MarketScope for Wireless LAN Intrusion Prevention Systems, 1H06

Gartner RAS Core Research Note G00138790, Rachna Ahlawat, 24 May 2006 R1864 09052006

This market will double in size in 2006 as more organizations look to tighten the security of their wireless LANs. Of the seven vendors we assess, two merit a positive rating: AirTight Networks and Network Chemistry.

WHAT YOU NEED TO KNOW

The choice between an integrated and an overlay system for wireless LAN (WLAN) intrusion prevention systems (IPSs) depends on whether wireless networking capabilities exist in the enterprise, the type of WLAN infrastructure deployed and the level of monitoring required. While WLAN infrastructure vendors offering third-generation products (coordinated access points [APs] and controllers) have the capability to detect intrusions on the wireless network, the monitoring and intrusion management capabilities of their products are somewhat limited. For example, integrated solutions today do not offer compliance reporting. On the other hand, overlay vendors are able to monitor networks full time and can generate various industry-specific compliance reports for auditing purposes, but require additional hardware components.

Use the individual vendor ratings given in this MarketScope, together with the following classifications, to determine an optimum solution for your company:

- **"No wireless" policy.** Such a deployment favors overlay solution vendors, especially if an enterprise has no plans to deploy a WLAN.
- **WLAN deployed and using Wi-Fi Protected Access 2 (WPA2)-certified WLAN products, but wireless intrusion capabilities are required to monitor illegitimate users and denial of service attacks.** Basic WLAN infrastructure components could provide "good enough" WLAN IPS.
- **WLAN infrastructure (APs or client devices) does not support latest security standards.** Overlay solutions will help overcome security weaknesses till the enterprise migrates to a more secure authentication and encryption mechanism.
- **WLAN in some locations but "no wireless" in distributed branch offices.** An enterprise can choose either option. Choosing an integrated option will allow the enterprise to use the same hardware for WLAN access in the future, but this may turn out to a be a more expensive solution if there are no plans to ever provide WLAN access in branch offices.

We recommend that, while selecting wireless IPS products, enterprises should carefully consider an 802.11n upgrade path, otherwise the primary useful life of the equipment will be less than two years.

MARKETSCOPE

The market and products for WLAN IPS are in an embryonic phase.

Many companies rely on integrated wireless intrusion prevention capabilities in basic WLAN infrastructure components from vendors such as Cisco and Aruba. The market is growing rapidly for point solutions as well, and certain vertical markets, such as finance, retail and government, are also considering overlay wireless IPSs from vendors such as AirDefense, AirMagnet, AirTight, Network Chemistry and Newbury Networks.

This MarketScope analyzes the recent performance of the seven vendors serving this market that meet our criteria, and it rates each based on our vendor-rating definitions. We also provide an overall market rating using the same definitions.

The wireless intrusion prevention market is evolving. Several vendors have improved their offering by providing solutions in the areas of:

- Pre-deployment planning: site surveys for sensor placement.
- Rogue and misconfigured AP detection.
- Prevention of denial of service attacks over the air.
- Location tracking.

- Post deployment: integration of site plans with ongoing security management.

Wireless IPSs provide an additional layer of security to an enterprise. A WLAN IPS seeks to ensure that only authorized devices (APs and wireless clients) participate in an enterprise's wireless network. Most wireless networks carry a variety of traffic types, of differing characteristics and importance. Many organizations want to protect their radio frequency (RF) environment from intruders and interfering external radiators. Given that wireless is a shared medium, and it is relatively easy and cheap for employees and visitors to set up small wireless networks, enterprises must consider deploying a wireless IPS to detect and mitigate rogues and prevent denial of service attacks. This can prevent illegitimate users from accessing the network and restrict employees from accidentally associating with rogue APs.

Market/Market Segment Description

Wireless IPSs operate at the Layer 2 (data link layer) level of the Open Systems Interconnection (OSI) model. They can:

- Detect the presence of rogue or misconfigured devices and prevent them from operating on enterprise networks.
- Scan radio frequency media for denial of service and other forms of attack.
- Help organizations enforce WLAN security configuration and access policies.

Inclusion and Exclusion Criteria

To help organizations with their WLAN IPS needs, Gartner has assessed vendors that offer overlay WLAN IPSs, as well as WLAN infrastructure (APs and traffic controllers) vendors that have integrated WLAN IPSs into their WLAN infrastructure components.

