



Alliance solution  
brief

## HP ProCurve and AirTight Networks

### SpectraGuard Enterprise

Proactive network  
protection from  
current and emerging  
wireless threats

### The challenge

As wireless technology proliferates in the enterprise, “wired” network security investments are insufficient to protect the enterprise from wireless vulnerabilities. Knowing what wireless devices are in the air and which ones actually pose a threat is paramount to defining and enforcing a wireless security policy. Organizations face the following challenges when addressing their wireless security:

- Lack of visibility into both local and remote offices
- Lack of understanding of which wireless devices really pose a threat
- The inability to physically block, locate, and remove unauthorized wireless devices
- Difficulty maintaining compliance with regulatory and internal security standards
- Lack of IT resources and expertise to manage their wireless security

The inability to address these issues prevents organizations from leveraging wireless technology to improve business productivity while securing sensitive data.

## How HP ProCurve and AirTight Networks help you meet the challenge

The HP ProCurve Open Network Ecosystem (ONE) provides an open-standards networking platform to ensure only tested and certified applications are able to run on your network and you get the security you need for your network. ProCurve ONE delivers a choice of applications—so you get the most business value from your network.

ProCurve ONE alliance partner AirTight Networks offers enterprises an integrated wireless security solution designed to protect the enterprise from current and emerging wireless threats on the HP ProCurve ONE Services zl Module.

Centrally managed, the AirTight Networks solution correlates all wireless devices with their associated wired networks to prioritize threats and automate the enforcement of wireless security policies. The solution consists of a centralized server that operates on the HP ProCurve ONE Services zl Module and AirTight Networks sensors. The sensors are utilized to monitor and protect the wireless airspace from threats.

The solution provides the network administrator with a clear view of the wireless airspace on a continuous basis. As threats to the wireless network emerge, the system notifies the network administrator. The AirTight Networks system also can be configured to provide on-demand or regularly scheduled reports that detail the threats seen in the wireless airspace and provide an inventory of all access points and devices.

The AirTight Networks system is designed to not only report on threats observed, but it can also shut down threats as they occur. In addition, the solution can prevent corporate-authorized wireless clients from inadvertently connecting to unsecured external access points from neighboring networks. The AirTight Networks solution not only protects the wireless network from unauthorized access, but it also produces reports to aid in documenting compliance with network security requirements.

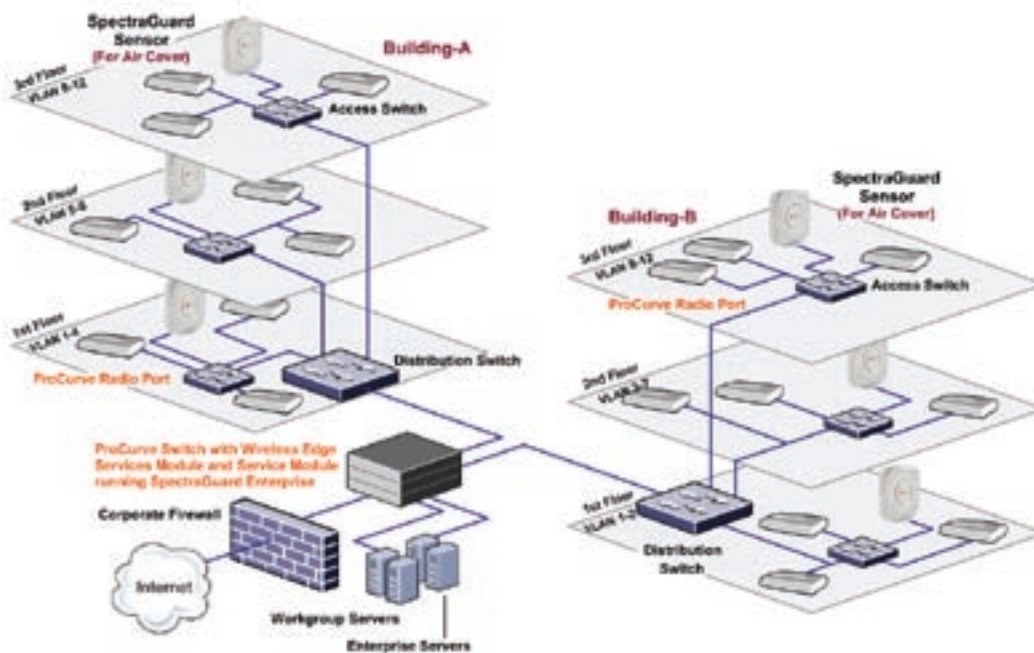
This WLAN-independent security solution uses the latest IEEE 802.11n technology to protect existing IEEE 802.11a/b/g wireless networks from existing 802.11n threats and requires no upgrade when customers are ready to migrate to 802.11n wireless LAN infrastructure.

