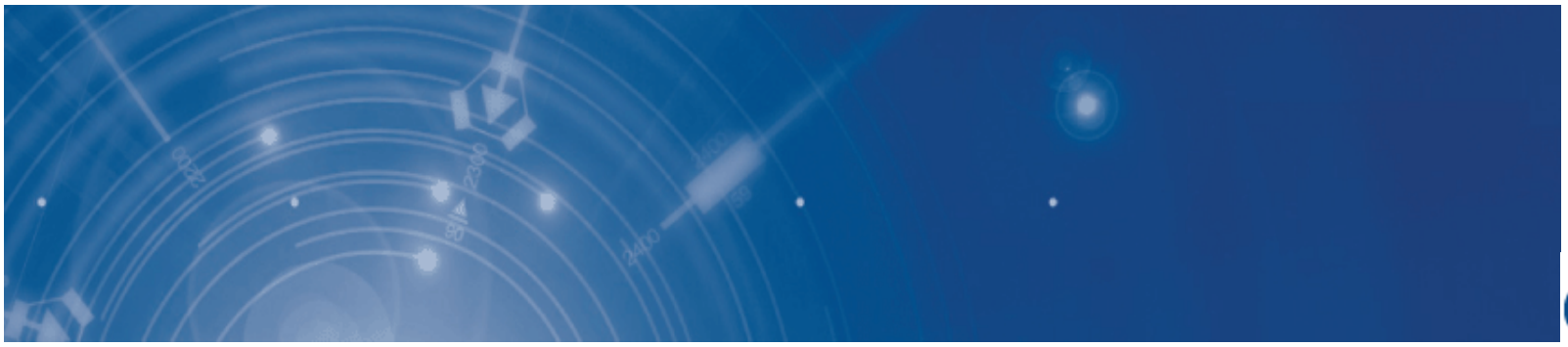

MarketScope for Wireless LAN Intrusion Prevention Systems

30 July 2009

John Pescatore, John Girard

Gartner RAS Core Research Note G00169482

Economic factors caused growth to slow in wireless LAN intrusion prevention systems in 2008. Changing requirements put a premium on new detection capabilities and increased levels of integration with network infrastructure.

What You Need to Know

This document was revised on 4 August 2009. For more information, see the Corrections page on gartner.com.

Wireless LANs (WLANs) built on Wi-Fi technologies are delivered in four basic specifications: 802.11a (a high-capacity 5GHz design), 802.11b, 802.11g and 802.11n. The latter three are 2.5GHz designs, each offering incrementally higher speeds and greater user capacities. Because Wi-Fi signals are easy to intercept and interrupt, interference is a common problem, and wireless monitoring is required.

The built-in security capabilities of WLANs have improved and stabilized with Wi-Fi Protected Access 2 (WPA2) Enterprise, but compromises of WLANs are still an all too frequent occurrence. Reasons for compromise include continued use of legacy equipment, weak security protocol choices, intentionally unencrypted guest networks and public hot spots, and configuration mistakes.

Because Wi-Fi support is increasingly a standard extension of corporate networks, enterprises must ensure that vulnerability management and intrusion prevention processes are extended to cover wireless and wired networks. WLAN security monitoring is required to ensure that supported WLANs are kept secure and that users do not install their technologies where WLANs are not allowed, or where newer, faster WLANs, such as 802.11n, have not been adopted.

Further advances in other wireless technologies and general concerns about the use of smartphones have carried the scope of wireless intrusion prevention system (WIPS) beyond Wi-Fi, and vendors in this market are expanding into Bluetooth, cell phones, wireless cameras, cordless phones, and other non-Wi-Fi services. These additional wireless signals can cause interference, expose information and violate usage policies, and it's logical for WLAN IPS vendors to consider them as a direction for expanding their WIPS business opportunities.

WLAN security monitoring capabilities can be implemented by using the integrated capabilities provided by the WLAN infrastructure vendor, or as separate "overlay"

Vendors Added or Dropped

We review and adjust our inclusion criteria for Magic Quadrants and MarketScopes as markets change. As a result of these adjustments, the mix of vendors in any Magic Quadrant or MarketScope may change over time. A vendor appearing in a Magic Quadrant or MarketScope one year and not the next does not necessarily indicate that we have changed our opinion of that vendor. This may be a reflection of a change in the market and, therefore, changed evaluation criteria, or a change of focus by a vendor.

