Gartner

Research

Publication Date: 27 July 2010 **ID Number: G00205031**

MarketScope for Wireless LAN Intrusion Prevention Systems

John Pescatore, John Girard, Tim Zimmerman

Economic factors caused growth to slow in wireless LAN intrusion prevention systems in 2008 and 2009. Changing requirements and a maturing vendor landscape put a premium on new detection capabilities and increased levels of integration with network infrastructure.

WHAT YOU NEED TO KNOW

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

Wi-Fi support is increasingly a standard extension of corporate networks, and enterprises must ensure that vulnerability management and intrusion prevention processes are extended to cover wireless and wired networks. WLAN security monitoring in the form of wireless intrusion prevention systems (WIPSs) is required to ensure that supported WLAN performance is not impeded by interference or denial-of-service attacks, WLAN traffic is kept private and secure, users are prevented from installing unauthorized WLANs, and unsupported/unauthorized WLAN technologies are barred from operation. Strong regulatory requirements in government and retail have particularly strong influence on WIPS purchases.

WIPS capabilities can be implemented by using the integrated monitoring functions provided by the WLAN infrastructure vendor, or as separate "overlay" capabilities. The former may be less expensive, while the latter almost invariably provides stronger security capabilities through full-time monitoring. As wireless technologies emerge, the overlay systems will provide the most flexible approach for rapidly incorporating monitoring and intrusion prevention; however, for many situations, the cost will be higher.

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 is a soft radio design that can be deployed in dual 2.4/5GHz options where both radios can be on one band or different bands. The 802.11n specification provides dramatically 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 new wireless chipsets in 802.11n gear are configurable and frequency agile, which make them new potential targets.

Further advances in other wireless technologies and general concerns about the use of smartphones have carried the scope of 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 create an opportunity for WLAN IPS vendors to consider them as a direction for expanding business opportunities.

MARKETSCOPE

This MarketScope analyzes the performance of vendors that have focused on the WIPS market from the second half of 2009 through the first half of 2010. 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.

High-performance, secure wireless connectivity is now an expected feature of any enterprise network. Although the built-in security capabilities of enterprise-class WLAN access points and controllers have matured and stabilized around WPA2, a number of factors drive the need for wireless-specific security monitoring capabilities:

- Misconfiguration and misadministration of wireless access capabilities (often driven by operational demands that drive tactical actions that violate the official policies) result in vulnerabilities that real live attacks have continued to exploit.
- The emergence of new technologies, such as 802.11n, cellular 3G data services and Long Term Evolution (LTE), means that additional forms of wireless technology will be brought in by users before equipment security capabilities and company security practices have matured.
- Military and government security requirements demand the best security practices.
- Compliance authorities, such as the Payment Card Industry (PCI) and the Federal Information Security Management Act (FISMA), include requirements for ensuring that vulnerabilities in WLANs are remediated and that wireless access is monitored for potential intrusions.

To deal with the risks of wireless use, the demand for WIPS evolved over time. Gartner sees three primary use cases in the current environment (in order of importance):

- **Vulnerability management:** The ability to quickly detect and mitigate misconfigured or unmanaged (rogue) wireless access points. The latest PCI standards drive this requirement for many organizations.
- **Intrusion detection and prevention:** Active detection and detailed investigation of potential malicious actions, including actions such as "evil twin" false access points, denial-of-service attacks and unauthorized wireless networks.
- **Overall WLAN health/operations monitoring:** WLAN vulnerability assessment integrated into efforts to ensure overall WLAN availability and performance (for example, the use of WIPS data gathering for nonsecurity purposes and interference analysis).

Because the PCI changed the WLAN security requirements to ban the use of Wired Equivalent Privacy (WEP), we have dropped the use case for shielding WEP from our priority list.

Enterprises have several architectural choices for WIPS:

- **Infrastructure-based:** Using their operational access points as monitors when they are not transmitting. This has security shortcomings but is often the least-expensive approach, because no additional hardware needs to be procured and installed. Higher-end access points can include dedicated radios to perform IPS functions.
- **Overlay:** Deploying dedicated monitoring-only sensors that are separate from and in addition to the operational access points. This provides the broadest and deepest approach to security. The number of installed sensors may vary from one sensor per every five to 25 access points. The variation in sensor density is attributed to the square footage of the facility and the level of protection that is being deployed. This approach is also used where heterogeneous (multivendor) access points are deployed.
- **Hybrid:** Augment operational access point sensors with some number of dedicated sensors in high-risk areas. This represents a compromise between security and cost. A typical hybrid scenario might only use WIPS sensors per building, regardless of the number of operational access points.

