



# ***Defending the Mobile Enterprise***

## **Overcoming Security Challenges and Evaluating Wireless Threat Management Solutions**

This white paper identifies wireless-enabled security threats to corporate IT infrastructure and explains how laptops and other mobile devices can become an open door to enterprise networks and data. By introducing the necessary components of a comprehensive wireless threat management strategy, this paper details the immediate actions IT managers can take to defend an organization's entire information technology infrastructure from all wireless originated threats. In addition, this paper provides an overview of the issues an IT security manager should be aware of when evaluating wireless threat management solutions and formulating a risk mitigation strategy.

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

## Introduction

The rapid growth and widespread usage of wireless technologies has created significant new security threats to corporate networks and information despite advances in WLAN encryption and authentication. These vulnerabilities must be addressed by all organizations, *whether or not wireless networks are officially deployed*, to meet the stringent security and compliance requirements of today's organizations.

The perimeter of the corporate network is becoming more difficult to define and control. Millions of employees now leave the workplace with volumes of proprietary data stored on laptops or other wireless devices. Adding to the security challenge is the fact that the simple connection of a wireless device to the corporate wired network can open up an entry point into the company's IT infrastructure, accessible by anyone with a wireless device, just as if they were seated at a desk in the office. The problem is further compounded in highly classified environments where cellular phones and other wireless devices can be used to leak sensitive data and in wireless environments, where interference and 802.11n network scalability issues can pose a significant threat to the performance of wireless networks.

This white paper identifies wireless-enabled security threats to corporate IT infrastructure and explains how laptops and other mobile devices can become an open door to enterprise networks and data. By introducing the necessary components of a comprehensive wireless threat management strategy, this paper details the immediate actions IT managers can take to defend an organization's *entire* information technology infrastructure from all wireless originated threats. In addition, this paper provides an overview of the issues an IT security manager should be aware of when evaluating wireless threat management solutions and formulating a risk mitigation strategy.

## Business Mobility: Productivity Gains and Enterprise Risk

Professionals are increasingly realizing the productivity benefits of mobility with on-the-go access to the Internet and corporate resources. While this mobile revolution is an advantage to professionals, it is creating a tremendous security management challenge for CIOs and other IT professionals. Unless remedial actions are taken, mobile devices can become an open door to the enterprise.

## Mobile Workers – Rapidly Increasing

Today millions of employees leave the workplace with volumes of corporate data stored on laptops or other wireless devices. According to IDC, 68% of the U.S. workforce was mobile in 2006 and IDC expects that by year-end 2011, one billion U.S. workers will be mobile<sup>1</sup>. When employees connect to insecure networks—from home, at the coffee house, in the airport—or fail to use wireless security best practices, it can place sensitive data at risk and introduce malicious code to the corporate network.

## Wireless Threats and Mitigation Strategies

Wireless security has improved dramatically since the introduction of IEEE 802.11 in 1997. When the most recent security standard, IEEE 802.11i, is employed, wireless networks can be as secure—or more secure—as many wired network implementations. Networks that are properly configured using wireless Protected Access (WPA2) are virtually impenetrable to common attack scenarios such as man-in-the-middle attacks, offline dictionary attacks or war driving.

However, because wireless technology does not require physical connectivity for data to be transferred, it effectively renders useless many of the conventional means that have traditionally been deployed to secure networks and information. As a result,

sensitive data and proprietary networks have been left vulnerable to both internal breaches and external wireless attack.

### **Rogue Access Points**

When an eager employee—unaware of the dangers—connects a rogue access point to the corporate network to speed wireless connectivity, he can open up an entry point into a company's wired network. Because rogue access points are typically installed in their default mode, proper authentication and encryption are not enabled—making the corporate network accessible by anyone with a wireless device (on a different floor, in the parking lot, or across the street), just as if they were seated at a desk in the office. If discovered by a hacker, a rogue device can place the enterprise at risk and in violation of regulatory policies. To prevent this vulnerability, businesses must have reliable wireless intrusion detection systems in place.