Gartner MarketScope Defined

Gartner's MarketScope provides specific guidance for users who are deploying, or have deployed, products or services. A Gartner MarketScope rating does not imply that the vendor meets all, few or none of the evaluation criteria. The Gartner MarketScope evaluation is based on a weighted evaluation of a vendor's products in comparison with the evaluation criteria. Consider Gartner's criteria as they apply to your specific requirements. Contact Gartner to discuss how this evaluation may affect your specific needs.

The various ratings are defined below.

MarketScope Rating Framework

Strong Positive
Is viewed as a provider of strategic products, services or solutions:

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

capabilities. The former is usually less expensive, while the latter almost invariably provides stronger security capabilities. As new wireless technologies emerge, the overlay systems will provide the most flexible approach for rapidly incorporating monitoring and intrusion prevention.

Return to Top

MarketScope

For most enterprises, WLANs have become a standard part of network architecture. Gartner has seen evidence of enterprises seeing WLAN connectivity reduce the density of users per wired port, especially as 802.11n with higher throughput is deployed and users default to WLAN as their standard means of connectivity. This has raised the stakes for network managers to look at tools for ensuring that WLANs are reliable, driving demand for wireless monitoring capabilities. At the same time, attacks exploiting misconfigured or outdated WLAN technologies have continued, as well as rogue (i.e., unauthorized, unknown and untraceable) installations of next-generation technology (802.11n) by impatient users. This has driven compliance regimes, such as Payment Card Industry (PCI) Data Security Standard (DSS) and the Federal Information Security Management Act (FISMA), to emphasize continual monitoring of wired and wireless networks.

Gartner sees four primary scenarios for WLAN IPS technology demand in the current environment, in order of importance:

- **Intrusion detection and prevention —** High-security, proactive organizations or those driven by compliance regimes to take aggressive stances toward WLAN security.
- **Vulnerability assessment —** A more passive, reactive approach to detecting misconfigured access points to more rapidly mitigate vulnerabilities.
- **Overall WLAN health/operations monitoring —** WLAN vulnerability assessment integrated into efforts to ensure overall WLAN availability and performance.
- **Shielding for use of known insecure technologies, such as Wired Equivalent Privacy (WEP) —** In a shrinking number of applications, enterprises cannot upgrade older, nonsecure WLANs and use the capabilities of the WLAN IPSs as compensating controls until the obsolete WLAN infrastructure can be replaced. The PCI Security Council has stated that WEP will not be allowed after 30 June 2010, which will further decrease the share of this use case.

New wireless technologies (such as 802.11n) and emerging forms of wireless communications (such as WiMAX and third-generation cellular) have broadened the types of WLAN signals that need to be detected. Also, as the use of WLANs becomes increasingly mainstream, vulnerability-seeking attacks will increase, and intrusion prevention capabilities will be used more. So, although the WIPS market has reached the early mainstream phase, it continues to be a dynamic market where new features are needed with each product release.

This MarketScope analyzes the performance of vendors that have focused on this market from the second half of 2008 through the first half of 2009. Gartner's evaluation is based on (in order of importance) continuing discussions with Gartner clients that are using and evaluating these products, survey responses from the vendors, and interviews with reference customers that were provided by the vendors. The ratings shown quantify Gartner's opinions of each vendor's performance in the market and should be used as just one input in your buying decisions.

Return to Top

Market/Market Segment Description

The WLAN IPS market consists of products used for performing continual monitoring

Positive
Demonstrates strength in specific areas, but execution in one or more areas may still be developing or inconsistent with other areas of performance:

- *Customers:* Continue planned investments.
- *Potential customers*: Consider this vendor a viable choice for strategic or tactical investments, while planning for known limitations.

Promising
Shows potential in specific areas; however, execution is inconsistent:

- *Customers:* Consider the short- and long-term impact of possible changes in status.
- *Potential customers:* Plan for and be aware of issues and opportunities related to the evolution and maturity of this vendor.

Caution
Faces challenges in one or more areas:

- *Customers:* Understand challenges in relevant areas, and develop contingency plans based on risk tolerance and possible business impact.
- *Potential customers:* Account for the vendor's challenges as part of due diligence.

