



## PCI Compliance Application Brief

On Friday, May 4, 2007, every retailer's worst nightmare came true when the *Wall Street Journal* published a front page article describing a wireless LAN security breach resulting in the largest credit-card theft in history. The PCI Council, consisting of the top five payment brands – American Express, Visa, Mastercard, Discover and JCB – has published the Payment Card Industry Data Standard (PCI DSS) to prevent just that type of breach. PCI requires retailers worldwide to treat wireless LANs as public networks and apply strong security controls for both applications over wireless LANs and prevent unauthorized entry through the wireless LAN.

However, meeting stringent PCI compliance requirements is costly and complex. Existing wired and wireless networks have to be re-architected and refreshed to enable the necessary security. Additional security services need to be installed. Re-architecting and refreshing networks quickly becomes very expensive and daunting, especially when changes have to be made across hundreds, if not thousands of stores. Aruba's User-centric Networks provide the only integrated security, wireless LAN and remote access solution to make PCI painless and cost-effective. Aruba offers a centrally managed security solution that fits on top of existing networks precluding the need for re-designs and refreshes. As an added benefit, Aruba's platform is an application-enablement platform; the same solution used for security can be used to securely support existing wireless applications and enable new ones.

## PCI Requirements For Securing Wireless LANs

The PCI security standards council published an updated Data Security Standard (DSS) in May 2006 that is in effect as of January 1, 2007. The PCI council mandates the implementation of specific security controls that differ based on the extent to which wireless LANs are used.

As shown in the diagram, even if no wireless LANs are used, retailers must implement "wireless analyzers" to ensure no accidental or unauthorized wireless networks are in place. At the other end of the spectrum, if wireless LANs are used for point-of-sale applications such that credit card information is transmitted over the air, retailers must implement strong encryption (not WEP), use an ICSA certified firewall between wireless LANs

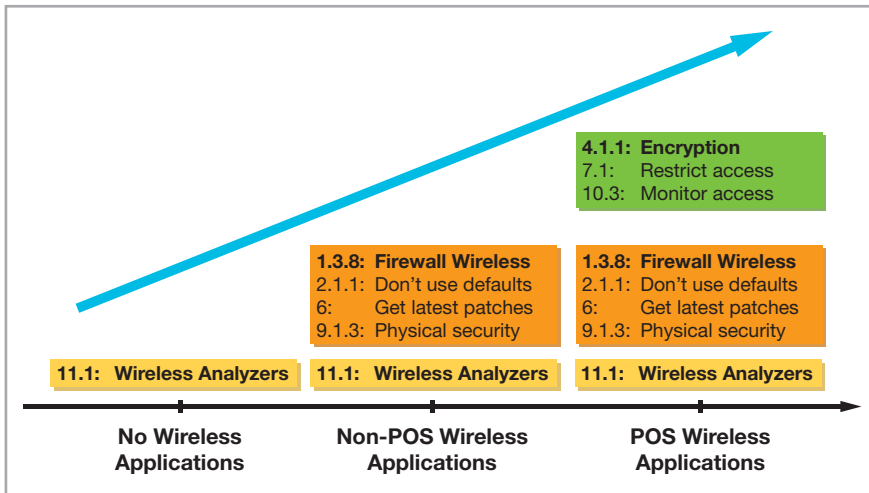
and the POS network and monitor the wireless LAN regularly.

PCI compliance is an urgent need. First, PCI compliance means securing networks from breaches, which protects your brand and your consumers. Second, payment brands have put forth additional incentives to increase the speed and rate of PCI compliance, where you can:

- Avoid non-compliance fines to the tune of \$25,000 per store per month
- Qualify for preferred transaction rates
- Be protected under the "safe harbor" provision where PCI compliant retailers are not liable or charged the approximate \$160 fee per stolen credit card record, in the case of breach.

