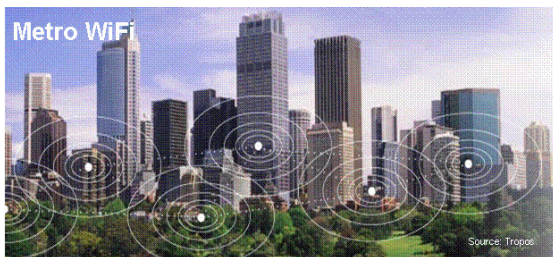

**Wireless Protection for the
Mobile Enterprise**

Wireless Protection for the Mobile Enterprise

An essential component of enterprise Wireless Intrusion Protection Systems (WIPS) is the ability to enforce corporate security policies and defend mobile wireless clients from attacks that happen outside the secure enterprise perimeter. Enterprises also need to enforce wireless access policies within the perimeter with the advent of pervasive wireless access from municipal Wi-Fi deployments. This paper addresses the security challenges faced by an enterprise submerged in a pervasive wireless environment. It also describes the rising threats to enterprise wireless laptops at hotspots, airports, hotels and other public access networks. Finally, the paper provides an overview of AirDefense Personal policy enforcement and centralized monitoring technology that can provide comprehensive protection for the modern mobile enterprise.

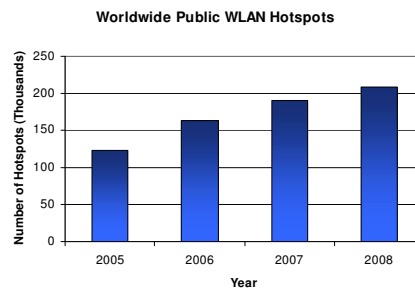
Wireless technology is growing in popularity. Businesses are not only migrating to wireless networking, they are steadily integrating wireless technology and associated components into their wired infrastructure. The demand for Wireless Local Area Networks (WLANs) is fueled by the growth of mobile computing devices, such as laptops and personal digital assistants, and a desire by users for continual connections to the network without having to “plug in”. **Figure 1** shows the trends in WLAN hotspot adoption based on Gartner Dataquest survey. In fact, according to Dell’Oro, there has been an 87% increase in hotspots worldwide from January 2005 through January 2006 - from 53,779 in 93 countries to 100,355 in 115 countries. The predicted growth in citywide or municipal Wi-Fi deployments is an astounding 84x over the next 4 years, according to ABI Research. Metro scale deployments are already on the way in 190 cities in 2006.

Municipal Wireless Deployments



- 84x increase in municipal Wi-Fi from 1.5K sq miles today to 126K sq miles in 2010 [ABI]
- Metro scale deployments already on the way in 190 cities in 2006

Worldwide Public WLAN Hotspots



- 87% increase in hotspots worldwide from January 2005 through January 2006 - from 53,779 in 93 countries to 100,355 in 115 countries [Dell’Oro]

Figure 1: Trends in WLAN hotspot adoption.

It is fair to say that Wi-Fi networks that are already present in several locations will continue to grow and become virtually pervasive with municipal deployments and increase in hotspots. The modern mobile workforce realizes business efficiencies that result from anywhere, anytime internet access. Based on the above trends enterprises face two daunting challenges:

- How do we enforce corporate internet/wireless access policies when we are submerged in pervasive wireless networking environments?
- How do we secure our mobile workforce from the rising threats and attacks that happen outside the enterprise perimeter?