Strong Negative
Has difficulty responding to problems in multiple areas:

- *Customers:* Execute risk mitigation plans and contingency options.
- *Potential customers:* Consider this vendor only for tactical investment with short-term, rapid payback.

and vulnerability assessment of WLANs, as well as in providing detection and active blocking of potential attacks. The radio frequency (RF) monitoring of WLANs also has proved necessary for managing the performance and capacity of WLANs, as well as in dealing with help desk calls when users report operational problems. This trend has increased the importance of WLAN system management capabilities (such as richer audit trails and the identification and location of interference sources) for buyers.

However, as new wireless technologies (such as 802.11n, WiMAX and particularly 3G cellular) penetrate, "rogue" problems have reappeared, which means that intrusion prevention capabilities will remain important. Although few buyers cite infrastructure operations management as the top buying decision, products in this market are also capable of coping with operational challenges for traffic, performance management and compliance that are posed by the increasingly complex mix of wireless traffic. Gartner believes that the dual use of WIPS across security and WLAN operations management will increase during the next three years.

Gartner estimates that global revenue in this market grew from $119 million in 2007 to $161 million in 2008, a one-year growth rate of 35%. This is nearly double Gartner's estimate of 18% growth for the WLAN infrastructure equipment in 2008, but is below our previously predicted growth rate of 41% for this period for WLAN IPS. We believe the growth rate slowdown is primarily due to three factors:

- Global economic factors resulted in delays in acquiring WLAN IPS and diversion of funds into higher-priority projects.
- Certain well-defined growth markets for distributed Wi-Fi protection were attenuated by the economic downturn — for example, the potential to sell products to protect PCI data in retail and branch locations was affected by closures of chain store locations.
- Enterprise perception of WLANs as mature technology, combined with acquisitions of WLAN IPS vendors by WLAN infrastructure vendors, caused many companies to use operational access points or other work-arounds as monitoring solutions instead of pursuing more-intensive sensor-oriented strategies.

These factors will still be in play throughout 2009 and into 2010, so we are predicting that 2009 revenue will grow no more than 30%, and will reach $209 million. A rapid upturn in the economy could result in higher growth, but other factors are not likely to change. On 17 July 2009, the PCI Security Standards Council issued Wireless Security Guidelines that specifically required all networks to be scanned for rogue access points, and that networks using WLANs to handle card data specifically need some form of wireless intrusion detection and prevention — see www.pcisecuritystandards.org/pdfs/PCI_DSS_Wireless_Guidelines.pdf. While this mostly restated existing PCI DSS requirements, the explicit mention of WIPS will likely cause PCI-qualified security assessors to be more rigorous in documenting deficiencies in WLAN security and should spur WIPS sales in the retail sector.

Our estimates continue to run higher than Gartner's estimate of growth in enterprise WLAN infrastructure revenue. While the large enterprise base in North America has been initially penetrated, there is still room for expansion of monitoring capabilities outside of headquarters locations into branch offices, as well as upgrades to deal with demands for detecting 802.11n in sites with older equipment, and for detecting non-Wi-Fi, such as 3G cellular voice and data.

Average costs among the six ranked vendors equate to 5 cents per monitored square foot, ranging from a low of 4 cents to a high of 15 cents on implementations averaging 42,000 square feet. Vendors are able to generate revenue on newer-model systems to detect 802.11n that run as much as twice what they are able to charge alone for legacy 802.11a/b/g. The highest revenue growth will likely be in Europe, while we still do not see major growth in demand in Asia/Pacific. Starting in early 2010, we expect increased demand for the need to monitor cell use. We also expect to see some adoption of WLAN monitoring as a service, but mostly in conjunction with the overall outsourcing of WLAN operations.

Vendors in this market include WLAN infrastructure vendors that sell differentiated WIPS solutions, as well as smaller vendors that sell only WLAN-monitoring capabilities. All vendors offer security monitoring, as well as WLAN performance and troubleshooting monitoring; however, in this MarketScope, the vendors are ranked

first and foremost on their abilities to fulfill the core requirements of WLAN IPS. Vendors with other lines of business receive credit for financial strength, as applicable, but their strengths and challenges in the core requirements of the market define their ratings.

For a detailed description of the core capabilities of WLAN IPS products, see "What to Look for in a Wireless Intrusion Prevention System."

