

Aruba PCI Compliance

Application Brief

PCI Compliance Application Brief

On Friday, May 4, 2007, the Wall Street Journal published a front page article describing a wireless LAN security breach at TJX Companies, Inc. resulting in the largest credit card theft in history. TJX is not alone – numerous retail, banking and other card-accepting organizations have been victims of such crimes. The PCI council, consisting of American Express, Visa, Mastercard, Discover and JCB, has published a data security standard, the PCI DSS, outlining security controls to prevent cardholder data theft.

The PCI DSS v1.2 standard defines mandatory requirements that must be met by all organizations that accept credit and debit cards. The standard's strict wireless LAN security requirements impact firewalls, authentication and encryption methods, monitoring and management systems, and can in some instances require costly and complex upgrades to existing networks. The cost of implementing previous versions of the PCI standard made some enterprises reticent to fully embrace the security requirements, leaving their wireless networks open to attack. Under the new PCI DSS v1.2 standard wireless security controls must be implemented or expensive fines will be levied.

Aruba's secure mobility solutions offer a cost-effective means of achieving PCI compliance. By providing an integrated solution, and eliminating the need to purchase and integrate multiple disparate network technologies, Aruba simplifies the task of securing a wireless network. Aruba also offers a range of solutions intended to fit varying needs for security controls on existing or legacy wireless networks, preventing the need for a wholesale upgrade.

- Significant capital and operational cost savings: Built-in security capabilities address every wireless LAN-specific PCI requirement (and many wired LAN requirements).
- Easy to integrate: Fits on top of your existing networks and thereby eliminates the need to redesign or replace legacy network infrastructure. Aruba's solutions extend the same high security paradigm to remote locations and stores, providing one common model for the entire enterprise.
- Protects existing investments: Securely segments legacy WEP-only devices to move them outside the scope of PCI compliance, thereby avoiding costly device upgrades.

Solution Overview



Benefits:

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

Solution Overview

Level 1: AirWave Wireless Management

- Server at HQ monitors all locations
- No dedicated sensor hardware required
- Monitors for and reports rogue APs

Level 2: AirWave Wireless Management, Aruba Mobility Controller, Sensor

- Server and controller at HQ
- Sensors in stores scan RF
- No change to existing LAN or WLAN
- Monitors for rogues, attacks, and reports
- Prevents rogues and attacks

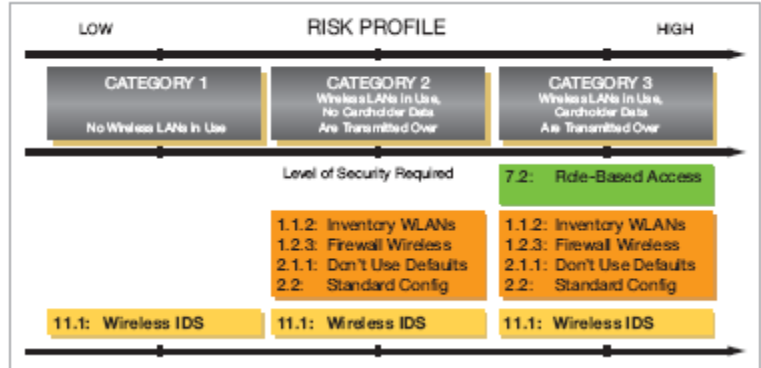
Level 3: AirWave Wireless Management, Aruba Mobility Controller, Aruba Hybrid Access Points

- Server and controller at HQ
- Sensors become hybrid APs
- APs added as necessary for coverage
- Stateful firewall segmentation
- Monitors for rogues, reports on attacks
- Protects legacy (WEP-only) client devices

LTI DataComm
 23020 Eaglewood Ct. #100
 Sterling, VA 20166
www.ltidata.com
 800-677-5050

PCI Requirements for Securing Wireless LANs

PCI DSS v1.2 includes twelve major steps for securing payment account information along with testing methodologies to ensure that these requirements are met. Wireless LAN security is a core component of these requirements. The PCI requirements specific to wireless LANs have been sorted into three levels of implementation in the illustration. Each category has a different risk profile, and a distinct level of mandatory security controls.



What Can Aruba Do?

Aruba Networks is a participating organization within the PCI council and supplies secure wireless LANs that are used by numerous leading merchants worldwide to comply with PCI standards and prevent network breaches. Aruba offers three levels of wireless LAN security to attain PCI compliance and beyond:

Level 1: PCI Monitoring

The PCI monitoring option entails installing Aruba's AirWave Wireless Management Suite (AWMS). AWMS is designed to inventory, monitor and manage multi-vendor wireless networks, and represents the most cost-effective approach to addressing applications in which legacy wireless networks are already in place - no hardware or software is required at any remote location.

Level 2: Wireless IDS

The AWMS PCI monitoring capabilities outlined in level 1 above are enhanced when used in conjunction with Wireless IDS (WIDS), while greater RF granularity is obtained by using dedicated sensors. By utilizing sensors in all remote locations, WIDS compares wired and wireless traffic, identifying and locating any rogue devices, attacks originating from outside the building, and most importantly, automatically blocks rogue devices and attacks. Both the level 1 and level 2 solution options enable merchants to outfit existing networks without replacing or re-architecting existing wired and wireless networks.

Level 3: Aruba Wireless LAN With IDS and Role-Based Access Control For Legacy WEP Devices

The wireless LAN with IDS and role-based access control option integrates the functions of a centralized wireless LAN, built-in stateful firewall, built-in wireless IDS, and AirWave monitoring. Aruba Controllers in the data center and remote locations are managed centrally through the AirWave Management Platform, which aggregates all wireless network information and provides PCI compliance reports.

The integrated Aruba WLAN provides all of the security controls necessary to meet wireless LAN PCI requirements, offers security controls for some PCI wired LAN requirements, and includes security controls that go beyond PCI requirements to help prevent breaches. Competing solutions require 3x - 4x the amount of hardware and software to provide comparable functionality. The level 3 solution is ideal for merchants that need to replace existing, legacy wireless LANs in order to comply with security, management and application requirements.