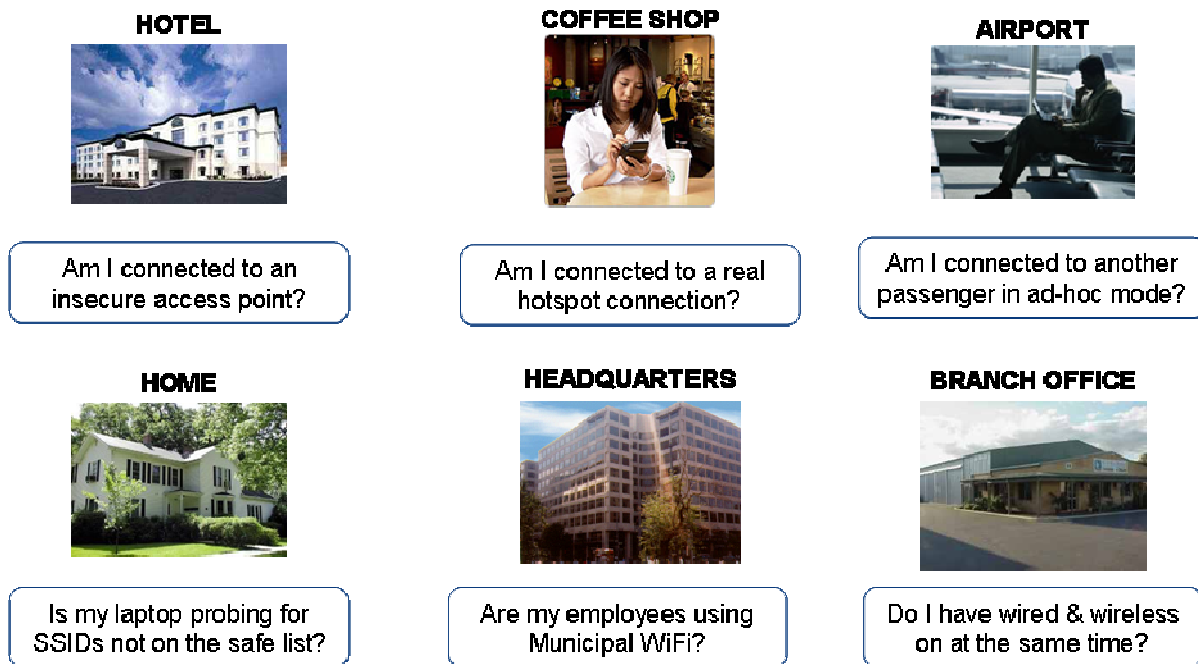


Figure 2: Typical mobile wireless access locations.

1. Wireless Threats Faced by the Mobile Enterprise

Today's mobile workforce is extending the edge of the enterprise network to such locations as shown in Error! Reference source not found.. Hotels, hotspots and other public access wireless networks are prime locations where hackers exploit wireless vulnerabilities to gain access into unprotected laptops. In addition, municipal Wi-Fi deployments are invading the enterprise air space.

Evil Twin

Using public hotspots is definitely convenient; however, you may want to think twice before accessing confidential information via hotspots. Recent headlines raise concern about wireless security issues around hotspots. Particularly the Evil Twin attack has received much attention, even though it is based on a tool that is relatively straightforward and has been around for several years. In this scenario, a hotspot user connects to the Evil Twin wireless Access Point (AP), believing it to be a legitimate commercial hotspot. Once connected the hacker impersonates a legitimate hotspot, and records all information entered into the web page, which can include your passwords, emails or credit card information.

