

## FOCUS ON: PCI DSS and Wireless Data Security.

### Maintaining PCI DSS compliance: The challenge of wireless security.

According to recent analysis by AirTight® Networks, a leader in wireless security and compliance solutions, there are very high incidences of wireless vulnerabilities among organisations which are, or are endeavouring to meet the compliance standards of the PCI DSS, especially those outlined in the [PCI DSS Wireless Guideline](#).

In its analysis of over 200 cardholder data environments (CDEs), AirTight found locations with open Wi-Fi access points using vendor default settings violating PCI DSS wireless Guideline 2.1.1, the lack strong encryption (violating 4.1.1), and with a potential to provide a backdoor between an un-trusted network and the CDE violating requirement 1.2.3

Other significant findings from the data were:

- 24% of enterprises had rogue access points (APs)
- One in three enterprises continues to deploy unsecured APs
- 68% of enterprises were exposed by vulnerable wireless users such as smart phones, wireless POS and laptops. Plus users in unencrypted ad-hoc mode such as a smart phone connecting to a printer, a laptop or to external WiFi Applications.

The proliferation of Wi-Fi enabled devices like smart phones, tablets etc... continues to be the number one wireless security threat, yet something that enterprises often overlook in their security assessment.

Only 24% of enterprises were completely clean in this AirTight assessment.<sup>1</sup>

<sup>1</sup> The wireless vulnerability scanning data was collected by AirTight, using its SpectraGuard® Online PCI wireless compliance scanning service during a six month period and suggests that many enterprises are still exposed to vulnerabilities that violate multiple PCI DSS wireless requirements..

As many organisations know, and some find out the hard way (see Hannaford Brother's PCI breach) compliance does not mean security. Compliance is, in fact, only a point in time; no organisation operates in a vacuum, and the level of information security in any organisation is affected by dynamic internal and external factors that fluctuate and change on a daily basis. The most significant, of these factors, and the hardest one to manage, is people.

### Who needs to worry about PCI wireless scanning ?

Whether or not wireless is legitimately deployed in the card holder data environment, consumer grade WiFi devices like smart phones are easily installed by end users anywhere. These are likely to ultimately compromise an secure network. Unauthorised devices can go unnoticed for long periods of time and be exploited by hackers. This means that all enterprises to need to worry about Wi-Fi vulnerabilities at all locations, all of the time whether or not CDE or legitimate WiFi is deployed.

### Beyond the Ad-Hoc check, and forward to PCI compliance, plus strong security.

PCI DSS operates on a minimum three-year cycle and hence the most cost effective solution is one that will protect for this period, and beyond even if your network configuration, and the devices on it change. Secondly, selecting the right tools to scan and secure your network from wireless threats today can save time and money instead of investing in point solutions that need to be replaced when you upgrade your network.

PCI DSS standard mentions four methods for scanning your environment to meet compliance namely WIPS, NAC, handheld scanners and even visual inspection. Lets us analyze what

each method delivers and whether it will truly protect your data or merely give you a single, snap shot in time.

**Handheld scanning** - Handheld analyzers are carried around the merchant's site to collect data, which is then interpreted manually or fed to an interpretation tool. Using these analyzers on a quarterly basis provides no data security – only a report on that days profile.

*“Handheld scanning is like locking your door occasionally hoping the burglar will try your house on those days.”*

Active compliance and awareness activities, such as automated policy management tools.

**NAC (Network Access Control)** – This method has not been widely adopted and, therefore, would be an unlikely choice since it requires the purchase of expensive equipment and licenses especially at the device level. A major drawback is that it will not detect a smart phone operating as a rogue AP connecting to the enterprise network via a valid desktop or laptop.

**Visual inspection** – Visual inspection appears to have some value for small locations such as a small shop or restaurant. However, it is questionable as to what one can see with that inspection? You might see something connected if it is in plain view. However, how will you determine if a smart phone is physically connected only for charging and hence harmless or if it is bridging to the network via the computer as a rogue AP. And how does one assure the quality of a visual inspection?

**WIPS (Wireless Intrusion Prevention System)** – WIPS is an automated solution and consists of wireless security sensors that sniff the surrounding airspace for available wireless data and send it to a central server. The central server, in turn, has an engine to correlate and mine the obtained information to create relevant information PCI compliance. It offers 24/7 monitoring and prevention and is especially useful for geographically distributed organizations because manual wireless scanning does not scale and can prove costly. WIPS will detect not only rogue APs but also incidence response as required for compliance with PCI DSS Wireless guideline.