As this market develops, we expect WLAN infrastructure vendors to improve their integrated solutions to match the capabilities of overlay solution providers. Gartner also expects wired IPS vendors to integrate wireless intrusion prevention capabilities into their product suites. This document looks at the solutions that are available in the market today, excluding wired networking vendors that may be offering just a few components of WLAN IPS. We may consider adding them in future updates if their capabilities match those of the vendors included in this report.

To be included in this MarketScope, vendors' products must, at a minimum, offer rogue detection (rogue APs, clients and ad hoc networks), monitoring of airwaves for denial of service attacks, quality-of-service enforcement or spectrum optimization (some level of integration between pre-deployment planning tools with ongoing management).

In this, Gartner's first MarketScope on this topic, we concentrate on vendors with measurable market share and suppliers with broad capabilities that have generated interest among Gartner's end-user clients. A number of vendors that meet our formal inclusion criteria (described below) are excluded because they have yet to achieve enough market penetration – they include Highwall Technologies and ManageEngine.

Only original equipment manufacturers (OEMs) have been included in this report.

Rating for Overall Market/Market Segment

Overall Market Rating: Positive

We rate this market as "positive," because there will be strong demand for wireless IPS products to improve the security of wireless networks even further. Several established vendors are offering products either on their own or in partnership with startups. In addition, vendors, both established and new, are continuing to innovate, especially in the area of intrusion prevention. We expect several partnerships to emerge between WLAN IPS and WLAN infrastructure vendors, and also between wired and wireless IPS vendors.

Gartner estimates that the WLAN IPS market was worth about $40 million in 2005, and this is expected to double in 2006.

Evaluation Criteria

Vendor Product/Service Analysis

AirDefense

AirDefense continues to stay relevant in the market. Being the first player in this market, the company set the stage for all the other players. It has built a substantial customer base since launching its products in 2002, but later market entrants are taking some of its share.

In 2005, AirDefense focused on the important technology area of the bandwidth requirements between sensors and the server. As the market evolves and the number of sensors deployed increases, bandwidth required by sensors becomes an issue. AirDefense has implemented a model in which the sensor and server collaborate to reduce the average bandwidth usage per sensor to less than 3 Kbps when communicating with the server. The company's original architecture required a lot of bandwidth between the sensor and the server, and this was one of the biggest reasons why AirDefense was losing market share.

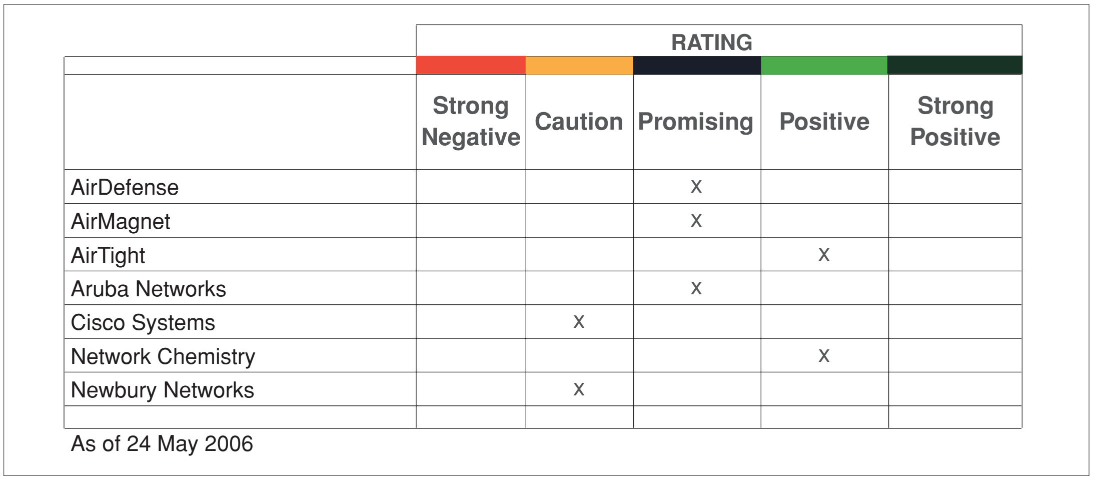
AirDefense has also improved its offering in the area of forensic storage. Archived data can be digitally signed to avoid tampering, and thus can be used in forensic investigations. It recently added site survey capabilities in partnership with Wireless Valley (acquired by Motorola in December 2005), which indicates a step in the right direction toward integrating site planning tools with ongoing security management tools. AirDefense has partnerships with service organizations for customers that want to outsource their site planning, or customers can buy the software and do it themselves in-house. However, doing it in-house is challenging, as the planning tool requires significant experience to be fully utilized. AirDefense also provides an option of using a "Y" cable approach, wherein sensors can draw power from the existing AP cables. This reduces the cost and the time required to deploy the sensors, but we believe sensor placement should be performed independently of AP location, as the range for traffic delivery, detection and prevention are very different. (Sensors work in passive mode while detecting and in active mode while preventing an attack. The prevention range is much smaller.)