The solution enables customers to:

- Improve the security of their WLAN infrastructure
- Enforce corporate Wi-Fi security policies (i.e., Wi-Fi security best practices or a no Wi-Fi policy)
- Simplify documentation of network security procedures compliance reporting and adherence
- Define and administer Wi-Fi guest access policies
- Monitor remote locations for wireless vulnerabilities
- Reduce the operational overhead of supporting and managing an additional security solution

With wireless breaches on the rise, organizations are looking for cost-effective and reliable ways to minimize their vulnerability to wireless threats. AirTight Networks and HP ProCurve provide an automated and comprehensive approach to detecting, blocking, and locating wireless threats using a cost-effective blade architecture.

## Solution architecture



## Solution features

- **Comprehensive wireless intrusion detection and prevention:** protection against a wide variety of existing and emerging security threats with one of the most accurate classification engines in the industry
- **Simplified regulatory compliance reporting:** on-demand, user-friendly predefined reports for regulatory standards (such as PCI, SOX, HIPAA, DoD, GLBA, etc.) with drill-down capabilities
- **Precise location tracking:** locates and displays any unauthorized (rogue) access point or client on the floor map for quick removal, provided within 15-foot accuracy
- **Alerting and notification:** Live Event Architecture reduces repetitive and superfluous events, prioritizes threat response, and provides comprehensive forensic data for incident analysis
- **Remote management, monitoring, and troubleshooting:** allows analysis and resolution of remote wireless network issues from a central location

## Solution benefits

- **Comprehensive monitoring and protection against wireless security threats:** blocks all unauthorized access and rogue traffic without disrupting authorized wireless communication
- **Protection of confidential business data:** wireless protection for corporate networks, making sure business data does not leak out of the corporate network through the wireless medium
- **Compliance with data security standards:** simplifies the task of both internal and external regulatory audits, providing user-friendly predefined reports for regulatory data security compliance standards
- **Investment protection:** automated, “lean back” or easy-to-administer WIPS products reduce customers’ operating costs by requiring minimal administrator intervention
- **Protection against brand erosion:** protects you from inadvertent leakage of customer or business data through wireless that can lead to brand erosion



## Solution components

- **Sensors:** monitor wireless activity, perform local analysis, and report summary information to the server securely using industry-standard AES encryption.
- **Server:** collects wireless and wired activity reports from sensors and network detectors for aggregation, correlation, storage, and display on Web-based management console. The SpectraGuard Enterprise server software is operated on the HP ProCurve ONE Services zl Module in a ProCurve switch.
- **Web-based management console** or a **network management console**

## Why HP ProCurve and AirTight Networks?

HP ProCurve ProActive Defense security solutions allow you to proactively protect, detect, and respond to threats to minimize risks. Our security technologies are built into our products and are interoperable with third-party products, giving you a choice of the best solutions to maximize your IT investment. ProCurve centralized management capabilities reduce the overall complexity of managing your network security.

Rated "Positive" in consecutive Gartner Marketscope reports on Wireless Intrusion Prevention, AirTight Networks SpectraGuard is an ideal fit for HP ProCurve customers looking for strong wireless security and rapid deployment with reduced overhead for setup and configuration. SpectraGuard Enterprise

delivers comprehensive protection against a wide variety of existing and emerging security wireless threats including rogue APs, misconfigured APs, denial-of-service attacks, and WEP cracking attacks. It is built on a best-in-class classification engine that automatically and accurately scans, classifies, and blocks all wireless security threats without requiring manual intervention.

## What is HP ProCurve ONE?

Businesses are continually seeking ways to improve competitiveness and manage costs. You need to enable new applications to support the business while addressing cost and network complexity. Today, you're forced to choose between integrating multiple appliances through open standards or being limited to a sub-optimal end-to-end solution from a single vendor.

HP ProCurve's Open Network Ecosystem (ProCurve ONE) allows you to choose from a selection of market-leading applications and to integrate them with your network, having the confidence that the solution has already been pre-tested. Should you run into an unforeseen problem, ProCurve's support team can provide fault-isolation assistance, and in the case of complex interactions will work closely with our alliance partner to isolate the cause of an issue and propose a resolution plan.

To find out more about the joint HP ProCurve and AirTight Networks SpectraGuard Enterprise solution, visit [www.procurve.com/one](http://www.procurve.com/one)

## For more information

To learn more about HP ProCurve Networking, please visit [ProCurve.com](http://ProCurve.com)

To learn more about AirTight Networks, please visit [www.airtightnetworks.com](http://www.airtightnetworks.com)

© Copyright 2009 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

4AA2-3937ENN, January 2009