We believe an important factor to consider is the need to monitor the growth of other forms of wireless communications outside the Wi-Fi bands, such as Bluetooth, WiMAX and, particularly, 3G/LTE. As metropolitan broadband wireless services become increasingly baked into

smartphones and laptops, enterprises will need to detect these wireless signals and determine whether their use represents a risk or exposure. Generally, there will not be enterprise infrastructure deployed for 3G/LTE or HSPA+, and overlay solutions will provide a large portion of the solutions needed to monitor these other services.

Market/Market Segment Description

The WLAN IPS market consists of products used for performing continual monitoring 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/LTE) penetrate, "rogue" problems will reappear, 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 continue to increase during the next three years, but at steadily declining growth rates and as infrastructure-based security monitoring capabilities. We have also seen the beginning of some demand for managed WLAN securing monitoring services, but this will not be a major trend before YE11.

Gartner estimates that global revenue in this market grew from $161 million in 2008 to $184 million in 2009, a one-year growth rate of 14%. This is much higher than Gartner's "no growth" assessment for enterprise WLAN infrastructure equipment in 2009, but is below our previously predicted growth rate of up to 30% for this period for WLAN IPS. We believe the growth rate slowdown is primarily due to three factors:

- 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.
- In keeping with the above trend, the acquisition of AirDefense by Motorola and AirMagnet by Fluke meant that these vendors were part of larger companies that focused on maximizing overall WLAN infrastructure or testing revenue (not just WIPS revenue).
- The PCI requirements for Wi-Fi rogue monitoring represented the largest market driver, but led to lower average deal sizes.
- General economic factors slowed spending on WLAN overall.

These factors will still be in play throughout mid-2011, so we are predicting that 2010 revenue will grow no more than 10%, and will reach $202 million. A rapid upturn in the global economy could result in higher growth, but other factors are not likely to change. As 3G/LTE starts to penetrate, Gartner believes that demand for wireless monitoring capabilities will see an increase, but this will not be a factor before 2012.

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.

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."

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 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.

Inclusion and Exclusion Criteria

This MarketScope evaluates vendors that actively compete through recognition and sales of WIPS products and services. All WLAN infrastructure vendors offer some basic security features, which become necessary to efficiently operate the infrastructure, including detection of rogue devices, monitoring of airwaves for attacks and misuse, the ability to detect misconfigured access points and wireless endpoints, and adjustments for quality-of-service and spectrum optimization. A vendor becomes *competitive* in this market when it does the following:

- Promotes its WIPS capability as a competitive advantage in its product/service descriptions, literature, white papers and website
- Presents itself in the market as a thought leader for WIPS practices
- Is perceived by Gartner clients, as evidenced through inquiries, as an influential WIPS vendor
- Competes in wireless markets by specific instances of leadership developed through its WIPS capabilities
- Is able to generate visibility, demand and competition solely on the basis of WIPS (this applies to any company with a WIPS capability, including infrastructure players)
- Offers advanced and use-case-specific features, including aggressive intrusion tracing with network-access-control-based isolation methods and remediation procedures against offending devices, detailed audit logs with forensic analysis, and compliance reporting keyed to major business practices and legislation mandates

Vendors Added or Dropped

No new vendors were added, and no incumbent vendors were dropped since the previous MarketScope.

Other Vendors

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

- **Meru:** This Wi-Fi infrastructure vendor has productized its WIPS solution, starting in mid-2010. Meru did not qualify for inclusion in the previous report and did not have a product on the market during the study period covered by this report.
- **Trapeze Networks:** This Wi-Fi infrastructure vendor did not qualify for inclusion in the previous report last year and declined to participate in this year's survey. It has not promoted a competitive WIPS position necessary to be recognized as a contender in Gartner client inquiries by peer vendors that Gartner considers to be qualified for this market segment.
- **Code-Red:** Code-Red's AirMarshal Wireless Management Software provides endpoint wireless protection but does not have all the central management capabilities required to meet the inclusion criteria, nor has Gartner seen the vendor in any enterprise competitions.
- **HP, Xirrus and Enterasys Networks (a division of Siemens Enterprise Communications):** These vendors offer basic WIPS but do not meet the competitive requirements set forth in the inclusion criteria for this report.
- **Zoho:** Its lightweight ManageEngine WiFi Manager was discontinued as of 4 May 2010.

