactionsmarketing.com/retailperceptions/2014/06/retails-reality-shopping-behavior-after-security-breaches/)

GUIDELINES FOR MAINTAINING COMPLIANCE

Merchants may need to engage with independent scan vendors or auditors to validate compliance. As a rule of thumb, the more transactions a merchant makes, the more involved the certification process will be. Any merchant that suffers a breach resulting in data theft may be escalated to a higher validation level. Figure 2 outlines the requirements for Visa and MasterCard.

SPECIFIC REQUIREMENTS FOR WIRELESS LANS

While the cardholder associations require different levels of compliance based on transaction volumes or past non-compliance, using wireless LANs (WLANs) has its own set of requirements. The WLAN-specific requirements of PCI DSS are organized into three categories:

- Category 1 – Merchants who do not use WLAN technology.
- Category 2 – Merchants who use WLAN technology that is not connected to the cardholder environment and not used for storing, transmitting or processing cardholder data.

Merchant level	Selection criteria	Visa validation actions	MasterCard validation actions	Validated by
1	Any merchant, regardless of acceptance channel, processing more than 6,000,000 credit/debit transactions per year. Any merchant that has suffered a hack or an attack that resulted in an account data compromise. Any merchant identified as Level 1 by any card association.	Annual onsite security audit Quarterly network scan	Annual onsite security audit Quarterly network scan	Independent security assessor or internal audit if signed by an officer of the company. Qualified independent scan vendor
2	1 million – 6 million credit/ debit transactions per year.	Annual PCI self-assessment questionnaire Quarterly network scan	Annual PCI self-assessment questionnaire Quarterly network scan At merchant discretion: Annual onsite assessment	Merchant Qualified independent scan vendor
3	20,000 – 1 million credit, debit or e-commerce transactions per year.	Annual PCI self-assessment questionnaire Quarterly network scan	Annual PCI self-assessment questionnaire Quarterly network scan	Merchant Qualified independent scan vendor
4	Less than 20,000 credit, debit or e-commerce transactions per year, and all other merchants processing up to 1 million transactions per year.	Annual PCI self-assessment questionnaire Quarterly network scan	Annual PCI self-assessment questionnaire Quarterly network scan	Merchant Qualified independent scan vendor Validation requirements and dates for Level 4 merchants are determined by the merchants' acquirer. Submission of scan reports and/or questionnaires by Level 4 merchants may be required.

Figure 2: Visa and MasterCard PCI-compliance levels.

- Category 3 – Merchants who use WLAN technology connected to the cardholder environment and store, transmit or process cardholder data over WLAN technology.

Figure 3 summarizes each category and outlines their requirements.

Category 1: No WLAN		**Category 2: WLAN not connected to cardholder environment**		**Category 3: WLAN connected to cardholder environment**	
11.1	Test for the presence of wireless access points (APs). • 11.1.2 Implement incident response procedures when unauthorized APs are detected.	1.1.2	Network diagram that identifies all connections between cardholder data and WLAN.	1.1.2	Network diagram that identifies all connections between cardholder data and WLAN.
		1.2.3	Install firewall between cardholder data and WLAN.	1.2.3	Install firewall between cardholder data and WLAN.
		9.1.3	Restrict physical access to WLAN and other network hardware and telecommunication lines in cardholder environment.	2.1	Always change vendor-supplied defaults and all unnecessary accounts before installing a system on the network. • 2.1.1 Change all wireless vendor defaults at installation.
				2.2	System configuration standards that include changing all vendor-supplied defaults and unnecessary default accounts.
		11.1	Test for the presence of wireless APs • 11.1.1 Inventory all authorized APs. • 11.1.2 Implement incident response procedures when unauthorized APs are detected.	4.1	Use strong cryptography and security protocols during transmission of cardholder data over open, public networks. • 4.1.1 Ensure wireless networks use best practices to implement strong encryption. The use of WEP is prohibited.
				6.1	Establish a process to identify and rank security vulnerabilities.
				6.2	Install all applicable vendor supplied patches.
				7.1	Limit access to system components and cardholder data to only those whose job requires access.
				7.2	Establish an access control system for system components that restricts access based on user's need to know.
				9.1.3	Restrict physical access to WLAN and other network hardware and telecommunication lines in cardholder environment.