### **Client Misassociation**

By default, the standard configuration of the most popular Windows® wireless clients are set to automatically connect to wireless networks previously utilized. So if a user sets up his laptop to connect to a wireless network called “linksys” or a hotspot called “tmobile”, the computer will automatically connect to any wireless network that comes into range with that SSID—typically without the employee's knowledge—unless the default settings have been changed.

A hacker can penetrate the wired network by luring laptops inside the corporate campus into automatically connecting with a bogus network through an attack known as Wi-Phishing. If this happens while the employee is connected to the corporate network through a wired Ethernet port, the hacker not only has an IP connection to the attacked laptop, but is also in a position to bridge from his fraudulent wireless network to the user's corporate network—at which point the hacker has access behind the firewall. In this case, hackers are given virtually undetectable open access to the corporate network and connected resources.

Traditional wired network intrusion detection or intrusion prevention systems (IDS/IPS) are not capable of detecting this threat because it happens behind the firewall.

To meet the stringent security and compliance requirements of today's organizations, this vulnerability must be addressed by all organizations, *whether or not wireless networks are officially deployed*. Technologies that automatically turn off the wireless adapter whenever a laptop is connected to a wired network port address the security deficiencies in standard Windows® XP and Vista wireless clients and prevent Wi-Phishing. As a further precaution, client policy enforcement software can limit wireless connectivity to the office network whenever it is within range to completely eliminate the possibility of users connecting to a rogue access point or other non-sanctioned wireless networks while at work.

### **Viruses and Malware**

Employees often ignore corporate policies and wireless best practices, including use of firewalls and antivirus protection either because they don't understand the risks involved or perhaps just don't care—favoring efficiency over security. When employees with mobile devices, which have been exposed to the Internet in the wild, return to the corporate campus and connect an infected device to the network, they can inadvertently expose the network to malicious code such as software viruses, Trojan horses or worms. To protect networks, enterprises must be able to secure the endpoints, enforce the presence of endpoint firewalls, and prevent the use of unauthorized devices within the corporate campus.

### **Network Performance Issues**

Network misconfiguration, equipment failures, and increasing bandwidth demands can cause network performance issues. In addition, malicious or non-malicious denial of service attacks can severely impact wireless network performance or block service completely. In reality very few

malicious denial of service attacks are seen in corporate environments. Most denial of service attacks are non-malicious events caused by interference from other non-wireless devices operating in the same band such as cordless phones, microwave ovens and other broadband radio devices. As businesses become increasingly dependent on wireless technologies for voice and data communications, the quality and reliability of wireless services becomes mission critical. Technologies capable of delivering comprehensive site survey information and reliably locating all wireless, cellular and broadband radio devices can help network administrators efficiently operate wireless networks and ensure service continuity.

#### **Ad Hoc Networks and Insecure Access Points**

A wireless network is basically an untrusted, insecure medium, just like the Internet. Unlike a wired network, where information travels through a network cable, a wireless network allows information to travel through a broad, unrestricted area, where the information can be intercepted from the air by anyone sharing the same access point. Employees who use open wireless access points—trusting some random hot spot operator or open access point somewhere—and don't use encryption or VPNs place corporate data at risk to numerous security exploits. To protect sensitive data and meet compliance mandates, client policy enforcement software can ensure that employees only connect to authorized wireless networks and force users to implement adequate security including VPN and encryption.

#### **Cellular Phone Originated Threats**

Cellular phones with built-in cameras and data storage and transfer capabilities introduce new fraud opportunities and threaten the security of proprietary and confidential information. Cellular phones may be used to circumvent IT policies, such as call recording requirements, or as a remote eavesdropping mechanism in highly classified environments, such as government intelligence agencies, research

institutions, and financial trading floors. In addition, cellular phones pose a threat to national security because they can be used to remotely detonate bombs.