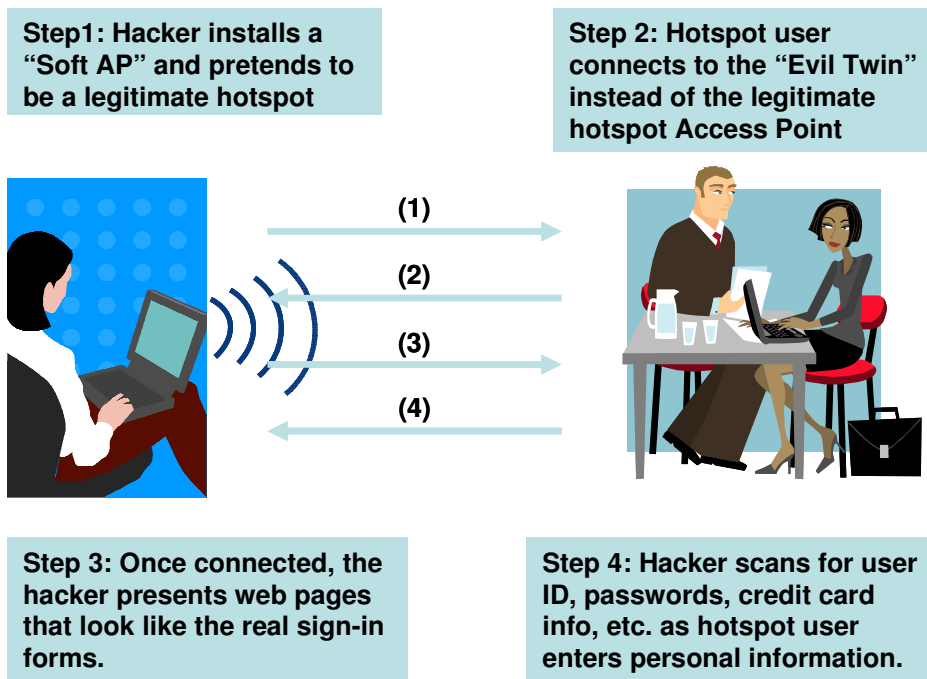


Figure 3: Wireless Evil Twin attack mechanism

The Evil Twin attack would work as shown in **Figure 3**. A hacker would set up his laptop to act as an AP. Several commercial and freeware software tools are available that can turn any laptop with a wireless card into a so-called soft AP. The soft AP will broadcast an identification beacon or Service Set Identifier (SSID) that lets other computers know it is available. The hacker can even give it a legitimate name, such as "tmobile", "Wayport", "Free Internet Access", to fool unsuspecting users. The hotspot users connect to what appears to be a legitimate hotspot. When connected the hacker will redirect the user to web pages created to look authentic. As the user enters passwords or creates a new ID with credit card information, all entries are logged by the hacker for future abuse.

In addition to tricking an unsuspecting user into connecting to their laptop, hackers have the benefit of taking advantage of the increasingly wireless-friendly nature of the Windows XP and MAC OS X operating systems. Due to the self-deploying nature of wireless, a wireless laptop will continue to "probe" for APs it has been connected to in the past. These probes are easily picked up in the air by

freely available wireless monitoring tools. If the Wireless Connection Manager in Windows XP sees a legitimate SSID it will automatically re-connect to that AP. All the hacker has to do is give his soft AP a detected SSID. Using a manufacturer's default SSID, such as "linksys", "belkin", "101" or "tsunami" increases the chance of connecting because most users that have not changed their default SSID almost certainly will not have enabled any authentication or encryption. The laptop will automatically establish a wireless connection without any required user action.

Furthermore, wireless devices are transient in the way they connect. If the signal strength of the Evil Twin is stronger than the legitimate hotspot AP, the wireless device could switch to the Evil Twin. Several wireless devices will automatically switch to the strongest signal, even if that means abandoning a secure connection.

Wi-Phishing

The Evil Twin attack is broader in definition and refers to the impersonation of a trusted network to establish a wireless connection. Once the wireless connection has been established the Evil Twin can be used for Wi-Phishing. Wi-Phishing is the act of covertly setting up a wireless-enabled laptop or AP (such as an Evil Twin) but for the sole purpose of getting wireless laptops to associate and track keystrokes, allowing the hacker to capture passwords and credit card information. This concept is very similar to the email phishing scams, where a message is sent to users tricking them to enter confidential information, such as bank account information or other sensitive username and password combinations. The process of tricking someone to voluntarily provide confidential information has been used for years in a variety of forms and is generally referred to as "social engineering". Gartner estimated that phishing scams cost banks and credit-card issuers more than \$1.2 billion in 2004.

Man-in-the-Middle Attacks

A man-in-the-middle attack is a type of attack where the user gets between the sender and receiver of information and sniffs any information being sent. In some cases users may be sending unencrypted data which means the man-in-the-middle can easily obtain any unencrypted information. In other cases, the attack could be used to break the encryption key.

Virus and Trojan Injection

AirDefense has also identified several instances where unsuspecting wireless users received a fake web page with a mouse-activated web overlay. Any click of the user's mouse would trigger a download of harmful content, such as a virus or Trojan.

Ad-Hoc Connections

Ad-Hoc mode connections allow one wireless device to directly connect to another device. Default ad-hoc mode usually does not require authentication or encryption. This allows hackers to easily connect to an enterprise laptop without going through the more involved Evil Twin setup. Often mobile users leave their wireless card on when connecting to the enterprise wired network. This can result in an easy access wireless "bridge" into the wired network that circumvents firewalls and traditional wired perimeter security.

Municipal Wi-Fi Threat

Municipal Wi-Fi is designed to provide cheap broadband access to cities and municipalities. It leverages the economies of scale that the massive adoption of Wi-Fi has realized. These deployments are based on wireless mesh networking technologies using 802.11 APs that can provide local Wi-Fi access as well as wireless backhaul to other nodes. Philadelphia was one of the first cities to adopt municipal Wi-Fi. According to the Wireless Philadelphia Business Plan, "...the more secure the network is, the more complicated the provisioning process can become. Open access in parks and public spaces should limit the provisioning requirement to confirmation of an acceptable use policy and disclaimer." This highlights the amount of security the municipal Wi-Fi networks will have. The head-aches associated with managing different security flavors (WEP, WPA, WPA2, etc.) and heterogeneous clients and users is a sufficient enough bottleneck that most municipal Wi-Fi access will essentially be "open".