Return to Top

Explanation of MarketScope Scores

The rankings of vendors are derived from the weighted evaluation criteria listed in the evaluation section of this research. The final rating for each vendor corresponds to a score that defines Gartner's overall assessment.

Strong Positive

The vendor shows a strong balance of forward-thinking technological development and competitive dominance in the market. High name recognition combines with business-relevant solutions to sell the technology more effectively than other market players. Strong Positive vendors are defining and refining the market by their actions and are forcing other vendors to conform. In this market, a Strong Positive vendor is seen as reducing the cost of implementing wireless security for current technologies, providing a path to easily deal with new threats and new wireless technologies, and being the lead in integrating with leading WLAN technology providers. It is difficult to achieve this ranking because of the growing breadth of wireless technologies and the fact that the market accounts for only a tiny percentage of network equipment and service revenue

Positive

Positive vendors are better than average at setting industry directions, attracting business and generating revenue, but their market influence is markedly behind what we would expect from a real or theoretical Strong Positive vendor. The position of Positive vendors, in terms of seats and revenue, shows growth for at least two years in a row, but Positive vendors do not control the market. Their products are an excellent fit for the market in terms of features and functions but may not be the broadest or most complete. Positive WLAN IPS vendors meet all market needs but may not have the channel reach or R&D strength to be clearly ahead of the competition.

Promising

Promising vendors have good and appropriate technologies for the market, although their offerings are not as complete or competitive as those that would garner a Positive rating. Promising vendors have reached a size (or their division in a larger company has reached a size) that offers some stability in a startup market. We expect to see sales moving and growth within the year of an evaluation but do not require a year-over-year growth record. The Promising vendor is a stable choice in the market. This vendor can be a niche player but runs the risk of going stale if it does not have a road map to demonstrate an understanding of the market and of competitors. Promising WLAN security vendors have sufficient financial strength and R&D capability to rapidly grow, but they may not have executed on this strength.

Caution

Vendors in the Caution category are stable in the market, although their products/ services are not strong contenders, because they do not adequately address the core requirements for the market or have not yet demonstrated competitive strength. Features are missing or incomplete. Road maps may show progress to build out the product/service during the next year, but, in our assessment, this will not alter the market position relative to other vendors in the MarketScope. WLAN security vendors that are rated as Caution represent acceptable buying choices, but they are not on

course to pursue the market in the long run.

Strong Negative

The Strong Negative vendor is in a rapidly deteriorating situation that involves one or more of these criteria: the loss of key people, key investors, income/finance and technology, and failures of the product/service reported to Gartner or the media. The vendor is unable to demonstrate a forward path that will remedy these problems so that purchasers will not be put at risk. Officially, this is a do-not-buy warning.

Return to Top

Inclusion and Exclusion Criteria

This MarketScope evaluates vendors that offer overlay WLAN IPSs, as well as WLAN infrastructure — such as access points (APs) and WLAN controllers — vendors that have integrated WLAN IPSs into their WLAN infrastructure components. To be included in this research, vendors must have a WIPS product that provides the functions listed below, must demonstrate that they are generating revenue for shipping products and must provide at least three reference customers that are making stable production use of their products.

The technical capabilities of these vendors' products must include rogue detection (rogue APs, clients and ad hoc networks), monitoring of airwaves for attacks and misuse, the ability to detect misconfigured APs and wireless endpoints, and quality-of-service enforcement or spectrum optimization capabilities. Location determination, the ability to mitigate the security deficiencies of Wired Equivalent Privacy-based WLANs and the availability of client software to provide policy enforcement on laptops that are in external environments are highly weighted capabilities but were not used as inclusion criteria.

Two vendors were added to the previous MarketScope:

- AirPatrol: This is the first company in this market space to create a business model based primarily on licensing OEM software to third parties, which it has done since 2006. Its time in the market under its brand name (since May 2008), capabilities and customer references are now sufficient to qualify for inclusion in this year's report.
- Motorola acquired AirDefense.