Category 1: No WLAN		Category 2: WLAN not connected to cardholder environment		Category 3: WLAN connected to cardholder environment	
				10.1	Audit trails should be implemented to link access to system components to each individual user.
				10.3	Record the detailed audit trail entries.
				11.1	Test for the presence of wireless APs. • 11.1.1 Inventory of all authorized APs. • 11.1.2 Implement incident response procedures when unauthorized APs are detected.
				11.4	Use intrusion detection and/or prevention (IDS/IPS) systems to monitor all traffic at the perimeter or CDE. Keep all IDS/IPS signatures up to date.
				12.3	Develop usage policies for critical technologies and define proper use of these technologies.

Figure 3: PCI 3.1 requirements pertaining to WLANs.

Category 1

Merchants that do not use WLANs must still monitor for the presence of rogue wireless APs. Due to the ease by which wireless APs can be attached accidentally or intentionally, the difficulty in detecting them, and the increased risks associated with unauthorized wireless devices on retail networks, controls must be in place to protect any retail network from attacks via rogue or unknown wireless APs and clients.

Merchants can utilize physical inspections, wireless scans, network access control or wireless intrusion detection and prevention systems (WIDS/WIPS) to test for the presence of wireless APs and detect unauthorized wireless devices.

Category 2

Merchants that use WLANs outside of the scope of their CDE must meet all of the Category 2 requirements. Category 2 is inclusive of Category 1 requirements plus it includes additional guidance for maintaining inventory of the WLAN, using a firewall to segment the WLAN from a wired network and appropriate physical security measures.

Category 3

Any merchant that uses WLAN technology to transmit cardholder data is required to meet the most stringent requirements. Category 3 is inclusive of Category 1 and 2 requirements as well as additional requirements such as not using default passwords and configurations, using strong encryption and authentication, regular patching of systems, role-based access controls and monitoring of all access.

ARUBA MOBILITY SOLUTIONS FOR RETAIL

Retailers that deploy Aruba enterprise-grade mobility solutions benefit from the value of a purpose-built access infrastructure that enhances customer engagement, increases employee productivity and improves security.

Mobility breaks traditional security models that remain focused on fortifying the network perimeter or protecting fixed endpoints. Security controls must now adapt to the dynamic nature of mobile devices and threats originating from anywhere. Aruba makes it easy to adopt identity-based networking and adaptive trust controls in retail environments.

The Aruba mobility architecture significantly reduces the complexities of meeting regulatory requirements without sacrificing employee productivity or affecting the in-store shopping experience. This approach delivers strong, comprehensive security tailored for the demands of today's wireless merchants, employees and customers.

Aruba provides multiple levels of protection to allow merchants to meet and even exceed PCI requirements. Strong authentication and authorization, WIPs, role-based access controls and advanced encryption ensure adherence to the stringent mandates of PCI DSS, even in the most challenging environments.

Retailers benefit from the productivity and enhanced customer engagement that mobility provides, while confidently adhering to corporate and industry security mandates.

Integrated features such as a stateful firewall, rogue detection and containment capabilities along with VPN services provide secure and consistent access for employees and customers alike – no matter where they connect, how they connect or which device they use.

Aruba unifies wired, wireless and remote networking into a single, centralized architecture that captures and correlates real-time contextual data about users, devices, apps and their locations. This intelligence automatically triggers security actions, assures peak network performance, and even engages users based on their location.

Aruba's comprehensive device profiling technology automatically identifies and classifies a wide variety of wired and wireless devices, such as barcode scanners, smartphones, tablets, mobile point-of-sale (PoS) terminals, laptops, printers, IP cameras and more.

Policy decisions can now leverage accurate contextual data including device attributes, allowing retailers to granularly define and enforce security controls that adhere to their business needs without compromising compliance.

Merchants can leverage Aruba to provide secure, end-to-end mobility in stores, distribution centers and corporate headquarters. Retailers can therefore craft specific policies for network access and quality of service (QoS) for individual applications as well as a variety of mobile devices across their entire distributed network.

