



## Industry

- Government Services

## Key Challenges

- Solution required to monitor traces of wireless intrusion and endpoint bridging to external networks

## Solutions

- Wireless Intrusion - AirTight SpectraGuard Enterprise & SAFE
- Network Monitoring - WildPackets OmniPeek Enterprise

## ROI

- Comprehensive visibility of wireless network
- Monitoring, detection and prevention of rogue access to internal wireless network
- Generate audit trail reports in both wireless & wired networks

## Overview

As Wi-Fi adoption grows, so do the stakes. Cyber-criminals are drawn to high-value targets like the enterprise servers and corporate data now reachable via wireless. New airborne threats continue to emerge, exploiting misconfigured networks, promiscuous devices, and naïve users. From on-site employees and guests to off-site travelers and tele-workers, all companies today face some degree of Wi-Fi exposure.

To safely reap the business benefits of Wi-Fi, we must move beyond weak first-generation deterrents like Wired Equivalent Privacy and passive Wireless Intrusion Detection Systems (WIDS). Surviving airborne threats requires a proactive, effective defense that incorporates both Wi-Fi Protected Access and an automated, accurate Wireless Intrusion Prevention System (WIPS).

WIPS goes beyond detection by neutralizing perceived threats in real-time. A well-oiled WIPS can prevent unauthorized network use, block unsafe client activities, and disrupt attacks before they do harm. But a misbehaving WIPS can disrupt mission-critical traffic and neighboring networks. Like any power tool, a WIPS must be selected and used with great care.

## Business

A large agency occupying 24 storey of a building who in the business of accounting & managing customer taxes faces wireless bridging and intrusion from nearby buildings. This agency houses 4000 machines and deployed 82 access points in the whole building with minimum security and features that does not allow the IT department to monitor, track and take actions.

## Operational Challenge

No proper operational control on wireless security and thus, results in external threats and internal bridging that will cause potential lost of customer data. Business information about customers is in high risk.

The IT team found it difficult to generate evidence of intrusion and endpoint bridging to external networks and potentially risking data losses.

## **Solutions**

### **Proposed of AirSpace Security Tracking Systems**

#### **AirTight SpectraGuard Enterprise & SAFE**

SpectraGuard Enterprise is an end-to-end wireless vulnerability management solution needed for today's global enterprise. It extends the trusted wireless intrusion prevention (WIPS) capabilities offered by AirTight. SpectraGuard Enterprise is suitable for large customers who want to purchase the wireless security equipment and host it at their site. AirTight SpectraGuard is the only WIPS on the market today to protect both 802.11n and legacy a/b/g wireless infrastructure. AirTight's 802.11n sensor is a dual radio 802.11n sensor platform that can detect, prevent and remediate all 802.11n wireless vulnerabilities.

SpectraGuard Enterprise provides complete wireless protection for your corporate network. It ensures that business data does not leak out of the corporate network through the wireless medium. It accurately classifies and blocks all unauthorized access and rogue traffic without disrupting authorized wireless communication.

Inadvertent leakage of customer or business data through wireless can lead to significant brand erosion. Traditional firewalls only monitor wired traffic and have no visibility into the wireless traffic that is flowing in the air. SpectraGuard Enterprise continuously scans the airwaves and provides automatic protection against data leakage through wireless means.

#### **3 main key factors in this solution:**

##### **- Vulnerability Assessment**

Prevent wireless threats by automatically scanning, detecting and classifying all unauthorized access and rogue traffic to your network with the industry's most robust and accurate wireless vulnerability assessment solution.

##### **- Regulatory Compliance**

Meet all your wireless compliance requirements for regulatory standards such as PCI, SOX, HIPAA, GLBA and others. Simplify the reporting process with user-friendly predefined reports.

##### **- Vulnerability Remediation**

Take proactive steps against any wireless security threat by blocking it and removing it by accurately locating it on your floor map with the most precise location tracking solution. This module includes all wireless intrusion prevention (WIPS) capabilities where AirTight has already established proven leadership.

