

AIR STOP®

AirStop® Endpoint Security Software

Defending Against Threats You Can't See

In many cases a public wireless network provides coverage not only for public areas but also for corporate offices. This creates severe security risks, especially when numerous corporate and public networks overlap in a densely populated area.

Two major security concerns with large number of WI-FI hotspots sprouting everywhere:

1. Wireless Bridging
2. Use of unauthorized WI-FI adapters in corporate environment

What is Wireless Bridging?

A corporate device (e.g. laptop) while connected to the corporate network, may connect to a public wireless network via a different adapter at the same time. A potential attacker could gain access to the restricted corporate network via the laptop, thereby compromising the security.



Figure 1 - Wireless Bridging

A proper security solution should ensure:

- Corporate laptops and desktops can only log on to the secure corporate network
- The Corporate Network is not compromised due to "Wireless Bridging" via authorized laptop and desktop computers

In addition, fixed and removable storage devices such as USB flash memory sticks and writable CD/DVD drives constitute another potential data leak which must be protected.

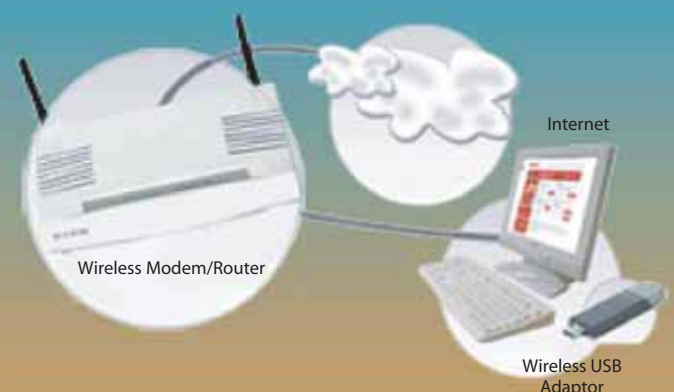
Configuration

Client

The administrator configures the AirStop Client by prioritizing the available communications adapters and storage devices on a typical machine. Once the security policy is finalized, the software can be distributed using Microsoft SMS or installed as part of the login process. AirStop is password protected and cannot be changed or removed even by users with local administrative rights.

Server

The AirStop Server collects data from all AirStop clients. The web based solution provides administrators with near real time information regarding adapter usage across the enterprise or historical data on specific adapter over time. All information can be viewed using a standard browser.





Simple and Effective Solution

AirStop prevents simultaneous operation of communications adapters thereby eliminating possibilities of unauthorized bridging. It also protects against leaks to USB storage devices and disk drives. The software gives IT departments the ability to define and enforce endpoint security policy and cannot be disabled by end users.

Features

- **Automated**
Senses primary communications adapter and disables others
- **Secure**
Prevents simultaneous operation of multiple adapters
- **Transparent**
Background operation is transparent to end users
- **Configurable**
Administrator defined dynamic security policy enforcement
- **Protected**
End users cannot remove or reconfigure the software
- **Dedicated**
End users can only log on to specific corporate wireless networks

Specifications

- **Client OS:** Windows XP
- **Hardware:** All leading laptop
- **Supported Devices:** LAN, WLAN, 3G/Cellular, Bluetooth, Fax/Modem, Firewire, USB flash memory, CD/DVD/Floppy drives

AIR STOP is a product of Code Red Systems Ltd, distributed by
PCS Security Pte Ltd.