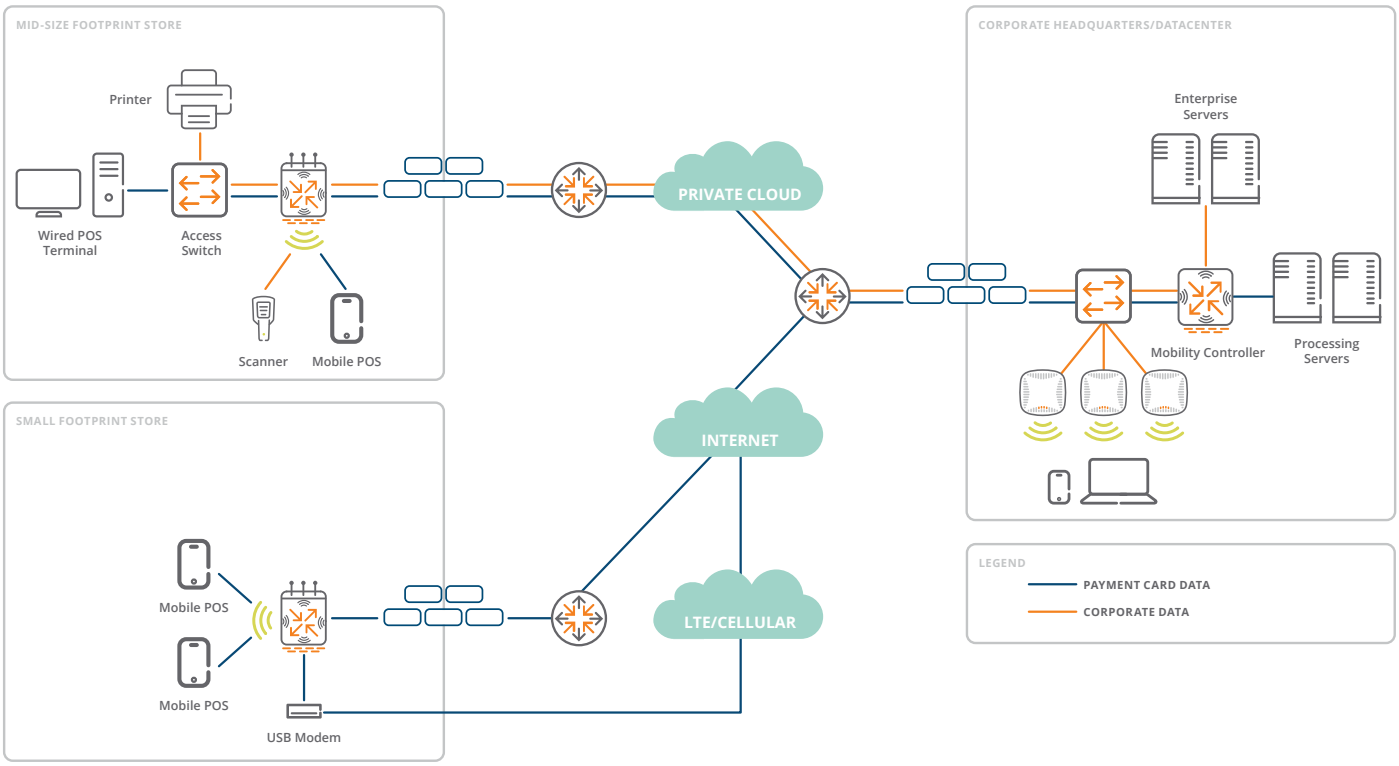

Figure 4: Aruba mobility solutions for retail networks.

What's more, Aruba simplifies the challenge of utilizing new mobile technology on in-store networks. Many retailers are embracing mobile technology for marketing and engagement opportunities with their customers. Aruba wireless infrastructure automatically detects new mobile devices such as smartphones or tablets and automates the configuration and provisioning process – without requiring IT support.

The Aruba mobility solution is designed for operational efficiency in any retail environment. Mobility services can be delivered centrally from a data center across thin access networking devices or served locally across any distributed infrastructure.

Aruba provides a comprehensive portfolio of access products, including; controller-based and controllerless 802.11n and 802.11ac indoor and outdoor access points, Mobility Access Switches, Mobility Controllers, Cloud Services Controllers and the Virtual Intranet Access (VIA) agent for secure remote connectivity.

The ClearPass Access Management System provides secure policy-based network access tailored for the needs of today's retail networks. It features ultra-scalable AAA with RADIUS and TACACS+ combined with a policy engine that leverages contextual data like user roles, device types, app usage and location.

ClearPass Onboard automatically configures and provisions mobile devices – Windows, Mac OS X, iOS, Chromebook and Android – enabling employees to securely connect these devices to retail networks in support of mobility and enhanced customer engagement initiatives.

ClearPass dynamically detects a device's operating system and the ClearPass Onboard portal guides users through appropriate configuration settings. This means that employees, contractors and partners can now securely self-configure their own devices without IT involvement.

ClearPass Guest is a scalable, easy-to-use visitor management solution that delivers secure automated guest access workflows for visitors, contractors, partners, shoppers and fans on wireless and wired networks.