Several vendors were not included in this MarketScope because they did not meet the inclusion criteria:

- Air Defense: AirDefense was acquired by Motorola.
- Meru Networks: This vendor sells production infrastructure access systems mainly in competition with Cisco and Aruba Networks. It developed patented "collision" methods for blocking unauthorized access to WLANs that are not breakable by hacking techniques. Meru does not effectively pursue a position in the intrusion prevention market, although compared with last year, it has begun to market some of its security capabilities. Meru does not have a stock-keeping unit for IPS and does not track the use of IPS, and the company was unwilling to provide direct or indirect financial and market share information needed to qualify for inclusion. Gartner clients who call with inquiries do not typically associate Meru with the WIPS market, and our extensive case study investigation conducted for this research did not reveal a single reference company that named Meru as a considered vendor. To be considered for inclusion in this MarketScope, Meru must position itself as a recognized IPS competitor, and must provide comparative revenue and sales data.
- Trapeze Networks: This Wi-Fi infrastructure vendor acquired Newbury Networks in December 2008, and released a new product, RF Firewall, based on Newbury Networks technology in July 2009. Trapeze provides patented location-based access control and other services, which can be a complement to a WIPS. To be included in Gartner's WIPS MarketScope in the future, Trapeze should develop a recognized competitive WIPS position, and it must

be perceived as a contender by buyers as well as peer vendors that Gartner considers to be qualified for this market segment. Newbury Networks has been not been included previously for the same reasons.

- Code Red Systems: Code Red's AirMarshal Wireless Management Software provides many of the WLAN monitoring functions but does not have the active protection capabilities required to meet the inclusion criteria, nor has Gartner seen the vendor in any enterprise competitions.

Return to Top

Rating for Overall Market/Market Segment

Overall Market Rating: Positive

We rate this market as Positive, because although the growth has slowed, Gartner expects to see positive growth for several years. We also believe established and new vendors are continuing to innovate, especially in the area of monitoring forms of wireless communication other than Wi-Fi. We expect several partnerships to emerge among WLAN IPS and WLAN infrastructure vendors, and among wired and WIPS vendors.

Gartner estimates that global revenue in this market grew from $119 million in 2007 to $161 million in 2008, an annual growth rate of 35%.

Return to Top

Evaluation Criteria

Table 1. Evaluation Criteria

Evaluation Criteria	Comment	Weighting
Customer Experience	This includes the simplicity and flexibility of the product range, as well as ease of deployment, operation and support capabilities. This criterion was assessed by conducting qualitative interviews with vendor references and by obtaining 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 to current and future requirements.	High
Overall Viability (Business Unit, Financial, Strategy, Organization)	Viability includes an assessment of the overall financial health of the organization and its commitment to the WIPS 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 customers.	Standard

Marketing Execution	This entails the success and "mind share" of the product in the WIPS market, including the installed base and market share, as well as the maturity and breadth of the organization's distribution channels. Also considered are the quality of customer case studies and references, and the level of interest from Gartner clients.	Standard
Product/Service	Breadth of 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 (July 2009)

Return to Top

Figure 1. MarketScope for Wireless LAN Intrusion Prevention Systems

	RATING				
	Strong Negative	Caution	Promising	Positive	Strong Positive
AirMagnet				x	
AirPatrol		x			
AirTight Networks				x	
Aruba Networks			x		
Cisco			x		
Motorola (AirDefense)				x	

As of 30 July 2009

Source: Gartner (July 2009)

Return to Top

Vendor Product/Service Analysis

AirMagnet

Description: AirMagnet offers two products that feature WLAN security monitoring. AirMagnet Enterprise provides monitoring and stateful analysis of WLAN traffic. AirMagnet's sensors perform local processing, reducing the traffic load on the network and minimizing central points of failure. AirMagnet Enterprise supports full-packet capture, interference identification, attack blocking, and WEP shielding for legacy networks. AirMagnet Enterprise can import Access Control Lists from Cisco WLAN controllers. AirMagnet Wi-Fi Analyzer PRO is a portable sniffer that is often used for performance monitoring and troubleshooting, but it can also identify misconfigured and rogue access points. AirMagnet has obtained FIPS 140-2 certification for most of its WIPS product line.

Strengths: AirMagnet continues to have the strongest range of WLAN performance-monitoring and troubleshooting capabilities in an enterprise and mobile analyzer form. Users that selected AirMagnet generally report these factors as the primary reasons for selection. AirMagnet users point to ease of use as a strong differentiator. Sensors can run stand-alone and record logs for up to three days in case of network interruption. AirMagnet's history and expertise in "sniffing" provides some of the

most aggressive and detailed methods for tracing suspicious devices and data traffic through wired and wireless networks. The vendor submitted the largest example list for templates of automatically generated compliance reports. Revenue is respectable and viable.