Enterprises with offices in the municipal Wi-Fi coverage area, in addition to regular RF interference with their own corporate WLANs, will have to deal with several serious security issues:

- Accidental associations of their wireless users to municipal Wi-Fi APs, especially with unmanaged "Zero Configuration" wireless clients running on corporate laptops
- Employees circumventing wired content filtering and internet access monitoring technologies that resided at wired access gateways by connecting to available municipal Wi-Fi APs
- Increased attack surface available to hackers on the municipal Wi-Fi network through Evil Twins, Wi-Phishing, Virus and Trojan injections, etc.

2. Best Practices for Securing Mobile Wireless Access

Industry analysts and security experts agree that taking the following precautions significantly mitigates security risks associated with mobile wireless access.

- Install a firewall
- Use hotspots only for internet surfing
- Enter passwords only into websites that include an SSL key on the bottom right
- Disable/remove the wireless card if you are not actively using the hotspot
- Ensure that your laptop is updated with the latest security patches
- Avoid hotspots where it is difficult to tell who's connected (hotels, airport clubs, conferences - large facilities)
- If the hotspot is not working properly, assume your password has been compromised, report to hotspot service provider and change your password at the next immediate opportunity
- Read all pop-up windows in their entirety
- Do not use insecure applications such as non-encrypted email or instant messaging while at hotspots
- Explicitly disable municipal Wi-Fi access from within the enterprise
- Install AirDefense Personal

"AirDefense is a clear leader in wireless surveillance and offers the best available solution on the market."
Rene Hirsch, Managing Director, AirWire

3. AirDefense Personal

AirDefense Personal is a software agent that runs on Windows PCs and monitors for policy compliance and security exposures while providing notifications to the user and the enterprise manager. It enables enterprises to manage security risks due to vulnerabilities associated with a mobile workforce. It is important to point out that classical client based firewalls focus on Layer 3 and above of the Open System Interconnection (OSI) protocol stack. A wireless connection between an AP and a laptop occurs at the MAC (Media Access Control) layer. The MAC layer is a sub-layer of the Data Link layer, also known as Layer 2 of the OSI model. This is one level below where most firewalls and VPNs operate. While firewalls and VPNs provide security at Layer 3 and above, AirDefense Personal ensures a secure wireless connection by identifying risks at Layer 2.

Features and Benefits

AirDefense Personal is designed for complete Wireless End-Point Security (WEPS). It has the following features and benefits:

1. Comprehensive real-time mobile threat detection and automated response for

- Evil-twin attacks
- Redirection attacks
- Man-in-the-middle attacks
- Soft AP connections
- De-authentication attacks
- Abnormal wireless activity – e.g., sudden significant change in wireless signal strength
- Phishing attacks
- Automatically enforce enterprise wireless policies anywhere
- Precise use of VPNs including specifying name of the VPN process (e.g. iPass, openvpn.exe, etc.)
- Use of Bluetooth
- Use of broadband wireless access such as EvDO, 3G/GPRS, EDGE and UMTS
- Use of hotspots
- Use of unsecured wireless networks
- Ad-hoc peer-to-peer networks, preferred SSID, encryption and use of multiple wireless cards

2. Automatically eliminate wireless bridging problems

- Simultaneous wired and wireless connection is managed with wireless disconnection when wired network is on, restored when wired connection is off

3. Automatically eliminate probing laptop problem

- Regular automated management of windows zero configuration client to reduce or eliminate probing laptop problem – a major threat to wireless intrusion

4. **RF Boost™ allows enterprises to easily create custom policies and alarms through step-by-step wizards. Policies can be based on**
 - Active applications
 - Registry key monitoring
 - Windows hot-fix patches installed
 - All alarms can have user-definable actions if triggered which take into account the way that wireless users work.

5. **Location information to track mobile laptops anywhere in the world**

6. **Ability to black-list non-sanctioned wireless networks such as municipal Wi-Fi or neighbor's networks.**

7. **Central monitoring and policy enforcement**
 - Define policies by groups (e.g., Sales, Engineering, Finance, etc.)
 - Create multiple profiles and actions (e.g., Telecommuters, administrators, etc.)
 - Stealth installation of agents into laptops
 - No user involvement, if desired

8. **Works in conjunction with client firewalls**
 - Low memory footprint (approximately 1 MB)
 - No special adapters or drivers needed

9. **Intuitive user interface to swiftly define policies and solve problems**
 - Quick glance detection of status, problem and actions
 - Minimized tool bar application which shows at a glance the current state of your mobile workforce.