Beyond security breaches, cellular phones can interfere with the proper functioning of equipment in hospitals, airplanes and other highly sensitive environments. To protect mission-critical operations, organizations may choose to enforce no-wireless policies or allow wireless in very limited areas. However, establishing policies without a means of enforcement is not sufficient to mitigate the security risks. To effectively enforce no-wireless policies and prevent exposures, enterprises must be able to accurately detect and locate all popular cellular technologies, on all bands.

### **A Growing Problem**

The 2007 CSI Computer Crime and Security Survey asked about "abuse of wireless network" as one of nineteen different kinds of security attack or incident. Seventeen percent of respondents reported this kind of incident, slightly up from the previous year. It ranked ahead of nine other categories. With the widespread usage of wireless technologies, enterprises are no longer in complete control of their IT infrastructure. Every wireless-enabled laptop used within the enterprise has the potential to place proprietary systems and information at risk. With over 300 million wireless laptops in use and over 100 million more being sold each year, businesses are at risk, whether or not they have a wireless network. Robert Richardson, Director Computer Security Institute, states, "We believe enterprise-connected notebooks with wireless capabilities can open potentially serious security holes."

The ability to tighten information and network security controls for both wired and wireless environments is critical for organizations that want to protect sensitive data and transactions, safeguard their brand reputation, and ensure compliance with regulations such as Health Insurance

Portability and Accountability Act (HIPAA), Graham-Leach-Bliley Act (GLBA) Sarbanes-Oxley Act (SOX), and Payment Card Industry Data Security Standard (PCI DSS).

## Using Policies to Minimize Security Risks

Although many organizations have established policies to govern the usage of wireless networks and devices, employees often don't understand the risks associated with not using wireless technologies in accordance with the policies or choose to favor efficiency over security. According to a 2007 study performed by the research firm InsightExpress, 73 percent of mobile users admitted they are not always cognizant of security threats and best practices. More than 25 percent also conceded they either hardly ever or never consider security risks and proper behavior, offering reasons such as "I'm busy and need to get work done" and "It's IT's job, not mine" as justifications.

## The Challenge of Securing the Wireless Frontier

Gaining control of the airwaves and wireless endpoints can be challenging at best as businesses face intense pressure to increase levels of security—driven by regulations and legislation as well as shareholder demands for more effective corporate governance. At the same time, competitive pressures are forcing companies to reduce over all costs and improve operational efficiencies. Disparate technologies, cumbersome user requirements and high costs can make wireless security deployments prohibitive to enterprises despite outside pressures to close security gaps. Adding to the burden is the fact that IT requirements are fluid and influenced by a number of forces as businesses, technologies and threats are constantly evolving.

## The Era of Corporate Accountability

IT departments are challenged by a seemingly endless list of regulatory compliance requirements, industry standards, and security and IT operational best practices. Addressing specific regulatory requirements can be difficult even for the most seasoned IT professional. Instead of being prescriptive, most regulations like HIPAA, SOX, GLBA, and PCI DSS, provide high-level requirements and expect organizations to implement "reasonable and appropriate measures" to protect information. Wireless vulnerabilities are often overlooked or underestimated by IT professionals, especially if the enterprise has a no wireless policy in place, and yet there are many scenarios that may place the enterprise at risk and in violation of regulatory policies for its industry.

## Balancing IT Security and Business Requirements

As wireless technologies continue to proliferate, new wireless vulnerabilities will be exploited. Businesses are left to consider the cost versus benefits of securing data and networks against wireless attacks. Even in a world clamoring for security, the reality of corporate budgets and the necessity of productivity gains dictate the need for clear justification for each and every expense. Often companies must make trade offs between security and productivity as security solutions often inject "speed bumps" in the path employees use to access and exchange data. In the past many enterprises have not been able to justify the deployment of wireless security technologies in non-wireless environments. As a result, sensitive data and proprietary networks have been left vulnerable.

