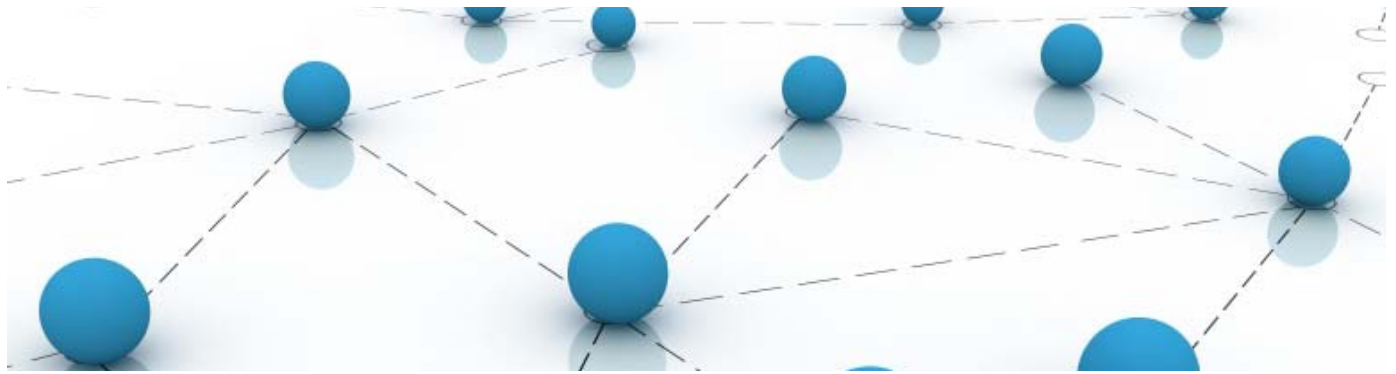


Pentura



Cost Effective PCI Wireless Compliance for Retail

The introduction of wireless technologies has created a new category of entry points into retail networks, potentially exposing sensitive data that is otherwise protected by wired security measures.

Whether an organisation has an official Wireless LAN (WLAN) or a no wireless policy, they need to account for these vulnerabilities; a single unattended wireless device, let alone a wireless LAN, can compromise the entire security of an enterprise network.

Key Benefits

Achieve cost effective Wireless PCI Compliance

Secure wireless airspace within stores/distribution centres

Cost Effective Wireless Monitoring

According to the independent research firm Gartner, identity theft through wireless vulnerabilities has increased by over 50% since 2003, and this number will continue to grow as more and more organisations adopt wireless for its huge business benefits.

The Payment Card Industry Data Security Standard (PCI DSS) has become the de facto standard in the payment card industry. Twelve best-practice principles are defined by the standard, aimed at securing credit card data. Participating vendors must comply with these requirements whenever they store, process, or transmit a credit card account number.

Those vendors that have wireless devices involved in storing, processing, or transmitting cardholder data, must follow the wireless-related requirements of PCI DSS.

Other vendors whose systems contain wireless devices that can access the cardholder data environment (from wired or wireless connectivity), also fall under the ambit of PCI DSS wireless requirements. For example, if a vendor has a wireless-enabled laptop that can access the cardholder data environment over the wired network, the vendor must follow PCI DSS wireless requirements and testing procedures.

PCI DSS 1.2, was released on October 2, 2008. While PCI DSS 1.2 does not add new requirements to the existing PCI DSS 1.1, it does expand on several of those requirements, especially those pertaining wireless to retail operations.

Pentura have analysed the wireless security requirements defined in PCI DSS 1.2 and have created a cost effective PCI DSS Wireless Risk Assessment (PCI DSS WRA) to assist vendors in compliance.

Below are the PCI DSS requirements related to wireless with an explanation of how the PCI DSS Wireless Risk Assessment will address the issues.

Regularly Monitor and Test Networks

11.1

Test for the presence of wireless access points by using a wireless analyzer at least quarterly or deploying a wireless IDS/IPS to identify all wireless devices in use

Pentura have solutions to deploy 24 x 7 wireless IDS/IPS; however we understand that deployments of this nature can be expensive. The PCI DSS WRA incorporates a quarterly assessment of each vendor network, store or distribution centre and identifies all wireless devices in use.

11.2

Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades).

If any significant changes are made to the network (such as new wireless Access Points being deployed) the PCI DSS WRA can quickly access and test any new aspects brought into the network.

Build and Maintain a Secure Network

1.1.2.

Current network diagram with all connections to cardholder data, including any wireless networks.

Keep an updated diagram of your network showing all the components and preferably showing the traffic flow across the network. Any wireless networks or devices that can potentially access the cardholder data environment must be included in the network.



Pentura's PCI DSS WRA will provide evidence of deployed wireless networks which will assist with the network diagram.

1.2.3

Install perimeter firewalls between any wireless networks and the cardholder data environment, and configure these firewalls to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.

Using the very latest wireless security testing, the PCI DSS WRA will confirm that the deployed security systems (such as firewalls) are protecting the cardholder data environment.

2.1.1

For wireless environments connected to the cardholder data environment or transmitting cardholder data, change wireless vendor defaults, including but not limited to default wireless encryption keys, passwords, and SNMP community strings. Ensure wireless device security settings are enabled for strong encryption technology for authentication and transmission.

The PCI DSS WRA tests to ensure that the wireless environment is secure and that default settings, encryption keys, passwords SNMP and any other areas of security which could lead to a compromise are reported.

Protect Cardholder Data

4.1.1

Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices (for example, IEEE 802.11i) to implement strong encryption for authentication and transmission.

- For new wireless implementations, use of WEP is prohibited after March 31, 2009.
- For current wireless implementations, use of WEP is prohibited after June 30, 2010.

Pentura's PCI DSS WRA will ensure that the deployed wireless networks transmitting cardholder data use industry best practices. Pentura will identify any areas of weakness in regards to encryption, authentication and transmission as part of the testing process.

Contact:

Pentura Limited
Diddenham Court
Grazeley, Reading
RG7 1JQ

Tel: 01189 768960

Email: info@pentura.com