### Aruba Benefits:

- Low TCO with built-in security for PCI compliance
- Protect legacy wired and wireless networks with an overlay architecture
- Prevent WEP-only device upgrades with identity-based security
- Easy migration to next-gen wireless LANs with multi-purpose platform
- Designed to scale for large number of remote retail stores

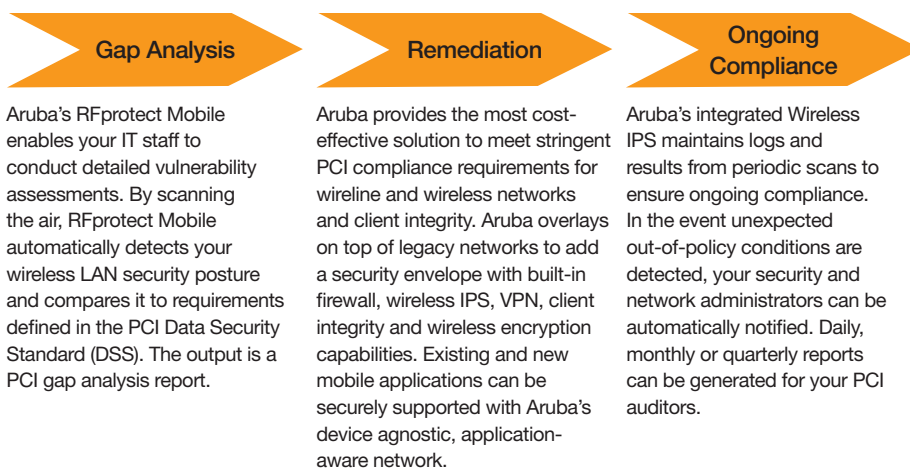


## How Aruba Enables PCI Compliance

Aruba Networks has pioneered a unique approach to painlessly and cost-effectively address PCI requirements. With an integrated solution for security, wireless/wired LAN and remote access, retailers can enable the necessary security for PCI compliance and enable business applications at the same time – without upgrading legacy networks. A detailed description of Aruba’s solution for PCI compliance can be found at

[http://www.arubanetworks.com/pdf/company/wp\\_PCI-Primer.pdf](http://www.arubanetworks.com/pdf/company/wp_PCI-Primer.pdf).

Aruba provides an end-to-end solution to ensure your wireless LAN meets stringent PCI compliance requirements and more importantly, your network is protected. From gap analysis to identify potential security holes to solutions for remediation to monitoring and auditing for ongoing compliance, Aruba has you covered.



**PCI SECURITY AS AN OVERLAY:**

Wireless Intrusion Protection Services (IPS) capabilities can be used as an overlay on top of existing wireless networks. Aruba's solution consists of an air monitor (or multiple) in the stores and a wireless intrusion protection server at the data center. Air monitors conduct wired and wireless scans on the store environment. Centralized servers then aggregate and analyze scans at each report to generate PCI scan reports to ensure compliance. In the event of unauthorized event, Aruba's wireless IPS will also generate alerts and automatically prevent attacks. Aruba's solution is unique in that the same hardware used for wireless IPS can also be configured to serve wireless access, providing an easy and cost-effective migration path to next-generation wireless LANs.

**PREVENT WIRED LAN UPGRADES AND REDESIGNS:** With Aruba's built-in ICSA-certified stateful firewall, VPN and wireless LAN authentication/encryption capabilities, existing wired network products such as routers and firewalls do not need to be upgraded to enable VLAN segmentation, VPN capability or AAA services for wireless security.

**IDENTITY-BASED SECURITY TO PROTECT WEP-ONLY DEVICES:**

Prevent WEP-only devices from opening a back-door into the data-center with Aruba's device and user-based security roles. Even if WEP encryption is compromised, access to the network is restricted using Aruba's built-in deep-packet inspection and stateful firewall.

**ONE PLATFORM, MULTIPLE USES:**

In addition to its strong security capabilities, Aruba's solution offers enterprise-grade, secure wireless LAN, mesh and wired LAN connectivity for a variety of applications. This includes simultaneous support for data, voice and video applications on any device.

**CENTRALLY MANAGED:** Aruba offers right-sized options for different store sizes that can all be centrally managed, as one network. Aruba's solution is designed to securely operate over private and public networks, extending to thousands of remote sites with all security policies centrally defined and monitored.



[WWW.ARUBANETWORKS.COM](http://WWW.ARUBANETWORKS.COM)

1322 Crossman Avenue, Sunnyvale, CA 94089 | Tel. +1 408.227.4500 | Fax. +1 408.227.4550