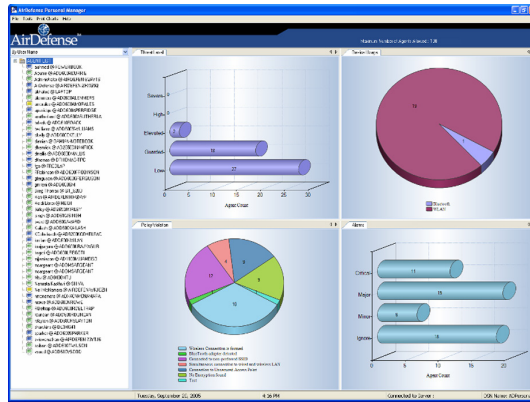




# MOTOROLA AIRDEFENSE Personal™ - Mobile Workforce Protection

Wireless Protection Anywhere



**BENEFITS**

Extends The Wireless Security Perimeter To Mobile Users

Comprehensive Detection Of Wireless Device Misconfigurations For Mobile Users

Supports All Known Wireless Network Adapters Including 802.11, EVDO, 3G, GPRS, HSPDA, And WiMax

Stop Probing Stations And Modem Use In A "No Wireless" Environment

Detection And Enforcement Of Windows Zero Configuration Client Settings

An industry first, Motorola AirDefense Personal™ enforces corporate policies for all types of wireless networks, including Wi-Fi, EVDO, 3G, GPRS and many more. Motorola AirDefense Personal protects the mobile workforce from the wireless-specific risks that could expose private data and confidential transactions. Many cities across the world are now in the process of creating a wireless access blanket in city areas; every desktop could potentially connect to this network if they have a wireless adapter. Motorola AirDefense Personal is a software agent that runs on Windows PCs and monitors for malicious or accidental wireless activity, as well as wireless device misconfigurations that may cause security exposures or policy violations. This solution complements personal firewalls and host-based IDS systems that don't protect the client against wireless attacks.

vulnerabilities of mobile stations at the edge of the network. Motorola AirDefense Personal can also be deployed in enterprises to stop ad-hoc usage, bridging and probing stations.

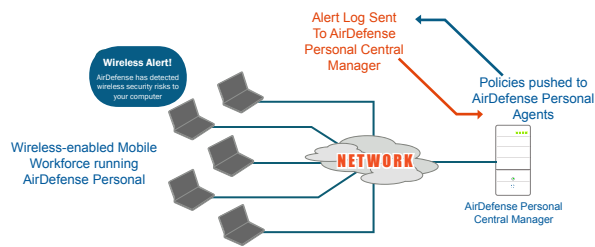
Multiple Motorola AirDefense Personal agents can be managed centrally using the Motorola AirDefense Personal Central Manager. Policy profiles that are defined centrally can be automatically downloaded to each mobile user or group of users. If threats are discovered, Motorola AirDefense Personal notifies the user and sends the logs to the Central Manager for centralized reporting & notification, enforcement of corporate policies and complete protection for the mobile worker, regardless of location. The Motorola AirDefense Personal Central Manager is fully integrated into Motorola AirDefense Enterprise, the industry's most advanced wireless IDS/IPS solution.

Motorola AirDefense Personal offers protection from a broad and growing set of new risks that directly target vulnerable wireless users, unobtrusively notifies the user when risky activity occurs or mitigate the risk entirely by proactively disabling the wireless connection. The data collected from Motorola AirDefense Personal can also be used by the network administrator to gain knowledge of the network usage patterns of mobile employees. Historical and current threat assessment can then be used for setting custom wireless policies that can automatically mitigate the risks of wireless

## SPECIFICATION SHEET

### MOTOROLA AIRDEFENSE

PERSONAL™ - MOBILE WORKFORCE PROTECTION  
Wireless Protection Anywhere



### AIRDEFENSE PERSONAL INTERGRATED INTO AIRDEFENSE ENTERPRISE

## Risks & Threats Identified

### Risky configuration

- Ad-hoc mode enabled
- Bluetooth enabled
- Bridging turned on

### Risky WLAN connectivity

- Non preferred SSID
- Blacklisted SSID
- Connected to insecure access point
- Simultaneous wired & wireless connection

### Insecure communication

- No VPN
- No encryption

### Suspicious WLAN settings

- More than one WLAN card
- Soft AP detected

### Suspicious Behavior

- AP Phishing (Hot Spot Evil Twin)
- Station probing for non-preferred SSID

For more information on Motorola AirDefense Solutions, visit us at [www.motorola.com/airdefensesolutions](http://www.motorola.com/airdefensesolutions)



**MOTOROLA**

[motorola.com](http://motorola.com)