## Operational Inefficiencies

To protect corporate infrastructure against wireless threats, IT departments must be able to monitor networks and detect unauthorized wireless devices, defend systems against wireless-enabled intrusions, and safeguard information stored on laptops in the enterprise and on the road. Historically, implementing a comprehensive solution meant deploying technologies from multiple vendors. The net result was a system that was costly to deploy, cumbersome to manage, and promised only marginal accuracy.

## The Evolution of Standards

Another major hurdle facing businesses is the constant evolution of standards and protocols and their impact on IT infrastructure requirements. In the case of wireless, changes to the 802.11 protocol

have been rapid and numerous. As advancements in protocols are made, otherwise operable systems often must undergo a forklift upgrade to meet increasingly stringent security requirements.

## Evaluating Wireless Threat Management Solutions

Today's next-generation wireless threat management technologies are redefining the costs versus benefits equation. Companies concerned with tightening their security controls and ensuring compliance with regulations are discovering that new comprehensive wireless threat management security offerings are enabling organizations to proactively protect networks and data against wireless-enabled attacks—in an affordable and efficient manner.

## Components of a Wireless Threat Management Solution

To deploy a unified corporate-wide wireless threat management strategy, enterprises require a comprehensive suite of network and endpoint security products that completely addresses all of the security issues related to the widespread use of wireless technology (wireless, cellular and broadband radio).

The solution should protect an organization's *entire* office-based and wireless laptop Infrastructure from all wireless-originated threats to corporate data and networks. In addition, the right wireless threat management solution can promote business efficiency by providing employees a convenient, and yet secure, way to wirelessly access and exchange data from within the corporate campus or from remote locations.

## Wireless Threat Management Solution Capabilities:

### A Useful Framework for Comparison

When evaluating wireless threat management technologies it can be helpful to use a consistent, structured framework to understand, evaluate and select the most appropriate wireless threat management solution from amongst a wide selection of alternatives. The framework presented reflects

not only AirPatrol's years of experience and market leadership in wireless security technologies, but also the additional structure and detail required to make an apples-to-apples, rather than apples-to-oranges, comparison of various wireless threat management technologies.



- Monitor and defend networks against wireless-enabled intrusions and service disruptions
- Safeguard sensitive information by protecting wireless endpoints in the enterprise and on the road
- Efficiently manage network health and endpoints from a single enterprise-wide wireless threat management console
- Leverage investments in existing hardware infrastructure to make wireless security and WLAN deployments affordable
- Accurately detect and quickly mitigate security threats without time intensive

**Table 1. A Consistent, Structured Comparison Framework**

<b>Total Cost of Ownership</b>	<b>Acquisition Cost</b>	What are the initial acquisition costs? This includes all additional hardware, software, servers, services, etc. associated with acquiring the wireless threat management solution
	<b>Deployment Cost</b>	What are the costs to deploy the wireless threat management solution? This includes the network cabling costs, ease of installation, ease of setup and configuration, calibration requirements, training administrators, etc. Does the solution leverage existing investments in infrastructure or require its own dedicate network?
	<b>Operating Cost</b>	What are the ongoing operating costs? This may include costs for replacement (e.g., broken / outdated) sensors; ongoing management; upgrades, etc. How many resources are required to manage the solution? Are there hidden costs, i.e. re-calibration requirements?
<b>Strategic Fit (Corporate)</b>	<b>Relative Security</b>	How secure is the implementation? Is it adequate for the information being protected? Can I control my perimeter and access to the network? Does it meet regulatory requirements (if any) for the protection of information?
	<b>Scope/Completeness</b>	Is the solution capable of identifying all wireless devices and threats (wireless, cellular, and broadband radio)? When used in conjunction with 802.11 protocols, does it secure both wired and wireless networks and endpoints?
	<b>Reliability/Accuracy</b>	Will the solution provide accurate device location information, i.e. can I actually locate a rogue device? Does the solution provide the tools/intelligence necessary to reliably mitigate threats in a time efficient manner?
	<b>User Convenience/Ease of Use</b>	How easy is it for end-users to learn how to use the client interface? How convenient is it for end-users to connect to the wireless networks they need to use, day in and day out? Does the solution improve employee productivity?
<b>Strategic Fit (Systems)</b>	<b>Interoperability/Back-end Integration</b>	Does the solution work natively with multiple WLAN products? How easy is it to integrate with back-end resources or applications?
	<b>Robustness/Scale</b>	Does the wireless threat management solution scale to the degree required now? Three years from now? Things to consider include support for growth needs, updated 802.11 standards (802.11n and 802.11r), convergence of voice and data traffic, etc.
	<b>Future Flexibility</b>	What future options may be available from the selection of this wireless threat management solution (whether you currently intend to use them or not)? What future options might be of interest? Things to consider might include expanded WLAN deployments, wireless VoIP, use of wireless capable cellular phones, etc.