Furthermore, self-registration and sponsor-involved options ensure credentials and pre-authorized access privileges are enforced for short-term and long-term guests, without putting a heavy burden on IT.

Finally, whether looking for a subscription model or a complete on premise solution, Aruba makes managing the mobile infrastructure painless. The freedom to choose management platforms means PCI compliance is handled on your terms and within your budget.

Aruba Central, a convenient software-as-a-service (SaaS) subscription in the cloud, gives IT organizations a simple, secure and cost-effective way to manage one or thousands of controllerless Aruba wireless APs and the wired infrastructure.

It's the fastest and easiest way to centrally manage any retail mobile network and comes with all the enterprise-grade features needed, including automatic maintenance and firmware management as well as PCI-compliance reporting and full technical support.

Aruba AirWave is the only network operations system that centrally manages multivendor wired and wireless networks across any number of locations.

Available as software or a complete turnkey hardware package, AirWave lets operations staff diagnose end-to-end connectivity and application performance issues and provides automated configuration management for tens of thousands of devices – all from a single console.

AirWave provides complete RF visibility, proactive troubleshooting, and historical reporting to let IT effectively mitigate threats. Historical data allows for detailed PCI compliance reporting.

MEETING PCI COMPLIANCE WITH ARUBA

Aruba helps merchants meet the requirements for PCI regardless of which category of WLAN usage model they deploy – no WLAN, no cardholder data over the WLAN, or transmitting cardholder data over the WLAN (see Figure 5).

What's more, with Aruba, merchants can easily migrate to a higher category of protection as their use of Wi-Fi expands while protecting their infrastructure investments further.

Category 1: No WLAN	Category 2: No cardholder data over WLAN	Category 3: Cardholder data over WLAN
• Aruba APs as air monitors to wirelessly scan for rogues. • Advanced policy management and access controls with Aruba ClearPass and Mobility Access Switch line. • Wireless intrusion detection and prevention. • Aruba Central or AirWave for compliance reporting.	• Aruba APs in hybrid mode – servicing clients and scanning for rogues. • Build-in firewall segments WLAN. • Role-based networking with strong authentication and encryption. • Aruba Central or AirWave for compliance reporting.	• Aruba APs in hybrid mode – servicing clients and scanning for rogues. • Dedicated air monitors for scanning only. • Built-in firewall segments WLAN • Role-based networking with strong authentication and encryption. • AirWave for compliance reporting and wireless and wired rogue detection, correlation and protection or Aruba Central for compliance reporting.

Figure 5: Aligning Aruba solutions to WLAN categories for PCI compliance.

Satisfying Category 1 requirements: No WLAN

Even if a merchant is not using any WLAN technology, they are still required to monitor for the presence of unauthorized wireless APs.

Merchants can meet this requirement by installing Aruba APs as dedicated air monitors to detect and contain rogue APs and clients as well as provide WIDS and WIPS capabilities. Aruba Central and AirWave can be used to aggregate wireless intrusion protection data and provide compliance reporting.

For added security, Aruba ClearPass and Mobility Access Switches can provide advanced network access policy management and enforcement while Aruba Central and AirWave provide compliance reporting. Aruba AirWave can also be used to consolidate rogue information across wired and wireless networks, log rogue scans and activity and provide detailed reporting.

Wireless scanning and rogue containment

Aruba APs can be configured to function in a variety of modes; controllerless Instant APs, controller-managed, air monitor or hybrid. As a dedicated air monitor, Aruba APs periodically scan the air for unsanctioned wireless devices.

Air monitors also identify and record other wireless devices in the area, including Wi-Fi clients, APs and bridges and provide detailed reporting and even a full packet captures.

When a rogue device is detected, Aruba can provide containment using wireless de-authentication or tarpitting. Wireless deauthentication messages indicate an air monitor is attempting to disconnect a client from a rogue AP.

Here, the air monitor impersonates the MAC address of the rogue AP and client associated to the rogue AP in order to disrupt both the AP and clients ability to connect. While this method is effective it can also be disruptive to nearby stations.

Tarpitting is similar to wireless deauthentication but adds the ability to lure clients attempting to associate to a rogue AP by using false channels, BSSIDs or both. In doing so, the client associates to the air monitor but all client traffic is ignored and any attempts to re-associate to the rogue AP are intercepted by the air monitor, thus containing both rogue AP and client.

Tarpit containment is very efficient and allows each air monitor near the client to participate without spending much time on any given channel.