Table 1. Evaluation Criteria

Evaluation Criteria	Comment	Weighting
Customer Experience	This includes the simplicity and the flexibility of the product range, the ease of deployment, operation and support capabilities. This criterion was assessed by conducting qualitative interviews of vendor references and feedback from Gartner clients.	high
Offering (Product) Strategy	The vendor's approach to product development and delivery that emphasizes differentiation, functionality, methodology and feature set as they map onto current and future requirements.	standard
Overall Viability (Business Unit, Financial, Strategy, Organization)	Viability includes an assessment of the overall financial health of the organization and its commitment to the wireless intrusion prevention market, along with the financial and practical success of the business unit. Also included is the likelihood of the organization/business unit to continue investing in the market and to continue developing innovative products to meet the requirements of several different types of customer.	high
Marketing Execution	The success and "mind share" of the product in the wireless intrusion prevention market, including the installed base and market share, as well as the maturity and breadth of the organization's distribution channels. Also considered is the quality of customer case studies and references, and the level of interest from Gartner clients.	standard
Product/Service	Breadth of the current feature set is a key evaluation criterion. We specifically evaluated wireless intrusion detection and prevention capabilities, RF monitoring and reporting, and the level of integration of site planning tools with ongoing security management tools.	high

Source: Gartner (May 2006)

Figure 1. MarketScope for Wireless LAN Intrusion Prevention Systems, 1H06



	RATING				
	Strong Negative	Caution	Promising	Positive	Strong Positive
AirDefense			x		
AirMagnet			x		
AirTight				x	
Aruba Networks			x		
Cisco Systems		x			
Network Chemistry				x	
Newbury Networks		x			

As of 24 May 2006

Source: Gartner (May 2006)

AirDefense's alarm and alert classification lags behind some of the other vendors, as some customers complained about it generating too many "false positives." But AirDefense claims that alarm priorities in its system can be adjusted based on the specific context of the user environment, and that the false alarms are generated if users fail to set up the system properly. The company either needs to better educate users on customizing the system, or else it needs to look into the causes of false positives and reduce the day-to-day management overhead of the system. AirDefense has the potential to achieve a "positive" rating, as it is well-known in the wireless intrusion prevention market and is filling in the gaps in its offering rapidly.

AirMagnet

AirMagnet continues to be a steady player in wireless intrusion prevention market and has the highest "mind share" among the WLAN IPS overlay vendors. The company got off to a slow start, but in early 2005 it took on more aggressive marketing tactics. Shifts in upper management in late 2005 created some uncertainties about the company, but it filled those positions quickly, and the uncertainties are fading.

Unlike other overlay WLAN IPS vendors, AirMagnet sensors perform complete Wi-Fi packet analysis, while alarms information is sent to the server for event correlation and anomaly detection. Sensors are able to store the data for about three days. Enterprises with distributed locations particularly like this feature, as they are able to retrieve data even if the wide-area network (WAN) link breaks down. While reports generated are similar to other overlay vendors, the current system does not allow administrators to schedule the e-mail delivery of reports.

AirMagnet's handheld/laptop tool is the most popular of all its products. It is sometimes used by its competitors' customers to narrow down the location of rogues detected by sensors on the ceilings. AirMagnet has an edge over its competitors because of the popularity of this tool. However, we would like to see tighter integration of the handheld tool with the ongoing RF management module to allow enterprises to synchronize databases in the handheld tool and server automatically. This remains an area for development for the company, along with its move to take the handheld user interface to the next level (that is, device-level monitoring).

AirMagnet has the functionality and proven installed base for a "positive" rating in the future. The company is aggressively pursuing its OEM partnership strategy with WLAN infrastructure vendors. This will help increase its market presence even more.