Challenges: Some Gartner clients report that, although AirMagnet is easy to use once it is up and running, the actual installation procedures are complex. AirMagnet is not as visible in security-centric procurements as the other overlay competitors, and because AirMagnet is not a WLAN infrastructure vendor, it does not show up in competitions when security is the only criterion.

Optimal-use case: AirMagnet is viable for all WIPS scenarios but is most appropriate for WLAN deployments where security and wireless network operations will be shared responsibilities, and where one product will be used for operational monitoring and security. AirMagnet is appropriate in situations where companies need broad spectrum detection and monitoring capabilities.

Rating: Positive

Return to Top

AirPatrol

Description: AirPatrol has several years of history in the wireless threat prevention area, but until 2008, its role was limited to licensing OEM software. In 2008, AirPatrol introduced its own line of sensor appliances and endpoint monitoring software to be installed on users' PCs and other devices. As the youngest entrant to the MarketScope, AirPatrol has effectively created awareness for its products in all industry sectors by featuring its strengths on real-time monitoring of a wide range of wireless signals.

Strengths: AirPatrol offers aggressive location tracking combined with abilities to selectively block Wi-Fi users based on device type. Using a black-box approach to packet monitoring, AirPatrol has developed behavior signatures that categorize *how* a device is being used. For example, the signatures can determine that a PC is streaming music, or having a VoIP call. They can tell if a phone is taking pictures and uploading them, being used in a conversation, or sending/receiving text messages. The behavior is captured and time-stamped in the events' log to support subsequent investigations. Emphasis on cellular monitoring opens up specialty markets that could grow into every industry sector. AirPatrol's software sensor design will make supporting future wireless technologies mostly a software upgrade issue.

Challenges: AirPatrol's revenue is tiny compared with the market average. It needs to grow to make the line of business viable in the long term, which is the only reason for a Caution rating. Fortunately, AirPatrol already is stable through its OEM revenue for wireless IPS. AirPatrol's abilities to provide active intrusion prevention and countermeasures, as well as integration with wireline network access control, need to be developed to better meet the baseline functionality of the market. Demonstrated server/AP scalability is limited compared with competitors. AirPatrol's lookup approach for tactical resolution of alarms requires integration to third-party products. AirPatrol lacks Federal Information Processing Standard (FIPS) and Common Criteria (CC) certifications, which reduce friction when selling into U.S. government contracts and naturally attract buyers in other markets.

Optimal-use case: AirPatrol's optimal-use case is for companies that have a high priority for deep real-time analysis of monitored wireless traffic or those that specifically want to detect cellular data use, and are willing to work with a small vendor.

Rating: Caution

Return to Top

AirTight Networks

Description: AirTight continues to be an overlay player solely focused on the WIPS market. Products include SpectraGuard Enterprise (WLAN IPS), SpectraGuard SAFE (endpoint agent), and SpectraGuard Planner for planning WLAN and WIPS deployments. AirTight products are certified to FIPS 140-2 and CC Evaluation Assurance Level (EAL) 2.

Strengths: AirTight showed strong revenue growth in 2008 and 1H09, proving that a stand-alone IPS company can buck the trend of consolidation with infrastructure vendors seen elsewhere (Aruba + AirWave + Network Chemistry; Motorola + AirDefense; Cisco + Perfigo + AireSpace). Customer references report that the product is easy to set up and that AirTight's methodology for classifying events avoids false alarms when identifying rogues. The administrative console help system can accommodate four different skill levels, from beginner to expert. One reference client explained that the ease of running AirTight (compared with other products) eliminated the need to dedicate staff and undergo extensive training. The products are available in software as a service (SaaS) via SpectraGuard Online, as well as for direct purchase. OEM license relationships with WLAN infrastructure vendors, such as Siemens/Enterasys, 3Com/H3C/TippingPoint and HP ProCurve (Colubris), contribute additional revenue in markets where these vendors have penetration.