Advanced policy management and access controls

To prevent unauthorized access ClearPass can be used to control which users and devices can reach cardholder data. Granular network access privileges are granted based on a user's role, device type, EMM/MDM attributes, device health, location and time-of-day.

Centrally-defined policies and enforcement eliminates the need for multiple AAA and policy management systems, which strengthens the overall security architecture.

ClearPass Policy Manager supports user and device authentication based on 802.1X, non-802.1X and web portal access methods. Multiple authentication protocols like PEAP, EAP-FAST, EAP-TLS, EAP-TTLS, EAP-PWD, and EAP-PEAP-Public can be used to strengthen security in any retail environment.

Built-in device profiling automatically discovers and classifies all endpoints, regardless of device type and contextual information about devices. MAC OUIs, DHCP fingerprinting and more – can be used within policies to granularly define device specific access privileges.

Posture assessments and remediation can be added to any enforcement policy – even for devices not owned by the retailer – to ensure they meet full compliance before they are allowed onto the network.

When combined with Aruba Mobility Access Switches, role-based access controls are easily extended to wired connections. Additionally, Aruba Mobility Switches can correlate potential wireless rogues with data from the wired network and mitigate potential threats.

If a threat is identified, Aruba Mobility Access Switches can shut off the affected port, or contain the device through de-authentication or delaying network connections via tarpitting. Shutting off access to rogue APs reduces risk while helping IT proactively manage security and compliance.

Traditional enforcement methods using RADIUS, RADIUS CoA and SMP are utilized for non-Aruba wired infrastructure.

Wireless IDS/IPS

Integrated into every controllerless Instant and controller managed Aruba AP, wireless intrusion detection and protection offers threat protection and mitigation while eliminating the need for separate RF sensors and security appliances.

The integrated wireless intrusion detection and protection system automatically monitors the network for the presence of rogue APs and clients, logs and reports on rogue APs and clients, and can even contain wired and wireless devices detected.

Aruba AirWave or Aruba Central network management are used to provide detailed event history and security reports to meet compliance requirements. Reports can be automatically generated and emailed to the appropriate IT staff or exported in a variety of formats.

For enhanced protection, Aruba RFProtect prevents denial-of-service (DoS) and man-in-the-middle attacks and mitigates over-the-air security threats. Available as a software license on Aruba Mobility Controllers, RFProtect provides a patented containment method for rogue APs as well as advanced intrusion protection capabilities for Wi-Fi infrastructure and clients.

Combining advanced wireless intrusion protection capabilities with full spectrum visibility, RFProtect safeguards the wireless network infrastructure against security threats and provides a critical layer of visibility into sources of radio frequency (RF) interference and its effect on WLAN performance. Network dashboards and configuration wizards make it easy to deploy and helps to simplify the challenges of managing WLAN security.

RFProtect security events and data can be further leveraged by Aruba AirWave to augment event history with correlation and location tracking information. Additionally, AirWave RAPIDS can aggregate and correlate scanning data from multiple sources to further reduce false positives for more accurate threat assessment.

With RAPIDS, IT security administrators can easily classify threats according to their specific security policies, thus allowing them to focus on the most important threats.

