AIRPATROL

Wireless Endpoint Security

I. Introduction

To enhance productivity and efficiency, employees are increasingly turning to wireless devices and networks to get the job done. The security experts at AirPatrol believe that a defense-in-depth approach to wireless security yields the greatest results, especially when it comes to protecting corporate laptops. Armed with AirPatrol's endpoint security solution, an IT administrator can ensure the proper use of wireless laptops for those users on the go. At the center of AirPatrol's protection suite is its Wireless Endpoint Client software (WEC), a small application that runs as a system service on wireless laptops. WEC protects the laptop by strictly defining how the wireless interface will be used. The policy defining wireless usage can be as flexible or rigid as the corporate security policy dictates. By leveraging Microsoft's Active Directory and AirPatrol's native Wireless Policy Manager (WPM), the Wireless Endpoint Client (WEC) can begin to ease the burden of managing and securing wireless assets.

II. Wireless Policy Manager

Enhanced wireless security policies can also be centrally managed using AirPatrol's Wireless Policy Manager (WPM). WPM is a web based server application that allows wireless security policy to be easily designed and effectively deployed. WPM enables configuration and enforcement of granular wireless usage polices and USB device control capabilities on your managed wireless assets. AirPatrol WPM is available as a stand-alone product and is also offered as a plug-in to McAfee's e-Policy Orchestrator (ePO).

Ease of Deployment

The foundation for building a secure wireless endpoint solution begins with the understanding of three configuration concepts: Users, Groups, and Policy. WPM utilizes existing Microsoft's Active Directory (AD) or McAfee ePO infrastructure to ease the burden of managing a large deployment across the enterprise. WPM can query AD and ePO to build a subscriber list of users that wireless security policy will apply. In addition, AD or ePO can distribute AirPatrol wireless endpoint client software to those laptops which require enforcement of wireless security policy.

Scalability

With ease of use and scalability at the center of its design, a single instance of WPM can manage up to 10,000 deployed endpoints. Larger managed installations (50,000 or 100,000 deployed endpoints) are feasible by using redundant WPM servers in a load-balanced configuration.

Security

All of AirPatrol's products undergo rigorous software security testing. All the underpinnings of WPM are security hardened to greatly reduce the attack surface of the application. Moreover, all network communications between WPM and wireless endpoints are fully encrypted. Once installed, the IT administrator simply opens a secure HTTPS connection to WPM using a standard web browser. Once successfully authenticated, the task of designing wireless security policy is underway. Just as HTTPS is used to secure connections between an administrator's web browser and WPM, the same secure SSL based communications paradigm is used for all communications between WPM and wireless endpoints.

This ensures the confidentiality and integrity of the policy data as it travels over the network. WPM based wireless security policies include:

- **AirSafe** – Automatic, out-of-the-box protection against multi-homing. Anytime a laptop's wireless interface (802.11 card or cellular broadband modem) is active, and a wired Ethernet connection is attempted, WEC automatically disables the wireless connection. This completely mitigates the possibility of bridging a potentially untrusted wireless network with a trusted corporate wired LAN. In addition, this protection is carried over into the realm of cellular broadband connections and traditional 802.11 networks. Should the system detect an active cellular broadband connection, it will automatically disable the wireless adapter.

- **Virtual Wi-Fi Control** – Windows 7™ Virtual Wi-Fi works by converting a single physical 802.11 Wi-Fi network interface card into multiple Virtual Wi-Fi devices. AirPatrol WPM addresses Virtual Wi-Fi security risks by enabling IT Administrators to enforce group-based Virtual Wi-Fi policies.

- **802.11 Infrastructure Authentication policy enforcement** – WPM allows the system administrator to define minimum levels of security that must be used when connecting to wireless networks.

- **802.11 AdHoc Authentication policy enforcement** – WPM allows the system administrator to set minimum levels of security used or completely disable the use of AdHoc wireless networks.

- **Virtual Private Network (VPN) policy enforcement** – The ability to force the use of a VPN within a specified amount of time. If a VPN connection is not made within the specified interval, wireless network connectivity is terminated protecting the laptop from a potentially unsecure wireless network.

- **Connection Exceptions** – Allows the administrator to create either a list of permitted or disallowed wireless networks. The network SSID must be present (white list) or not be present (blacklist) in order to allow wireless network connections.

- **Endpoint Firewall** – The ability to enforce the use of a host-based endpoint firewall prior to allowing wireless network connections.

- **Location-Aware** – The ability to predefine a list of trusted, preferred wireless networks that will be made exclusively available for connection when their presence is detected. This ensures connectivity control whenever corporate laptops are within range of corporate wireless access network while preventing accidental or intentional wireless connections to uncontrolled (rogue) access points residing off premise.

- **USB Device Control** – Provides the capability to control what types of USB devices can connect to the managed laptop. For example, the user may be allowed to connect a USB capable mouse while USB mass storage devices are disallowed.

- **Secure Passphrase Distribution** – WPM enables administrators to easily and securely distribute SSID passphrases to users, mitigating the risk that comes with writing passphrases on paper or distributing in emails. Also, passphrases are hidden from end users, preventing accidental SSID passphrase loss.

III. System Requirements

Wireless Endpoint Client (WEC)

Each endpoint managed WPM must have an installed version of the AirPatrol Wireless Endpoint Client (WEC). Once installed, the overall footprint and processor consumption of WEC running on a laptop or wireless workstation is minimal. The installed package uses only 16MB of system memory along with 10 MB of hard disk space. The host platform running the WEC client must meet the following minimum requirements:

- 1000 MHz Pentium class machine or better
- 128 MB of RAM or higher
- Ethernet 10/100 Network Interface Card (NIC)
- NDIS 5.1-compliant wireless adapter and driver
- Microsoft Windows® XP (32 bit only), Microsoft Windows® 7 (32-bit and 64-bit)

Wireless Policy Manager (WPM)

The server hosting WPM must meet the following minimum requirements in order to manage up to 10,000 WEC endpoints:

- Quad Core 2.6 GHz Pentium Class Processor or better
- 4 GB of RAM or higher
- 10 GB of hard disk space or greater
- Microsoft Windows® Server 2008 R2

IV. Summary

At AirPatrol, we believe that wireless and security are not mutually exclusive terms. Armed with the proper tools, IT departments can effectively manage and mitigate wireless risks while supporting all the benefits that wireless networking offers.

AirPatrol's Wireless Policy Manager plays an integral part in any organization's approach to enforcing wireless security policy. Whether an IT department is responsible for only small number of wireless laptops or tens of thousands of wireless laptops, WPM facilitates the secure use of these valuable assets.

About AirPatrol Corporation

AirPatrol Corporation offers an end-to-end suite of location-based mobile and wireless enterprise endpoint security solutions that enable businesses and governments to keep pace with the expanding requirements of a wireless world. AirPatrol delivers the capabilities required to confidently deploy, monitor, manage, empower and protect enterprises 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 products or our company, please contact us at info@airpatrolcorp.com or call us at +1-866-430-4227.