Challenges: With only WIPS revenue to grow on, as a relatively new company, AirTight faces procurement hurdles for low-risk buyers. Because AirTight is not a WLAN infrastructure vendor, it has to rely on its partnerships with infrastructure vendors to bring it into many deals, rather than automatically included in every WLAN upgrade procurement. Thus, AirTight is largely limited to selling its products as add-ons separate from infrastructure procurements. AirTight has shown the ability to focus on security-centric overlay opportunities, but it does not fare as well when security is not the decision driver, and network operations needs are equal or stronger in the mix. AirTight must be prepared to grow customer service and support in line with its relatively strong success rates.

Optimal-use case: AirTight is appropriate for buyers that are looking for an easy-to-deploy solution with minimal training/skill requirements, and that are willing to take on a second wireless vendor to provide WIPS in exchange for strong security and rapid deployment with reduced overhead to set up and configure.

Rating: Positive

Return to Top

Aruba Networks

Description: Aruba Networks is a well-established WLAN infrastructure vendor, and is no longer seen as David to Cisco's Goliath, although its market share for WLAN infrastructure and WLAN IPS is still much smaller than Cisco's. In July 2007, Aruba acquired the RFprotect and BlueScanner WLAN security products from Network Chemistry, giving Aruba the ability to sell overlay wireless security monitoring as well. In 2008, Aruba acquired AirWave, which sold wireless system management tools that also had security monitoring capabilities. Aruba's WIPS product line consists of RFprotect Distributed (the overlay solution), RFprotect Mobile (a laptop-based Wi-Fi sniffer), RAPIDS (a rogue detection module that is part of the AirWave Wireless Management Suite) and the Aruba Wireless Intrusion Prevention module for use with the Aruba Controller's ArubaOS software (the infrastructure solution). Aruba recently announced wireless and wired branch-office products that support WIPS functionality as well. Aruba products are certified to FIPS 140-2 and CC EAL 2.

Strengths: Aruba is a dependable longtime player in WLAN infrastructure with a history of successful competitive wins and takeouts over Cisco. Aruba's infrastructure-based WIPS capabilities are enhanced by the policy enhancement firewall that is part of the Aruba Controller family. Aruba has integrated its earlier acquisitions into a fairly seamless system with strong security capabilities. Aruba is often a strong choice for wireless guest networks, where its Network Access Control and WIPS

capabilities provide the necessary security functions for supported secure wireless access by unmanaged laptops. Aruba continues to be responsive to the needs of the government vertical industry. Aruba's references continue to give its offerings high marks for quality service and support, ease of deployment and ease of management, but they chose Aruba mostly for WIPS because users were employing Aruba WLAN gear. In 2009, Aruba introduced a new line of low-cost remote access points starting at $99 that are ideal to link enterprise security policy to remote small and home offices. Functionally similar products are available from other WLAN vendors, but starting prices are hundreds more.

Challenges: Aruba's success as a company is based primarily on selling its Controller family and APs against other WLAN infrastructure vendors (such as Cisco and Motorola), not on selling stand-alone WIPS products. Aruba can benefit from increased efforts to market outside the Aruba infrastructure installed base, because it's very clear that companies will buy WIPS separately from WLAN infrastructure. Aruba's rogue scanning range on hybrid access points is limited to checking only the legal Wi-Fi channels in the country of location. Buyers must be aware of their spectrum-monitoring needs so they can determine whether they will want to configure dedicated sensors to detect non-Wi-Fi traffic and unapproved Wi-Fi channels. For example, rogues might use the unapproved channels to avoid being caught by scanners that presume only legal channels are vulnerable. Aruba's sensors report non-Wi-Fi signals as noise and provide rough location estimates for sources.

Optimal-use case: Aruba Networks' WIPS module is appropriate for use with Aruba wireless networks, while the RFprotect Distributed product is an appropriate choice for the buyer whose primary driver is ease of use. Companies that need to invest heavily in remote branch/office coverage should consider the low entry cost of Aruba's basic remote access points.

Rating: Promising

Return to Top

Cisco

Description: Cisco is the major player in the WLAN infrastructure market. Its infrastructure products include autonomous APs, lightweight APs managed by a controller and a platform for infrastructure management. Cisco's wireless security product provides core IPS functions as part of Cisco's Adaptive Wireless Intrusion Prevention System. Cisco products are individually certified to FIPS 140-2. Common Criteria certification is in process.