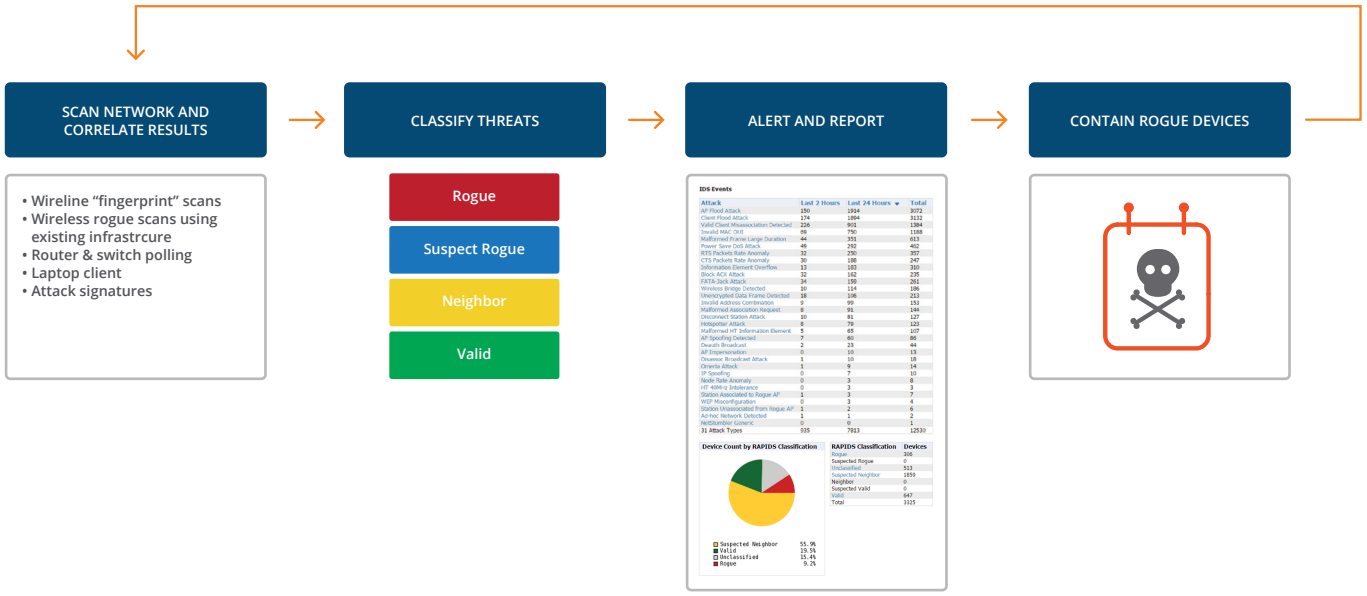

Figure 6: Aruba AirWave RAPIDS advanced intrusion and rogue protection.

Satisfying Category 2 requirements: No cardholder data on WLAN

Retailers that have wireless networks but do not process or transmit cardholder data over a WLAN must meet Category 2 requirements for WLAN usage. To meet these requirements, merchants can use Aruba hybrid APs which provide Wi-Fi access to users as well as periodically scan the air for rogue APs and clients or other Wi-Fi security issues surrounding WIDS and WIPS.

For added security, Aruba integrates the stateful Policy Enforcement Firewall (PEF) into the WLAN infrastructure to effectively segment wireless network traffic from the cardholder data environment. What's more, with Aruba retailers have the ability to inventory all WLAN components as well as enforce physical security for WLAN APs.

Aruba hybrid APs

In addition to being configured as a dedicated air monitor, Aruba APs can also be configured for scanning, or hybrid, mode. This configuration allows APs to service clients and periodically scan the RF spectrum for unsanctioned wireless devices and other attacks against the Wi-Fi infrastructure.

AirWave RAPIDS can augment wireless IDS/IPS services for Aruba hybrid APs to mitigate rogues and provide added protection from DoS attacks.

Aruba hybrid APs provide the same level of Wi-Fi infrastructure protection as dedicated air monitors but prioritize client traffic over scanning or containment. Thus, in environments where wireless containment is a requirement, Aruba recommends deploying dedicated air monitors with APs for the highest level of wireless security.

Firewall WLAN traffic from cardholder data

Stateful Aruba Policy Enforcement Firewall (PEF) effectively segments wireless traffic from any retailer cardholder data environment (CDE). PEF technology provides identity-based controls to enforce application-layer security and prioritization for all traffic across the wireless network.

With PEF, IT can enforce network access policies that specify who may access the network, with which mobile devices and which areas of the network they may access. Unauthorized users and devices that attempt to connect to the Aruba Wi-Fi network can be blocked and even denylisted.

Policies can also be generated for any device to include bandwidth limitations, time-of-day restrictions and QoS, ensuring adherence to established company device guidelines. Aruba Mobility Controllers can further extend the role of PEF to support multiple user categories on a single network, spanning wired, wireless and VPNs.

One of the common uses of the PEF in retail is to isolate traffic from barcode scanners that do not support modern encryption and authentication methods. PCI DSS 3.1 strictly prohibits the use of Wired Equivalent Privacy (WEP) due to well publicized weaknesses in the WEP algorithm.

However, many older generation barcode scanners are only capable of supporting WEP, thus placing retailers in the awkward position of replacing systems and equipment. Firewalling WEP-only scanners from the CDE keeps them out of scope of PCI DSS compliance, shielding merchants from the costs and network disruptions of migrating away from their legacy systems.

Other scenarios where firewall segmentation is desirable include; role-based policies for mobile POS devices that transmit credit and debit card data over the Wi-Fi network, price updates over Wi-Fi, inventory status lookups on mobile devices or shoppers using a store kiosk connected to the Internet.

