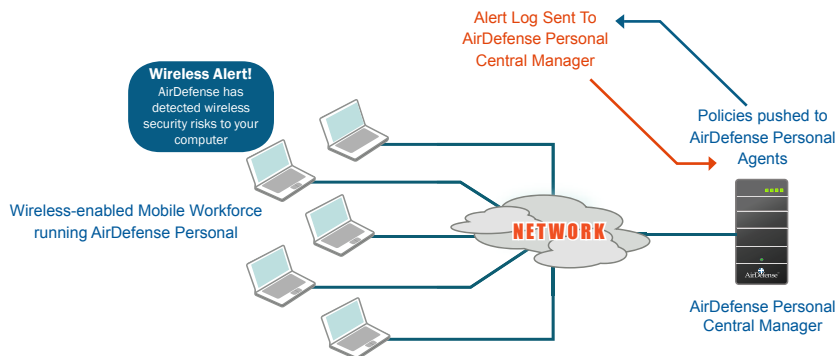


WIRELESS PROTECTION ANYWHERE

An industry first, AirDefense PersonalTM enforces corporate policies for all types of wireless networks, including Wi-Fi, EVDO, 3G, GPRS and many more. 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. 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.

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

Multiple AirDefense Personal agents can be **managed centrally** using the **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, 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 AirDefense Personal Central Manager is fully integrated into AirDefense Enterprise, the industry's most advanced wireless IDS/IPS solution.



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

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