Rating for Overall Market/Market Segment

Overall Market Rating: Promising

We rate this market as Promising, because Gartner expects to see slow, but steady, positive growth in WIPS investments for several years, as well as continuing enhancements and innovations by the companies that show leadership in WIPS. However, the viability of WIPS to be sustained and tracked as a separate market is waning. Basic WIPS features offered by WLAN infrastructure vendors will continue to improve and will become good enough for typical buyer needs by 2012. Stand-alone WIPS players will continue to play important roles, but the buying decision for WLAN infrastructure and IPS will be increasingly combined as buyers continue to upgrade to new-generation access points. Therefore, the opportunity for new stand-alone vendors to enter will be difficult. In 2011 research, Gartner expects to treat WIPS as a critical capability for WLAN security monitoring, rather than a separate market.

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

Evaluation Criteria	Comment	Weighting
Offering (Product) Strategy	This assesses 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 2010)

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 (Air Defense)				x	

As of 27 July 2010

Source: Gartner (July 2010)

Vendor Product/Service Analysis

AirMagnet

Description: AirMagnet offers two products that feature WLAN security monitoring. Both solutions are overlay implementations, which means that they require dedicated sensors and do not use the access points that may already be in place for wireless communications. AirMagnet Enterprise provides an easy-to-use console that incorporates monitoring and stateful analysis of WLAN traffic. Dedicated sensors perform local processing, which reduces the traffic load on the network and minimizes central points of failure. The full-featured solution supports full-packet capture, dedicated spectrum analysis and attack blocking, as well as enhanced compliance reporting and helpful step-by-step explanation and configuration. AirMagnet has obtained Common Criteria EAL 2 and FIPS 140-2 certification, which are often required for government installations. In addition to AirMagnet Enterprise, the company offers WiFi Analyzer Pro, which can be configured for performance monitoring and troubleshooting, as well as identify misconfigured and rogue access points.

Strengths: AirMagnet continues to have strong WLAN performance-monitoring and troubleshooting capabilities in an enterprise but also is being deployed by customers in security-only applications. 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 in record logs for up to three days in case of network interruption. AirMagnet's history and expertise in "sniffing" provide some of the most aggressive and detailed methods for tracing suspicious devices and data traffic through wired and wireless networks. AirMagnet submitted the largest example list for templates of automatically generated compliance reports. Revenue is respectable and viable.

Challenges: Wireless IPS is becoming a requirement for wireless implementations as wireless access continues to gain momentum for access layer connectivity, and is the de facto standard for guest access and temporary connectivity. Some usage scenarios do not require full-time security monitoring and, because AirMagnet is not a WLAN infrastructure vendor, it does not show up in competitions where time-slicing implementations meet the business requirements. AirMagnet continues to work through integration issues associated with being acquired by Fluke Networks. Although its network monitoring solution continues to be strong, it appears that AirMagnet has lost marketing momentum in the wireless IPS space.

Optimal-use case: AirMagnet is viable for WIPS scenarios where full-time scanning is needed and when decisions about the wireless environment need to be made at the sensor, such as

branch offices or mission-critical scenarios, where connection to a centralized server may not always be available. It is not a solution where wireless IPS needs can be implemented through time-slicing scanning efforts or a dedicated sensor within an existing access point.

Rating: Promising

AirPatrol

Description: AirPatrol declined to reply to the MarketScope survey, but it is ranked in this report because it is still recognized by Gartner as qualified to compete in this market. Because AirPatrol has appeared to focus more on specific requirements of narrow segments of the government market, we continue to give it a Caution rating. AirPatrol is a small company headquartered in Columbia, Maryland, with R&D facilities in Canada. For enterprise users, its solutions consists of Wireless Locator System, Wireless Policy Manager and Wireless EndPoint Client. AirPatrol provides a sensor that detects Wi-Fi and cellular signals, as well as its Rapid Deployment Sensor for field use.

Strengths: AirPatrol's primary strength has been its ability to detect the use of cell phones and cellular data services, which is a growing need. AirPatrol software-based sensor design supports simpler upgrades. AirPatrol provides very granular policy enforcement to detect particular uses of wireless communications. AirPatrol integrates to Check Point OPSEC and McAfee ePolicy Orchestrator.

Challenges: Gartner has not recently talked to clients using AirPatrol's solution, and AirPatrol did not provide any references. Although AirPatrol recently formed a Commercial Advisory Board, much of the company's sales focus has been on government buyers. AirPatrol has only minimal capabilities to support the management of WLANs. Because AirPatrol did not provide any revenue or installed base information, Gartner has to assume that it has not increased its installed base during the past year.

Optimal-use case: AirPatrol's optimal-use case is for government agencies 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 take the risk of using a small, opaque vendor.