AirTight

AirTight Networks launched its products in 2005 and has progressed in several ways during the past year. Being a late entrant, it is not as well known as AirDefense or AirMagnet, but it is gaining some momentum. AirTight offers capable, easy-to-use attack classification and alert prioritization, with a good reporting console and site survey tools. But it needs to improve its sales and customer support strategy. The company's list of customers is growing, mainly by way of winning some accounts from its competitors. However, unless it increases its presence directly by "getting more feet on the ground" or by signing up some of the larger incumbent WLAN or wired security vendors as partners, it will remain a niche vendor in the enterprise WLAN intrusion prevention market.

Some features have recently been added to AirTight's tool, such as the ability to import site planning maps for sensor placement onto the ongoing RF monitoring tool. Using the same tool, enterprises can see coverage of APs (by importing previously conducted site surveys for AP placement into its tool), sensor detection and intrusion prevention ranges. AirTight offers site planning services for sensor placement based on its planning software. We believe this service offering, if priced competitively in requests for proposal (RFPs), will help the company achieve some level of mind share among many enterprises as they struggle to find a good alternate to cumbersome and expensive site surveys, especially for enforcing "no wireless" policies.

AirTight customers like the company's interface for day-to-day reporting but are not very happy with its customer support services and firmware upgrade process. Enterprises considering AirTight will benefit from its sensor placement services but should carefully evaluate service-level agreements. AirTight is expanding and plans to focus more on improving its service offerings. Overall, the company received very positive feedback from reference customers, but we also warn enterprises to be cautious of overly aggressive sales presentations and marketing tactics deployed by AirTight.

Aruba Networks

We believe WLAN IPS functionality will be integrated into WLAN infrastructure components over time. Aruba's primary focus is WLAN infrastructure, and it is demonstrating its commitment by integrating all pieces of wireless security and management into its basic WLAN infrastructure components and becoming a "one-stop shop" for enterprise WLAN needs. Aruba's WLAN IPS module is sold as software that runs on its mobility controllers, and its APs can be deployed as dedicated sensors or in dual mode of traffic delivery and sensing. Aruba provides "good enough" WLAN IPS, which is better than Cisco but lags behind overlay WLAN IPS solutions.

Aruba's customers like its AP classification capabilities. The system has four categories for wireless devices: valid, interfering, known interfering and rogue. Known neighbor devices may be placed into the "known interfering" category by the administrator and alerts are not generated for these devices. Very few users currently experience problems with interferences from neighboring networks, but as WLAN become pervasive, proper classification will become an important feature in WLAN IPS solutions. This will help planning for network expansion as well as minimizing false alarms. Aruba was also the first vendor to do RF signature-based wireless intrusion detection.

Some of Aruba's initial wins were due to its wireless intrusion detection capabilities, but, over time, several overlay vendors have entered the market with improved WLAN IPS offerings. Now, Aruba's WLAN IPS solutions are mainly deployed by its existing customer base, and though some are deploying APs as sensors, the most common approach among its customers is to deploy AP in dual mode of traffic delivery and sensing.

Cisco Systems

A year after the Airespace acquisition, Cisco has begun to clearly articulate its wireless strategy based on third-generation WLAN products. Cisco's wireless products consist of:

- Aironet series APs that are fully functional stand-alone APs.
- Airespace controllers and coordinated APs.

Wireless networks deployed using Cisco's stand-alone APs require a WLAN service engine (WLSE) for network element management. Enterprises usually deploy a wireless intrusion prevention system as an overlay product from any of the other vendors mentioned in this report. Cisco's third-generation centralized Airespace controller has integrated WLAN IPS functionality and we have evaluated this offering for this report. There are many advantages of using a common hardware platform (coordinated APs working as sensors by time-slicing between the two functions, and controllers also carrying out correlation engine tasks). Not having to deploy separate sensors brings down the cost of the infrastructure, service and support, site planning, cabling and installation, but it does not provide 24x7 “stateful” monitoring of RF. APs can be deployed as dedicated sensors, but their sensing capabilities do not match those of other vendors evaluated in this report. Cisco is focusing on making WLAN infrastructure more robust and integrating WLAN features into wired networking switches – WLAN IPS does not appear to be high enough on its list of priorities. The company must also improve on ease of implementation, management and reporting of its WLAN IPS solution. We believe that there are substantial opportunities for Cisco to integrate wireless intrusion capabilities into its WLAN infrastructure, as well as into its wired IPS offering. The company has yet to sell WLAN IPS outside its customer base, or to customers enforcing “no wireless” policies, but being able to bundle a WLAN IPS offering into a WLAN infrastructure component is a step in the right direction.