In each of these scenarios, the Aruba PEF is able to effectively segment all traffic to prevent unauthorized individuals with access to the wireless network from connecting to the CDE and potentially compromising cardholder data.

Strong encryption for authentication and data transmission

PCI DSS requires the use of strong encryption for wireless transmission whether or not credit or debit card data is transmitted. Aruba supports multiple authentication and encryption methods and even permits multiple methods to be used simultaneously (see Figure 7).

This allows Wi-Fi Protected Access 2 (WPA2) with 802.1X authentication and Advanced Encryption Standard with Counter Mode CBC-MAC Protocol (AES-CCMP) encryption to be the preferred authentication method while also supporting pre-shared key (PSK) for less sophisticated devices like IP phones or barcode scanners.

Additionally, Aruba Mobility Controllers can be configured to support Suite B cryptography, providing government-grade security for organizations that transmit classified or highly confidential information.

For devices that do not support WPA2 or VPN, Aruba WLAN or ClearPass products can leverage captive portals that identify users and can restrict access based on time-of-day, location or type of encryption.

Captive portal authentication is encrypted by Secure Sockets Layer (SSL) and supports both guest users and their devices who provide an email address or other required information.

User and device role	Authentication	Encryption
Employee	802.1X	AES
Guests/visitors	Captive portal	SSL
Handheld devices	802.1X or PSK as supported by the device	AES if possible, TKIP or WEP (combined with restricted PEF role)

Figure 7: Authentication and Encryption combination examples

Once a user or device's role is assigned, the corresponding firewall policies are applied to all traffic to and from the device. PEF firewall policies are tightly coupled to user identity and authentication state to prevent man-in-the-middle or spoofing attacks.

For added security, retailers can use ClearPass Guest to provide wireless and wired access to shoppers, contractors, vendors or other visitors and their devices. Guests can be allowed to self-register for network access or are asked to provide the name of a sponsor before being permitted to join the network.

The sponsored model provides a useful model for permitting employees to access the Internet without connecting to store networks.

Once registered, ClearPass Guest can be programed to deliver account credentials to users in a variety of ways; printed scratch-cards, SMS text message, email or any combination thereof. Guest accounts can be set to expire automatically after a specific number of hours, days or based on the amount of data consumed.

ClearPass Guest helps retailers manage secure, identity-based access for tens of thousands of visitors on their network. Administrative access to any Aruba mobility solution is also identity-based, allowing access to administrative settings to be tailored to specific job functions.

Inventory the network

Merchants can use Aruba ClearPass and AirWave to create an inventory of the access network and all devices associated to it. ClearPass device profiling provides a complete inventory of all devices associated to the access network including MAC OUIs, DHCP fingerprinting and other identity-centric device data.

Stored profiling data is used to identify device profile changes and to dynamically modify authorization privileges. For example, if a printer appears as a Windows laptop, ClearPass Policy Manager can automatically deny access.

AirWave provides device inventory reports on every component of the wireless network, including brand, model, version, IP address, MAC address, SSID and notes on the physical location. AirWave's VisualRF feature uses information about the physical location of a wireless device and displays it on a sitemap for documentation purposes and for more effective troubleshooting.

Physical security

Retailers are required to restrict physical access to wireless APs and other networking gear, an important first line of defense against malicious or unintentional activities. Aruba indoor APs can be secured using third-party enclosures, a Kensington lock or bolted in place such that they cannot be easily moved.

Satisfying Category 3 requirements: Cardholder data on WLANs

Aruba enterprise-grade mobility solutions incorporate multiple layers of security, manageability and reporting to help retailers satisfy the PCI DSS requirements of transmitting cardholder data over Wi-Fi.

Merchants may want to augment their Wi-Fi security by deploying dedicated air monitors for additional scanning coverage. Aruba's integrated stateful PEF, along with the advanced rogue and WIPS capabilities, ensure the integrity and security of the Wi-Fi infrastructure while Aruba Central and AirWave provide detailed compliance reporting.

Additionally, Aruba ClearPass simplifies network policy definition and enforcement by controlling every aspect of user and device connectivity from a dedicated platform. Performing comprehensive authentication and enforcement also happens without changing the existing infrastructure.

Don't use vendor defaults

PCI DSS requires any merchant to change all vendor default settings for any Wi-Fi equipment connected to the CDE, including default wireless encryption keys, passwords and SNMP community strings. All Aruba mobility products prompt administrators to assign new passwords when powered on for the first time. Aruba WLANs also prompt administrators to assign SSIDs, encryption key and other parameters to ensure default settings are never used.