In this framework, there are three high-level categories, each of which can be broken down slightly further for a total of ten basic attributes. Any wireless threat management technology can be compared—in a consistent manner—using this simple framework to compare and contrast various wireless threat management alternatives.

## Total Cost of Ownership

Cost is a critical consideration, but enterprises need to consider *all* the elements of cost. The total cost of ownership for first generation wireless prevention and intrusion detection solutions (WIPDS) were costly because the sensors cost between \$600 and \$1,000 each and required a dedicated network connection, which added an additional \$600-\$800 per sensor in cabling and switch port costs,

bringing the average deployment to about \$6,000 per 10,000 square feet. Threat mitigation strategies depended on resource intensive analysis of packet-level data and ongoing calibration requirements—placing a burden of IT staff and inflating system maintenance costs. New solutions feature a lower cost per sensor, the ability to integrate sensor networks into existing hardwired networks, an intelligent approach to threat mitigation, and automatic calibration capabilities to bring down the total cost of ownership.

## Strategic Fit Corporate

Security is only as strong as the weakest link. When formulating a risk mitigation plan, it is important to address all threats arising out of the proliferation of wireless technologies. After conducting a comprehensive assessment of the risks introduced by wireless technologies, enterprises must identify which wireless threat management strategies will allow them to effectively and reliably mitigate known risks across all wireless channels (wireless, cellular, and broadband radio). By adding cellular and RF broadband detection to the standard wireless location capabilities, enterprises can effectively enforce no-wireless policies or control risks by limiting wireless connectivity to designated areas. To avoid integration issues between disparate technologies, enterprises can benefit by choosing wireless threat management technologies from a single vendor that can provide a total end-to-end solution for all network security,

endpoint security, policy management and interference capabilities needed. Some vendors are also integrating their wireless threat management solutions with popular network security products—enabling seamless deployments in wired environments.

End user acceptance, ease of administration and reliable performance can be equally, if not more important than the technology itself. To quickly and accurately manage wireless threats, network managers need a simplified way to control the perimeter, monitor network health and remediate security issues. Configurable alarm zones can help to minimize false positives and intrusion event alerts that can be sent to cell phones or other email-capable mobile devices can help speed response times. In addition, reliable device location data and the use of firewalls for traffic blocking, can help administrators easily determine whether a security event is malicious and mitigate risks on the fly. Finally, if security interferes with an end-users ability to conduct work efficiently, policies meant to protect the enterprise will be circumvented. Location-based wireless policies can help to control client devices without inhibiting users or slowing performance.

## Strategic Fit Systems

The success of a security method depends on more than just technology—scalability to accommodate growth, and interoperability with existing systems and future plans are all important components to a successful implementation. Whether a solution integrates with and compliments network security measures already in place can be an important consideration. In addition, choosing wireless threat management solutions that support hardware from multiple WLAN infrastructure vendors can provide future flexibility.