The company has the best overall reach and its share in WLAN infrastructure vendors will also help, but enterprises that need best-of-breed WLAN IPS solutions are better off considering WLAN IPS overlay solutions.

Network Chemistry

Network Chemistry has progressed in several ways during the past year, increasing its direct presence in the market and working on its partnership strategy. The company initially sold its products only through OEM partners, but it changed this sales strategy in 2005 and started selling under its own brand name as well. While this shift in strategy has hurt the company, Network Chemistry’s share is increasing gradually. Like other startups, its distribution and support capabilities are somewhat limited. It continues to be an OEM partner to Newbury Networks for sensors and is strengthening its ties with other security vendors from the wired networking market.

Network Chemistry is perceived as a “no frills” vendor by its customer base. Its management console dashboard screen, with a drill-down approach, is well thought out and helps in quickly getting to the most relevant information. However, some work is required on location tracking capabilities and integration of pre-deployment survey results with ongoing monitoring and management capabilities. Network Chemistry’s sensors have dual 11a/b/g radios. This gives them a better capability for scanning while mitigating – while one radio is engaged in mitigating an attack, the other radio can continue to scan on both frequency bands. However, the duration for which sensors are able to store information locally is short (about nine hours). This might create problems for enterprises with distributed locations in case the WAN link breaks down and the data is not offloaded onto the server in time.

Network Chemistry’s operational costs are much lower than most of its competitors, but the amount of funding it has received is also less than its competitors. Recent partnerships with wired security vendors, and the hiring of a new CEO from a security company, indicates that Network Chemistry will focus more on being a networking security vendor rather than just an overlay security solution for WLAN.

In our interviews with company references, Network Chemistry received the best score for customer experience.

Newbury Networks

Newbury Networks has made relatively slow progress since launching its products in 2004. The company sources its sensors from OEM Network Chemistry, but it has developed its own correlation engine, which is a Linux-based server that collects data from sensors for reporting and prevention decisions. Newbury has also done a significant amount of work to integrate its correlation engine with Cisco Aironet APs. Overall, the product offering is adequate, but it lacks certain additional tools that enterprises like to consider. Newbury currently does not offer any site-planning tool of its own for sensor placement, and, unlike most of its competitors, it does not offer products for protecting users when connected on open wireless networks such as “hot spots” or home offices.

The vendor's overall strategy is to focus on applications that can be supported over WLAN IPS solutions, such as providing location-specific contextual information. It uses RF fingerprinting as a location tracking methodology, which, in theory, should require fewer sensors, unlike triangulation, which needs at least three APs for accuracy. But what we found in our customer interviews is that, with this method, the number of sensors did not really go down but the accuracy improved. Accuracy also depends on extensive calibration that is required for RF fingerprinting to work, which is a very labor-intensive process. Newbury Networks needs to improve its calibration technique to reduce the amount of time required for set-up. It also needs to clearly differentiate itself, so that enterprises consider it for the applications that it is developing over basic WLAN IPS infrastructure. Of the vendors we evaluated, Newbury Networks has the smallest functional and geographical coverage in the wireless intrusion prevention market.

Acronym Key and Glossary Terms

AP	access point
IPS	intrusion prevention system
OEM	original equipment manufacturer
OSI	Open Systems Interconnection
RF	radio frequency
RFP	request for proposal
WAN	wide-area network
WLAN	wireless local-area network
WPA2	Wi-Fi Protected Access 2

MarketScope Rating Framework

Strong Positive

Is a solid provider of strategic products, services or solutions.

- *Customers:* Continue investments.
- *Potential customers:* Consider this vendor a strong strategic choice.

Positive

Demonstrates strength in specific areas, but is largely opportunistic.

- *Customers:* Continue incremental investments.
- *Potential customers:* Put this vendor on a shortlist of tactical alternatives.

Promising

Shows potential in specific areas; however, initiative or vendor has not fully evolved or matured.

- *Customers:* Watch for a change in status and consider scenarios for short- and long-term impact.
- *Potential customers:* Plan for and be aware of issues and opportunities related to the evolution and maturity of this initiative or vendor.

Caution

Faces challenges in one or more areas.

- *Customers:* Understand challenges in relevant areas; assess short- and long-term benefit/risk to determine if contingency plans are needed.
- *Potential customers:* Note the vendor's challenges as part of due diligence.

Strong Negative

Has difficulty responding to problems in multiple areas.

- *Customers:* Exit immediately.
- *Potential customers:* Consider this vendor only if there are no alternatives.