



Tel: +44 (0)1256 301900  
email: sales@reacttechnologies.com

## Wireless Infrastructure and PCI Compliance

Is it time to focus on ensuring our wireless infrastructures are impenetrable?

### THE PAYMENT CARD INDUSTRY THINK SO!

As you will no doubt know, there is a need for some technology in your retail branches to adhere to the PCI compliancy rule. What you may not know, is that your wireless infrastructure is very high up on the list... regardless of it's involvement with card transactions!

### The common resistance to upgrading the security on the wireless networks are these:

- We don't use WiFi to our cash registers (POS), so the added security is not needed!
- We don't store credit card data, so no need for WiFi security!
- We have a compensating control in place that eliminates the need for WiFi security!

The above statements DO NOT eradicate the requirement to have your wireless infrastructure be PCI Compliant.

### The repercussions for failing to comply to these requirements are as follows:

- Fines of up to £10,000 per month!
- Your right to do card transactions will be revoked!
- You are potentially the next victim in the long line of enterprises who have lost thousands or even millions of their customers details, losing trust and business in the process!

Prevent breaches, secure your network, gain control, free yourself of hassle?  
REACT have the answer!

This ruling is not a passing phase, it is a necessity and what the Payment Card Industry are enforcing to ensure the safety of card user details will effect you unless you realise, plan and upgrade!

The biggest headache the compliancy will cause will be proving the safety of the solution. Every three months! This will require you to enlist and pay for the services of a wireless monitor or..... **talk to REACT!!!**

1. Only Aruba's base platform is PCI ready with no additions to security..... **Job done**
2. The Airwave management tool allows you to provide proof on paper that your solution (whether it be Aruba, Cisco, HP, etc) is complying with PCI ruling. Simple, no hassle, no time wasted in hiring the services of others come in every three months to prove it for you!
3. Aruba's IDS security can be laid over any other main stream solution, allowing you to be secure in the knowledge that no matter your current solution, you can have the confidence of Aruba behind you.

*Realise, Plan, execute, protect your company!*

*Do not hesitate.... REACT!*





Tel: +44 (0)1256 301900  
email: sales@reacttechnologies.com

## Wireless Infrastructure and PCI Compliance

Risk Profile	PCI Requirement	React Recommendation
Don't Use ANY Wireless	Req 11.1: Quarterly monitor to ensure no unauthorized wireless devices are in use (that open a backdoor into the network)	Instead of relying on a quarterly scan that has a 3-month "blind-spot," consider using the built-in Wireless IDS capabilities of Aruba's WLAN or use Aruba's RFProtect™ / Airwave® suite as an overlay to the existing (Aruba or non-Aruba) WLAN.
Use Wireless for Inventory	Req 11.1: As defined above + Req: 1.3.8: Firewall (stateful) wireless networks away from the credit card environment to ensure even if wireless is breached, the rest of the network is protected.	Same as above + Beware of ACLs pretending to be stateful firewalls. Aruba offers an ICSA-certified firewall to protect the credit card environment. In addition, Aruba's firewall can protect WEP-only networks against exploitations of barcode scanners.
Use Wireless for cash registers	Req 11.1: As defined above + Req: 1.3.8: As defined above + Req: 4.1.1: Encrypt credit card transmissions over wireless networks with better-than-WEP technology.	Same as above + WEP, Keyguard and even WPA-PSK (pre-shared key) can be easily evaded as using publicly available tools. Aruba recommends the use of WPA-802.1x or WPA2-802.1x or VPN security to prevent eavesdropping of wireless transmissions. With centralized encryption, Aruba ensures client-to-core security even in distributed retail environments. In addition, identity-based security should be implemented to restrict access to credit card systems on a need-to-know basis.

Thank you for taking the time to read the above PCI Compliancy information. We at React are proud to offer our services in helping you upgrade your security. Conversations hold no obligation; the information passed to you is for your reference and education.

Please contact us to check your Compliancy.

**01256 301900**