Strengths: Cisco's dominant position in wired and wireless infrastructures means it is automatically on the shortlists of enterprises of all sizes and is the most widely deployed in the enterprise WLAN infrastructure market. The security monitoring capabilities of Cisco's product line match the needs of the typical Cisco trained network security engineer. Cisco's Adaptive WIPS can be deployed using only operational APs as part-time sensors, or using extra APs as receive-only sensors, or a combination of both. Reference users report excellent management capabilities and integration. The user interface appearance includes many features that rely on contrast and icons instead of color. In all-Cisco environments, Cisco's integration of Adaptive WIPS with other Cisco wired network security solutions is a strong differentiator. Cisco's approach to dealing with legacy Wi-Fi issues, such as the use of WEP, is considered a major positive. Cisco's pricing is very competitive and often comes in well below overlay solutions.

Challenges: Cisco's WIPS is better communicated in competitive sales situations than seen in previous years but is sometimes dismissed by clients that may not realize the significant progress and improvements that have come to Cisco's wireless IPS. Gartner clients still find Cisco's unified network strategy to be complex and typically do not recognize or understand how to take advantage of the WIPS capabilities. For example, in a unified network scenario that is often proposed by Cisco as part of a new wireless network buildout, the user might have to deal with cross-configurations of standard and lightweight APs used in production and hybrid modes, WLAN controllers (WLCs), a wireless control system (WCS) console, mobility

service engines (MSEs), Cisco MARS and others. Cisco's actual WIPS technology does not require all these elements, but users report that a configuration proposal often includes all of them. Cisco recommends that buyers use a combination of dedicated APs and production APs for listening purposes, but it has been unable to interrupt growth from pure-play WLAN IPS companies that continue to make compelling arguments for dedicated sensors. Clients often perceive the incremental cost of adding a third-party product to be the easiest way to supplement Wi-Fi management and security for a Cisco network. Cisco must continue to improve its wireless security channel education and sales messages. Troubleshooting could be complex because of the drill-down approach to resolving problems.

Optimal-use case: Cisco is a strong choice for production wireless-access infrastructure-based monitoring when deploying dedicated sensors isn't feasible, and there is a strong desire to minimize vendors. Cisco can be used for high-security, managed environments, although client perceptions continue to favor Cisco for low-security and simple management environments. Extensive case study interviews indicate that security buyers seeking strong wireless security in 2009 will continue to consider overlay products.

Rating: Promising

Return to Top

Motorola (AirDefense)

Description: Motorola acquired AirDefense in 2008. AirDefense introduced its first WIPS product in 2002, and is the largest overlay WIPS vendor. The WIPS product line consists of AirDefense Enterprise and AirDefense Personal for laptop protection. AirDefense also sells a laptop-based WLAN scanner to compete with AirMagnet's product, as well as WLAN-planning and survey tools. AirDefense obtained Common Criteria EAL 2 certification for its product and has a strong presence in the government market. Motorola/Symbol improves its channel strength in nonoffice WLAN markets, such as retail, transportation, manufacturing and utilities.

Strengths: The acquisition has dramatically increased Motorola's visibility in the WLAN market and has created many new opportunities for deals. AirDefense historically enjoyed the highest level of visibility of all the overlay WIPS vendors and appears on most enterprise shortlists. It has a history of being early to market with new security features and provides the most detailed event information on wireless activity. Users typically give AirDefense high marks for support and scalability: 225,000 devices can be monitored per server. If sensors are cut off from the console, they will serve as stand-alone functions, and will set up their own mesh network to coordinate updates and to try to find their way back to the server.

Challenges: The visibility of the acquisition has raised questions from existing and prospective WIPS customers because, in nonindustrial markets, Motorola's WLAN is not a default player against Aruba and Cisco. Buyers will look for assurances that the AirDefense products will continue to be competitive as an independent overlay solution. It is important for Motorola to maintain high levels of service responsiveness to ensure a smooth transition. AirDefense has an extraordinarily broad array of features; however, simpler management schemes offered by other vendors have sometimes trumped better functionality. The system offers excellent sensor scalability, but users have reported some difficulties when attempting to consolidate control of distributed/remote sites under a central console.

Optimal-use case: AirDefense is an appropriate choice for users of Motorola/Symbol WLAN products, as well as for security-focused buyers with very large-scale monitoring needs and with high-end security monitoring needs.

Rating: Positive

Return to Top