



Aruba's Wireless Intrusion Protection Solution

Today All organizations require the ability to enforce a stated wireless policy to prevent unauthorized access to the corporate network and to maintain data privacy and integrity. The Aruba wireless intrusion detection and prevention (WIDP) System provides this ability by protecting against rogue access points and identifying signatures of known attacks.

Using Aruba's Wireless Intrusion Detection/Prevention

ENFORCING NO-WIRELESS:

The Aruba WIDP system identifies, locates and contains unauthorized APs to help organizations that are not yet ready to deploy a WLAN to enforce a no-wireless policy.

SECURING ENTERPRISE WLAN:

The Aruba WIDP system protects against attacks through Wi-Fi and alerts the administrator on detection. This helps enterprises deploy secure wireless networks.

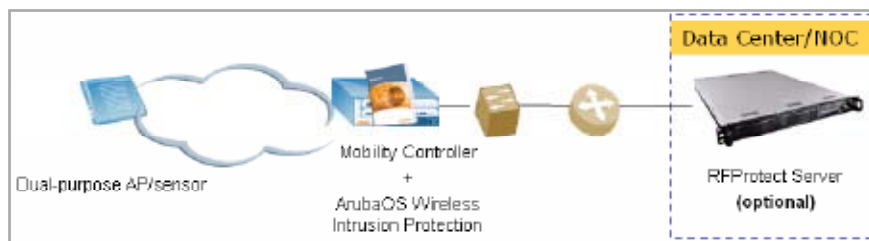
MANDATED REPORTING:

The Aruba WIDP systems provides organizations with the ability to create reports for Payment Card Industry (PCI) compliance, HIPAA compliance and DoD policy 8100.2 compliance to meet industry policy mandates.

Benefits:

- **Reduced deployment and management costs through integration:** Avoids the need for overlay IDS system using dedicated sensors
- **Automatic containment of unauthorized clients and ad-hocs, even as they roam**
- **Customizable security policies:** Provide organization-specific security policy enforcement and reduce false positives
- **Fully automated reports for compliance with PCI, HIPAA, DoD 8100.2, GLBA**

Aruba's WIDP Solution



In the Aruba WIDP solution, a combination of dedicated air monitors/sensors and access points provides 24x7 monitoring of all channels. These sensors and access points provide inputs to the Aruba Mobility Controller and the (optional) RFprotect Distributed server. The controller correlates the data from multiple sensors and access points to provide centralized rogue AP detection, classification and containment.

The RFprotect Distributed server enhances the capabilities of the solution by enabling the creation of customized security policies using PolicyEnforce™. Additionally, the RFprotect Distributed server can be used to create industry standard and customized reports about the security posture of the organization's wireless network. This includes industry-standard compliance reports for policies such as Payment Card Industry (PCI), DoD 8100.2, GLBA and HIPAA.