10. **Integrated with AirDefense Enterprise and also available standalone**

Figure 4 shows sample screenshots of the Personal client. The client alerts the mobile user when attacks or vulnerabilities are detected. In standalone mode, the client also allows the user to define and enforce individual policy. **Figure 5** depicts one of many screenshots available within the Personal Manager. The Manager provides a centralized view of threat levels, usage summary, policy violations, etc., of all wireless assets along with the ability to access remote agent connection details. It also allows the administrator to define new policies and enforce them globally.

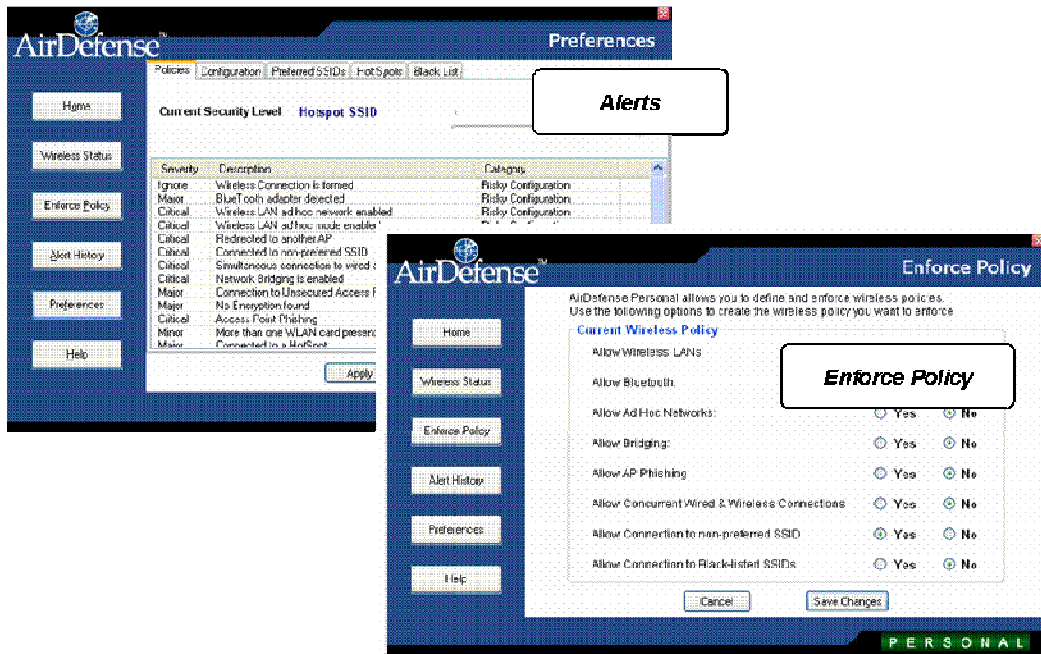


Figure 1: AirDefense Personal Client Agent

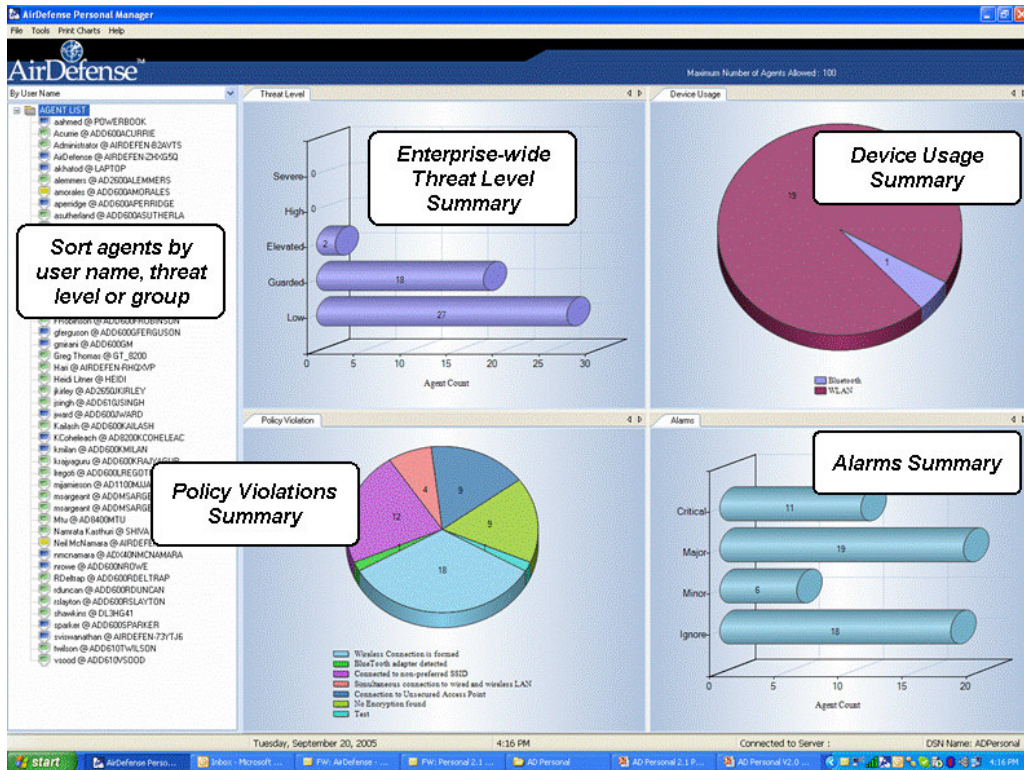


Figure 2: AirDefense Personal Manager

4. Summary

Mobile wireless devices are often the weakest link in the enterprise security infrastructure. While perimeter security is critical, realizing that laptops and mobile workers are extending the edge of the network to risky areas such as hotspots is essential. Further, pervasive wireless networks such as municipal Wi-Fi are invading the enterprise perimeter. Firewalls and VPNs provide only limited protection to wireless devices from the rising threat of Layer 2 attacks. AirDefense Personal, works in conjunction with firewalls and VPNs to defend mobile wireless assets from all Layer 2 attacks and vulnerabilities while allowing enterprises to centrally monitor and enforce common policies across all stations.

“With this (AirDefense Personal) technology, customers can control not only what they have in their own environment, but also what they are doing when they take their laptops out into the world. From an enterprise perspective, that’s a technology I think just about every customer would want to have.”

John Sieg, Business Security Executive, International Systems Marketing

AirDefense, the market leader in anywhere, anytime wireless security and monitoring, is trusted by more Fortune 500 companies, healthcare organizations and high-security government agencies for enterprise wireless protection than any other wireless security provider. Ranked among *Red Herring's* Top 100 Private Companies in North America, AirDefense products provide the most advanced solutions for rogue wireless detection, policy enforcement and intrusion prevention, both inside and outside an organization's physical locations and wired networks. Common Criteria-certified, AirDefense enterprise-class products scale to support single offices as well as organizations with hundreds of locations around the globe.

