DATASHEET

AirTight® Mobile

Your workforce is mobile. Your security must follow.

Protecting the Mobile Edge

An increasing number of enterprises are relying on a mobile workforce that needs to stay connected with the corporate wherever they are on the road – hotels, airports, restaurants, coffee shops, or working from home or a remote office. With the bring your own device (BYOD) culture, the workforce is increasingly using a mix of corporate owned and personal devices – laptops, smartphones, and tablets.

As these devices move in and out of corporate premises, they connect to multiple known or trusted and untrusted networks. To avoid these devices from getting compromised wherever they go and in turn to prevent them from compromising, albeit inadvertently, the corporate network security, the security perimeter must move with these devices.

Mobile Security Perimeter

AirTight Mobile gives you an "always on" mobile security perimeter. Once installed as a lightweight software agent, it gives IT security administrators the visibility into how the devices connect or behave and more importantly, enforce corporate security policies 24/7 wherever the devices go .

Secure Wi-Fi Usage

Almost every laptop and mobile device today comes with Wi-Fi built-in. And with an omnipresence of Wi-Fi networks – at home, in the office and as hotspots on the road – Wi-Fi is becoming the primary mode for Internet access at the edge. AirTight Mobile can protect mobile devices by proactively blocking Wi-Fi misuse or Wi-Fi hacking attacks, such as Café Latte that target the Wi-Fi client. The AirTight Mobile agent can enforce policies such as:

- Block unsecure Wi-Fi connections, e.g., Open, WEP, Ad-hoc networks;
- Enforce VPN usage over an untrusted network;
- Delete unused SSIDs from the cached list to prevent inadvertent probing and Wi-Fi connections; and
- Control device behavior based on the context of location, e.g., home, work, away.

Location-sensitive policies can control the behavior of mobile endpoints differently depending on whether they are connected to the enterprise network, home network or an untrusted independent network.

Mobile Connection Management

AirTight Mobile can manage the multiple communication and storage interfaces on laptops, smartphones and tablets. Enterprises can control simultaneous use of any combination of these interfaces or simply enforce a "one-interface-at-a-time" policy to prevent bridging or tethering of interfaces, which could compromise

Key Features

- Extends your security perimeter to your mobile workforce wherever they go
- Enforces secure Wi-Fi and VPN usage
- Policies in the context of the location or network, e.g., home, office, public area
- Granular management of connections and interfaces
- Prevents network bridging or tethering
- Secure BYOD onboarding
- Centralized deployment, management and reporting
- Constant monitoring and endpoint policy enforcement

Supported platforms:

Windows

XP, Vista, 7 and 8

iOS

iOS 4 onwards

android

Android 2.2(Froyo) onwards

AirTight NETWORKS

the enterprise network security, for instance, by sharing access to the enterprise Ethernet LAN to unauthorized users or devices over Wi-Fi.

AirTight Mobile agent can enforce policies such as:

- Control device interfaces: Wi-Fi, Bluetooth, 3G/4G, Ethernet, USB, Firewire, IrDA, mass storage devices, and modems;
- Prevent unauthorized access to the enterprise network via bridging; and
- Block mobile hotspots on smartphones and tablets.

Secure BYOD Onboarding

AirTight Mobile seamlessly integrates with AirTight Wi-Fi and WIPS products, enabling a fully automated endto-end enterprise mobile device onboarding and security solution.

The AirTight Mobile agent can be leveraged to implement enterprise network access control over Wi-Fi. For instance:

- As an additional method (e.g., over and above WPA2/802.1x) to authenticate devices;
- To onboard personal mobile devices by allowing them to download and install the agent;
- To automatically classify devices with no agent as unapproved and block their enterprise network access.

Centralized Management

AirTight Mobile agents can be centrally deployed across all corporate Windows devices using common software distribution and management systems such as Microsoft SMS, Altiris and McAfee ePO. In case of mobile devices, the agent can be downloaded and installed from the Android app market, iTunes app store, or as a part of the package delivered from a mobile device management (MDM) server. For BYOD onboarding, the agent could be hosted on a captive portal where user devices are redirected when they connect over Wi-Fi, and from where they can download a pre-configured agent.

From a single management console, network administrators can manage security profiles and push policies, generate or schedule consolidated reports on device usage, wireless security incidents and risk levels.

AirTight® NETWORKS
Secure Cloud-Managed Wi-Fi

AirTight Networks, Inc.
339 N. Bernardo Avenue #200, Mountain View, CA 94043
T +1 (877) 424-7844 T (650) 961-1111 F (650) 961-1169
www.airtightnetworks.com | info@airtightnetworks.com

Datasheet: AirTight Mobile [Doc ID: ATN-DS-1013-004-00-EN]