

## Extending CyberGatekeeper Policy Enforcement to Wireless LANs

PARTNER SOLUTION BRIEF



infoexpress airespace

### InfoExpress Selects Airespace Wireless Enterprise Platform as Integration Partner

Although the wireless LAN (WLAN) has demonstrated significant boosts in employee productivity and communication, it has also introduced new security risks to an enterprise. Wireless endpoints are not only vulnerable to the same viruses and worms that affect devices on wired corporate LANs, but they are exposed to additional security threats when used in untrusted WI-FI hotspots, such as those found in airport terminals, hotels, libraries, restaurants and coffee shops, and even sports stadiums. Switching between these untrusted sites and the user's trusted company network increases the likelihood of an infection that can be rapidly spread to other devices on the network. Unless corporate security policies and tools are updated, enforced and monitored on all wired and wireless endpoints, then the risk of serious network problems will continue to plague organizations.

In order to provide full network security protection solution, InfoExpress extended the comprehensive endpoint policy enforcement capabilities of its CyberGatekeeper family to include wireless LAN connections. InfoExpress selected Airespace and its popular Wireless Enterprise Platform as the technology integration partner for providing policy enforcement in a combined LAN and WLAN environment.

An integrated InfoExpress/Airespace solution has many advantages to enterprises that want a seamless and secure LAN and WLAN environment:

- Seamless LAN and WLAN protection, from client to infrastructure, from a single product
- Centralized policy management for all LAN and WLAN endpoints
- Works with existing LAN and Airespace Wireless Enterprise Platform – no upgrades required
- Continues to monitor the security level of devices in real-time for ongoing protection
- Minimal hands-on intervention and highly transparent to users
- Strengthens security for all user types, including office employees, mobile workers, telecommuters, contractors and partners, and suppliers
- Minimal bandwidth and performance overhead
- Works with all wireless authentication and privacy schemes

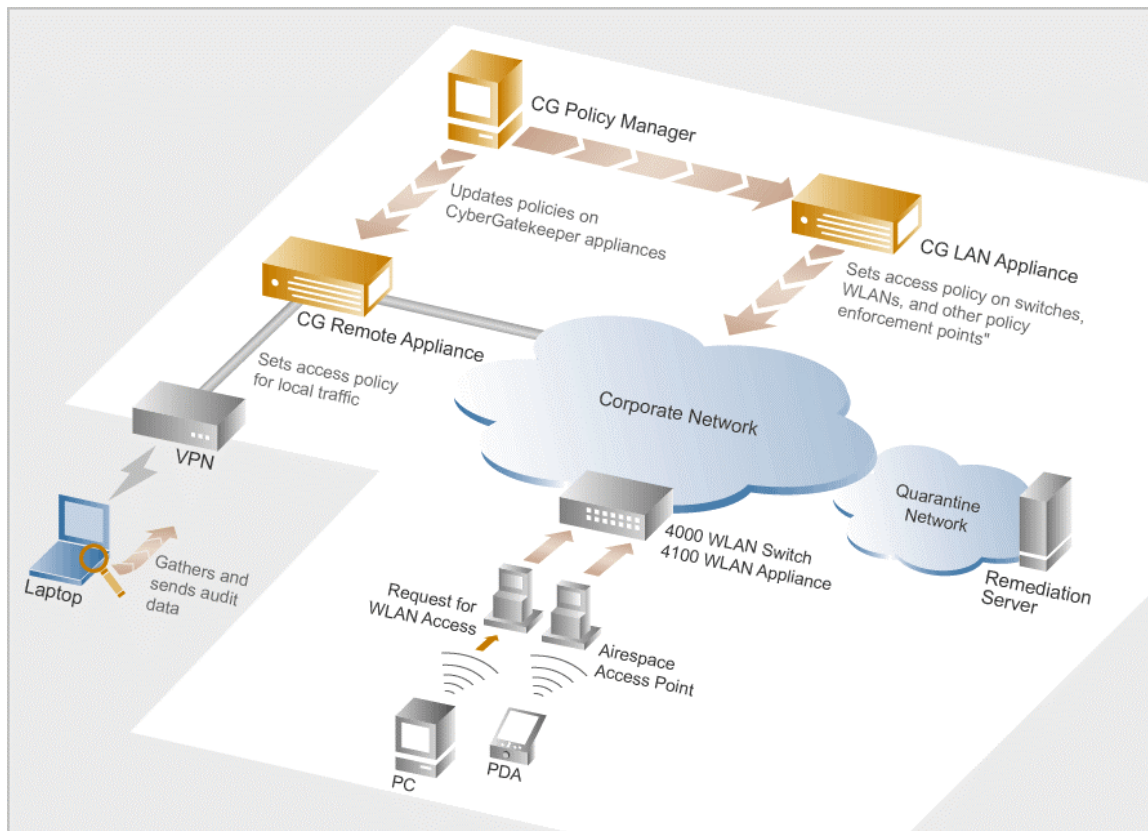
The integrated solution adds extensive endpoint integrity checking to the wireless security arsenal to ensure that only policy compliant and non-infected end user devices are allowed access to the Airespace Wireless LAN. CyberGatekeeper issues integrity checks for:

- Endpoint system configurations, including operating system updates and patches
- Presence of up-to-date anti-virus, personal firewalls and other key applications
- Unauthorized use of various programs and applications such as peer-to-peer software
- The joint solution also includes the following real-time capabilities:
  - Rogue AP detection, location, and containment
  - Ad-hoc containment
  - 802.1X authentication
  - WEP, WPA, and WPA2 encryption
  - IPSec termination, including “Follow ME VPNs” that roam with wireless clients
  - Signature detection for RF-related attacks

## How it Works

---

Administrators take advantage of the centralized CyberGatekeeper Policy Manager to define and create and define security policies. When a wireless client attempts to gain access to an Airespace wireless network, the device is quarantined while the Airespace system queries the CyberGatekeeper LAN product (via custom designed Application Programming Interfaces). CyberGatekeeper scans the endpoint device to ensure that it is compliant with pre-established security policies. If it passes the check, CyberGatekeeper notifies the Airespace WLAN system, which then allows the device to access the network (assuming other authentication, authorization and access criteria are successfully met). If it fails, then the system must be remediated per the policy. Endpoints requiring patches or updates can be automatically configured to have the fix quickly installed, or the users can be directed to a Web page where necessary fixes can be installed with a few clicks. The CyberGatekeeper endpoint policy enforcement process ensures that networks remain secure while business activities continue with virtually no interruption.



The integrated InfoExpress/Airespace solution can be configured to perform checks every time a client attempts to access the network. If a host fails one of these ongoing checks, that device is immediately quarantined by the Airespace WLAN system pending future action