AirDefense Enterprise, the flagship product, is a wireless intrusion prevention system that monitors the airwaves 24x7 and provides the most advanced solution for rogue detection and mitigation, intrusion detection, policy monitoring and compliance, automated protection, forensic and incident analysis and remote troubleshooting. As a key layer of security, AirDefense Enterprise complements wireless VPNs, encryption and authentication. Using a monitoring architecture of distributed smart sensors and a secure server appliance, the AirDefense Enterprise system provides the most comprehensive detection of all threats and intrusions. Unlike any other solution on the market, AirDefense Enterprise analyzes existing and day zero threats in real time against historical data to more accurately detect threats and anomalous behavior originating inside or outside the organization. The system automatically responds to threats according to appropriate business process and compliance requirements on both wireless and wired networks, making AirDefense Enterprise the industry's most secure and cost-effective wireless intrusion prevention and troubleshooting solution.

AirDefense Personal, the industry's first end-point security solution, provides uninterrupted protection for all mobile employees and their enterprise wireless assets, regardless of location – at work, home, airports or other wireless hotspots. Policy profiles are defined centrally on AirDefense Enterprise and automatically downloaded to each mobile user. If threats are discovered, AirDefense Personal notifies the user and sends the alerts to AirDefense Enterprise for central reporting and notification. This unique solution allows the network administrator to enforce corporate policies and provide complete protection for the mobile workforce, regardless of location.

The **AirDefense InSite Suite** is a collection of powerful tools available today for network architects to design, install, maintain and troubleshoot wireless networks. Tools included in the suite are: **AirDefense Mobile**, complementary to AirDefense Enterprise allows administrators to perform wireless assessments, security audits, locate and manage rogues. **AirDefense Architect** provides complete design and 3D RF simulation of wireless LANs based on building-specific environments. **AirDefense Survey** provides real-time, in-the-field measurements of Wi-Fi RF environments for site-specific surveys.

For more information or feedback on this white paper, please contact info@airdefense.net or call us at 770.663.8115. **All trademarks are the property of their respective owners.**