Organizations interested in using technologies to enforce a no-wireless policy

today may want to consider whether the solution can be leveraged as the foundation for a WLAN deployment in the future should the decision be made to go wireless. Future flexibility is like having an *option*. Options have real value today, not because you use them today but because they represent something that you could take advantage of sometime in the future. Of course, some options are never exercised—but having options definitely gives you a degree of future flexibility. Because technologies, threats and businesses are constantly changing it is important to anticipate growth and changes over the coming years. Present requirements might include using a WLAN for data traffic only—but as bandwidth capacities increase and technologies evolve, a solution that has the capability to handle the convergence of voice and data network and new 802.11n/r protocols when they are ratified may be

required in the future. Whether or not there are firm plans to use these additional capabilities, the option to use them exists and that provides a degree of future flexibility.

Finally, enterprises that are eager to take advantage of the bandwidth capabilities of new wireless technologies may be surprised to learn that increased throughput could result in clogged central switches and controllers. The high performance capabilities of 802.11n can pose a significant scalability challenge for products that perform encryption and decryption on the wireless switch. Companies interested in deploying WLANs may want to consider the use of firewalls at the perimeter in a distributed model to enable superior network configuration flexibility and almost infinite scalability.

## AirPatrol’s Wireless Threat Management Solutions

AirPatrol’s Wireless Threat Management solutions help build confidence in today’s increasingly mobile world by providing comprehensive protection for business communications, critical information, and IT infrastructure—making it possible for businesses worldwide to mitigate IT risks, support compliance requirements, and improve operational efficiencies.

### Evaluating AirPatrol Products

The following section uses the comparison framework to give an objective assessment of AirPatrol’s Wireless Threat Management solution.

Total Cost of Ownership		
<p>AirPatrol greatly simplifies and dramatically lowers the cost-of-deployment of wireless technology to less than half of the cost of traditional solutions and enables wireless networking technology to be integrated into existing network infrastructure, rather than being deployed as a parallel network with a discrete overlay security strategy. Once deployed, administrators can manage the entire wireless threat environment from a single easy-to-use console that concurrently displays all cellular, 802.11 and broadband radio devices.</p>		
Acquisition Cost	Deployment Cost	Operational Cost
<p>Available as software versus appliance Sensors cost below the industry average</p>	<ul style="list-style-type: none"> <li>▪ Leverages investments in existing network infrastructure to reduce deployment costs</li> <li>▪ wireless sensors can be piggybacked onto existing network infrastructure without dedicated cabling and switch ports</li> <li>▪ Sensors include two Ethernet ports on with full pass-through Power Over Ethernet capabilities to integrate into existing hardwired networks without any cabling and switch port costs and enables sensor networks to be deployed by internal staff</li> </ul> <p>Wireless Locator System automatically calibrates itself during set up without manual intervention</p>	<p>The visual real-time approach to security enables administrators to act quickly and remediate issues without time intensive analytical investigations</p> <p>Automatically adjusts to dynamic wireless environments without manual intervention –eliminating, ongoing recalibration requirements</p> <p>Allows network administrators to efficiently operate wireless networks by providing the user-friendly set of planning tools and interference detection capabilities necessary to deploy wireless networks and ensure service continuity</p> <p>Once deployed, administrators can manage the entire wireless threat environment from a single easy-to-use console that concurrently displays all cellular, 802.11 and broadband radio devices</p>

**Strategic Fit (Corporate)**

AirPatrol's Wireless Threat Management represents the most comprehensive portfolio of wireless infrastructure and endpoint security solutions currently available to deliver a unified corporate-wide wireless threat management strategy that completely addresses all of the security issues related to the widespread use of wireless technology (wireless, cellular and broadband radio).

**Relative Security**

- Monitors the airwaves 24x7 to provide a live enterprise-wide view of network posture at a single glance
- Enables network administrators to restrict access to wireless networks based on location – restoring the most fundamental concept of conventional network security
- Uses industry-standard firewalls at the edge of the network to block unauthorized wireless traffic and protect network infrastructure
- Alerts network administrators in real-time to security threats
- Network administrators can define wireless connectivity policies to control how, when, where and if users can connect to wireless networks.
- Policies can be documented as required to comply with industry mandates