## Criteria to consider when implementing a wireless scanning solution

**Reporting** - Does the solution provide a detailed clause by clause compliance report for any given site and across multiple sites? A comprehensive report also helps to speed the audit process, as all the required information will be readily available in the report.

**Configuration and management** - Many retail chains often lack dedicated IT support at remote sites, which means the PCI wireless solution should be easy to configure and maintain, even without trained IT staff. The solution should accurately detect wireless threats because false alarms can add unnecessary work. Ideally the solution should be automated and require minimal human intervention for day-to-day operation.

**Scalability** - A scalable tool can be easily deployed at multiple sites and be easily extended to new sites. If you plan to deploy Wi-Fi for CDE operations in the future, consider a solution, which can up-scale as your organisations needs change.

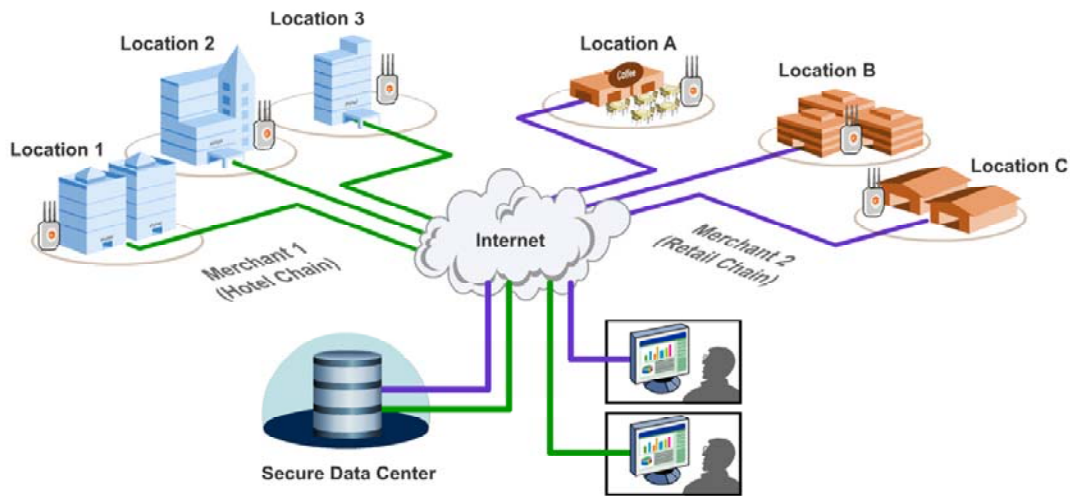
**Comprehensive threat coverage** - A compliance solution should be non-vendor specific , and cover all wireless vulnerabilities – i.e. rogue AP and other mismanaged APs, misbehaving wireless users, MAC spoofing and denial of service attacks and all their variations. The solution should be easily upgradeable to cover newly discovered vulnerabilities and threats.

**Accurate device classification** - This is fundamental to detecting rogue APs. PCI wireless solutions that have comprehensive classification engine require fewer inputs. Classification policies should automatically classify devices scanned over the air into categories such as corporate, rogue and external thus providing full visibility of wireless devices using the air space.

**Reliable and automatic prevention** - Incident response to a wireless security incident is one of the requirements in the PCI DSS. Having sound automatic prevention enables merchants to quickly and easily respond to detected threats and prevent damage.

**Precise Location tracking** - Tracking location of devices helps physical remediation of erring wireless devices, for example a smart phone and track the inventory of wireless devices.

**Cost and Cloud based WIPS** Prices of the tools vary greatly. A cloud-based solution is lower in cost and is available within most operations budgets. In this option, wireless security sensors at each location are connect to the WIPS server(s) in the cloud. This solution can be just as effective for for a small merchant with few locations, or a global corporate retailer.



AirTight Cloud based WIPS for PCI Compliance

*With the proliferation of Wi-Fi enabled devices it has never been more imperative that organisations are able to enforce wireless policies and , meet the requirements of both legislative and best practice compliance standards such as DPA, ICO, PCI-DSS, and ISO270001 .*

**If Information and Data Security compliance is important to your organisation, talk to us now...**

**Tel: 01908 - 565608**

**Email:**

[sales.support@euroteknetworking.co.uk](mailto:sales.support@euroteknetworking.co.uk)

**Visit:**

[www.euroteknetworking.com](http://www.euroteknetworking.com)



**ASV Certificate Number:  
3974-01-05**