



**FOR IMMEDIATE RELEASE**

**AirPatrol Finds Wireless Security Vulnerabilities at RSA,  
World's Premier Information Security Conference**

*AirPatrol Uses its Leading Wireless Locator System Product  
to Sniff Out Many Rogue Wireless Access Points and Suspicious Ad-Hoc Networks*

**RSA Conference—San Francisco—April 23, 2009**—AirPatrol Corporation, a leading mobile and wireless threat management solutions company, today announced results of wireless monitoring it conducted Wednesday, April 22, at the RSA Conference, the world's premier information security conference, using its Wireless Locator System Version 3.0 product. AirPatrol discovered 2,792 WiFi client devices, including smart phones, PDAs and laptops in use. While the WiFi network offered by RSA Conference organizers was well secured, AirPatrol discovered 94 unofficial (potentially rogue) access points which were not affiliated with the conference organizers.

A large fraction of the detected clients were associated with the unofficial access points, signaling potentially insecure network connections. Also, 35 Ad-Hoc networks with common Service Set Identifiers (SSIDs) were discovered, which also signals a potentially insecure security posture for those WiFi clients associated with them. To speak with Ozzie Diaz regarding AirPatrol's wireless monitoring results, stop by the McAfee Partner Pavilion at RSA, Booth #1017 or contact Bill Keeler at Schwartz Communications, 781 684-6542 or [airpatrol@schwartz-pr.com](mailto:airpatrol@schwartz-pr.com).

“Amazingly, some of the world's leading IT security professionals still think of wireless security as an afterthought and our RSA Conference wireless monitoring results demonstrate there is still a disconnect between what they practice and what they preach,” said Ozzie Diaz, CEO, AirPatrol Corporation. “Industry experts tracking the phone and PC market expect more than 1.5 billion new devices to be sold in 2009 alone. Each device is a threat for malware and/or information extrusion. Blackberry's, iPhones, Nokia Symbian devices, and many more are ‘always connected’ storage, photography, recording, and yes, telephony devices. The diligence and awareness of keeping information secure is the only option for corporations.”

## **Other interesting findings from AirPatrol's wireless monitoring:**

**Rogue Access Points-**AirPatrol discovered 94 rogue or unauthorized Access Points (APs), the devices used to connect wireless devices to a network. In a corporate setting an IT administrator managing a wireless network would be looking to immediately shut down all rogue or unauthorized APs that could be a threat to security.

**Adhoc Networks-** AirPatrol discovered 35 Ad-Hoc networks using common SSIDs such as Linksys, Free Public WiFi and hpsetup. Ad-Hoc networks present problems as there is often times no firewall on the wireless interface, leading to potential security issues.

### **About AirPatrol Corporation**

AirPatrol Corporation is the most trusted authority on mobile and wireless threats to enterprises. The company's comprehensive suite of location-based products enable security administrators in the government, financial, healthcare, corporate enterprise and retail industries keep pace with the expanding requirements of an increasingly mobile world. For more information, please visit the company's website at [www.airpatrolcorp.com](http://www.airpatrolcorp.com).

### **Media Contact**

Bill Keeler

Schwartz Communications

781 684-6542

[billk@schwartz-pr.com](mailto:billk@schwartz-pr.com)

###