## Solutions

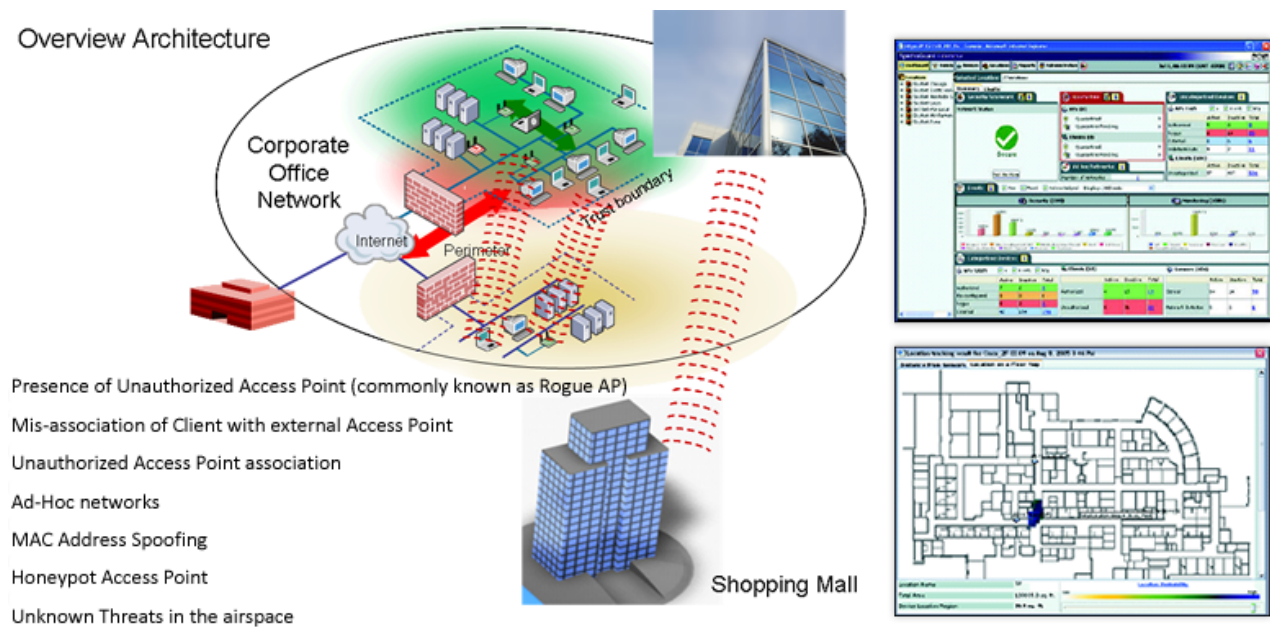
### WildPackets OmniPeek Enterprise

OmniPeek Enterprise is WildPackets' flagship product. It combines all of the features of the OmniPeek product line in one product, including support for local captures from multiple interfaces and connections to an unlimited number of OmniEngines. It also supports data collection from any network topology, including Gigabit networks, WAN links and local matrix switches.

OmniPeek Enterprise is ideal for IT organizations responsible for network analysis and network services SLAs for the entire organization. A license of OmniPeek Enterprise should be considered for each location that will be supported by a network engineering professional. OmniPeek Enterprise also supports the Advanced Voice & Video Option.

### Solutions Implementation Diagram

Overview Architecture



## Return of Investment

### Comprehensive Visibility of Wireless Network

The entire solution has provided the agency with comprehensive visibility in their entire wireless network.

The IT dept is able to monitor, detect and prevent of rogue access point to internal wireless network.

The wireless security solution has help IT team to track the location of rogue access points.

### Full Control of Access with Audit Trail Capabilities

The wireless client installed on the users' workstations has given the agency full control of their access in public, home and internal network access.

In addition, the IT dept are able to generate an audit trail reports in the wireless & wired network on users' access and the entire network traffic flow in their Local Area Network.