Aruba Central or AirWave allow retailers to centrally configure and manage their networks. To automate deployments at stores and other remote locations, default configurations are automatically updated and changed when devices sync to an Aruba conductor Controller at a corporate headquarters.

Configuration standards for system components

During a PCI audit, merchants are required to provide evidence of configuration standards used for all system components, including WLAN equipment, and explain how the standards are enforced. Aruba provides tools to help merchants meet this requirement.

Administrators can use Aruba Central or AirWave to centrally define the configuration policies for their WLAN deployments on a group-by-group basis. This allows different configuration policies to be defined for retail stores, distribution centers and corporate headquarters.

For added support, AirWave's automated custom compliance audits check the configuration of every network device against policy. A high priority alarm, or trigger, is generated if a violation is detected.

What's more, an administrator can then instruct AirWave to automatically correct any violations or to create a complete list of improperly configured devices and other settings that do not meet established policies.

Get the latest patches

Aruba has an established history of making patches available as quickly as possible to keep customer mobility equipment protected. Aruba's wireless security incidence response team automatically alerts customers of any security issues or updates.

For added convenience, the central configuration of Aruba Wi-Fi simplifies patch management. As system updates are uploaded to any Instant AP or Mobility Controller, all managed APs in the network are updated without intervention.

Retail chains with hundreds or thousands of locations can update their entire Aruba Wi-Fi network with the latest software and security patches at the same time.

Role-based access

Aruba mobility solutions allow retailers to enforce the principle of least privilege – meaning users and devices are able to access only the information and resources that are necessary for their role, function or other legitimate purpose.

To enforce this, retailers need to accurately identify users and devices, place them in distinct roles, and permit or deny access to resources and information based on these roles.

ClearPass gives retailers a single, powerful tool to manage access privileges across distributed locations that leverage contextual data about user roles, device types, locations and even time-of-day.

A wide range of network-based policies are enforced by ClearPass, including dynamic role-based access enforcement, VLAN and access control list (ACL) assignments, and bandwidth prioritization using application-aware QoS.

ClearPass is capable of leveraging multiple identity stores within one service, including Microsoft Active Directory, LDAP-compliant directories, ODBC-compliant SQL databases, token servers and internal databases.

The support of multiple identity stores enables IT to manage and enforce policies across multiple domains where autonomous departments exist or organizations have recently merged. Identity stores can also be utilized to authenticate users and authorize the use of resources.

ClearPass makes network policy definition and enforcement simple by controlling every aspect of user and device connectivity from a single platform. Performing comprehensive authentication and enforcement also happens without changing the existing infrastructure.

Aruba WLAN solutions logically segment all traffic and permit access only to the level granted by the administrator based on business needs. The stateful PEF simplifies the enforcement of role-based access controls to ensure compliance with established policies and regulatory requirements.

Monitoring access

Aruba ClearPass provides complete audit logs of any authentication request, whether successful or failed, including any contextual information gathered about the user, device, location and time-of-day. ClearPass audit logs can be exported to external syslog servers.

Aruba AirWave also provides audit logs for all administrative actions pertaining to the WLAN. AirWave stores up to 500 days of information and maintains detailed audit trails and system logs of all activities on the wireless network.

Aruba WLAN products also provide audit logs. These logs are stored locally and may be exported in real-time to external syslog servers.

Available logs include:

- Wireless associations, including time, MAC address, AP number and physical address.
- Authentication attempts, including time, user name, MAC address, IP address, AP number and physical locations.
- Network traffic, whether permitted or denied, including time, user name, MAC address, IP address, AP number and physical locations.
- All access to WLAN management interfaces, including configuration changes made to the system. Information in these logs includes: time, IP address, user name and the configuration that was changed.
- Wireless attacks and intrusion attempts, including time, MAC addresses, AP number and physical locations.

ARUBA FOR SECURE MOBILITY IN RETAIL NETWORKS

Many of the leading retailers across the globe rely on Aruba to provide in-store mobility solutions that optimize store operations, enhance in-store mobile marketing and provide mobile engagement programs while meeting the requirements of PCI DSS.

With Aruba, merchants are able to confidently provide their employees and guest consistent, secure access to network resources leveraging role-based access controls while at the same time protecting their cardholder data environment.

These retailers have mobilized and rightsized their networks by consolidating Wi-Fi and wired network access and security services so they can engage customers in compelling new ways and drive new levels of profitability.

WP_PCIDSS_102020 a00073391enw