**Scope/Completeness**

- Delivers the most comprehensive portfolio of wireless infrastructure and endpoint security solutions currently available
- Addresses all of the security issues related to the widespread use of wireless technology (wireless, cellular and broadband radio)
- Protect communications, critical information, and IT infrastructure against present and future wireless threats
  - Locates sources of interference to ensure service continuity

**Strategic Fit (Corporate)**

**Reliability/Accuracy**

- Locates all authorized and unauthorized 802.11, RF and cellular devices with an accuracy of 3 to 5 meters
- Uses reliable location data and firewalls for threat mitigation vs. shot gun DNS approach

**User Convenience/ Ease of Use**

- Automatically turns off the wireless adapter whenever a laptop is connected to a wired network port
- Automatically detects and connects to wireless networks and stores personalized profiles so that users can automatically connect to preferred networks without reconfiguring settings each time
- Allows users to instantly set up secure ad-hoc networks and share resources (such as a high-speed connection to the Internet) and data within a workgroup – without requiring a wireless access point

**Strategic Fit (Systems)**

AirPatrol delivers the proven capabilities today's businesses require to protect communications, critical information, and IT infrastructure today and in the future.

**Interoperability/Back-end Integration**

Tightly integrated with various Check Point solutions including the VPN-1 Edge W device, SMART (Security Management Architecture), Integrity™ end-point firewall and SecureClient™ VPN client

Supports a wide range of access points from a variety of manufacturers

**Robustness/Scale**

Supports scalability requirements through a distributed model using firewalls at the perimeter for traffic blocking

Eliminates the scalability limitations of traditional switch-based approaches

**Future Flexibility**

Can be used as an intrusion detection solution in no-wireless environments and easily scales to protect and manage wireless networks

Supports convergence of voice and data

Solution is designed to meet future bandwidth requirements without speed degradation -- Future-ready for new 802.11 standards

## Summary

High-speed wireless networks are transforming the economics and user experience of enterprise computing worldwide. Mobile, real-time access to systems, applications, and information can enable dramatic improvements in employee efficiency, customer service, and organizational agility. Based on an expert understanding of the wireless security and performance issues that plague enterprises and government agencies, AirPatrol delivers the capabilities customers need to confidently deploy, manage and protect networks against present and future wireless threats.

By addressing new security vulnerabilities before they occur, AirPatrol's Wireless Threat Management suite transforms the way the wireless networking can be deployed. Once IT departments gain confidence in their ability to defend hardwired systems against wireless-enabled attacks, they begin to see the real value of wireless technologies. IT departments can demonstrate real ROI by not only securing the enterprise against wireless threats, but also enabling business mobility and reducing the costs of implementing new networks—adding both top and bottom line benefits. For the first time, wireless technology can be deployed as it was originally envisioned, by simply adding low-cost WPA-capable access points to the edge of an existing wired network.

AirPatrol continues to deliver the market-leading advancements customers require to mitigate a broad range of wireless threats—including breakthrough solutions for interference locationing and cell phone detection. AirPatrol's innovations allow enterprises to take advantage of an increasingly mobile world and protect traditional IT infrastructure against wireless-enabled attacks.

## About AirPatrol Corporation

*As the most trusted authority on wireless threats to wired and wireless networks, AirPatrol Corporation delivers the security and network management capabilities today's businesses and government agencies require to solve the industry's most pressing wireless security and network management issues. By offering a comprehensive suite of wireless threat management solutions, AirPatrol enables entities to keep pace with the expanding requirements of a mobile world while complying with pertinent regulations and protecting communications, critical information, and IT infrastructure against present and future wireless threats. Customers and partners include leading network infrastructure and wireless vendors, Fortune 100 enterprises and high-profile government agencies around the globe.*

*For more information about the contents of this white paper, AirPatrol Corporation products or our company, please contact us at [info@airpatrolcorp.com](mailto:info@airpatrolcorp.com) or call us at +1-866-430-4227.*

---

<sup>1</sup> The IDC study, Worldwide Mobile Worker 2007-2011 Forecast and Analysis (IDC #209813)