Rating: Caution

AirTight Networks

Description: AirTight Networks is a security overlay provider 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 2009, continuing to prove that a stand-alone IPS company can buck the trend of infrastructure vendors selling bundled IPS. 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. Feedback from Gartner clients and reference customers continues to praise its overall ease of installation and use, as well as its treatment for different skill levels (console operators with limited knowledge get extra assistance). AirTight holds several patents for a trademarked marker packet technology, a method of using tagged packets for tracing wireless activity in a way that quickly determines whether the packets originated from the monitored network. This method is fast and efficient for accurate determination of rogue versus foreign/neighboring or unauthorized wireless activity.

AirTight has generated additional revenue through OEM license relationships with WLAN infrastructure vendors Enterasys Networks (a division of Siemens Enterprise Communications),

3Com/H3C/TippingPoint and HP ProCurve (Colubris), as well as go-to-market partnerships with WLAN infrastructure vendors Meru, Trapeze, Aerohive Networks and Nortel/Avaya, and security vendors McAfee, Qualys and Rapid7. The products are also available as software as a service (SaaS) via SpectraGuard Online, as well as for direct purchase. AirTight's drop-in SaaS package is affordable and was well-timed to PCI law fortifications that became important in 2009. A typical, but not exclusive, example would be retail operations where the budget to upgrade old WLANs is nonexistent, but operations funds can be obtained for service-based compliance-monitoring tools that require minimal training. In competitive situations, AirTight's costs are relatively inexpensive.

Challenges: Because AirTight is not a WLAN infrastructure vendor, it has relied on its partnerships with infrastructure vendors to bring it into many deals, rather than be automatically included in WLAN infrastructure buys. From a revenue perspective, AirTight has done well in licensing deals and go-to-market referral partnerships, because its technology works well, and its ease of use minimizes third-party bundling and support problems. 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 continue to grow customer service and support in line with its relatively strong success rates. As the market matures, and consolidations continue, AirTight could be an acquisition target for another infrastructure vendor or for a cloud security provider.

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 an additional vendor to provide WIPS in exchange for strong security and rapid deployment with reduced overhead to set up and configure. AirTight has proved to be popular when companies need to add monitoring at a time when they are not able to upgrade their infrastructure or not interested in upgrading it.

Rating: Positive

Aruba Networks

Description: Aruba Networks is recognized by Gartner clients as an established WLAN infrastructure and IPS vendor that can make its way onto a shortlist and compete with Cisco. Although its market share for WLAN infrastructure and WLAN IPS is much smaller than Cisco's, Aruba grew its revenue across all product lines through the tough second half of 2009, and showed good performance for the first half of 2010. Aruba's wireless product portfolio is based on access points that can be configured as dedicated sensors or hybrid access point/sensors. In 2008, Aruba acquired AirWave, which sold wireless system management tools that also had security-monitoring capabilities. Aruba's WIPS product line consists of 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, with CC EAL 4 certification in progress.

Strengths: Aruba is a proven longtime player in WLAN infrastructure with a history of successful competitive wins 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 give its offerings high marks for quality service and support, ease of deployment and ease of management. In 2010, Aruba added a SaaS program intended to target

a monthly rental cost that will undercut AirTight. Aruba's rogue scanning range on hybrid access points has been expanded to cover a much wider range of channels. In its latest release, the dwell time per channel has been cut in half, which means that scanning of a large range of frequencies will be accomplished more efficiently.

Challenges: Aruba's success is based primarily on selling its Controller family and access points against other WLAN infrastructure vendors (such as Cisco and Motorola), not on selling stand-alone WIPS products. Its new foray into SaaS may provide a new way to capture WIPS revenue but will need time to build a following. Aruba can partially manage third-party access points, but doing so with reduced functionality is not a strong selling point.

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. Gartner considers this type of product to be potentially transformational to branch office and home office security, but so far, it has not caused a marketwide competitive change in remote access security and product configurations. Aruba's low-cost access points may only appeal strongly to companies that are existing Aruba customers, because the required back-end gateway investment is potentially a barrier to companies that chose a different WLAN provider.

Aruba is also investing in virtual private network (VPN) and remote access technologies outside of its core WLAN and WIPS offerings, which will take it into enterprise VPN markets where it is not currently competitive against Juniper, Cisco, F5, SonicWALL, Microsoft and other long-term providers. Given Aruba's size, the new investment could be a resource drain, and the value is yet to be proved.

Optimal-use case: Aruba's WIPS module is appropriate for use with Aruba wireless networks, while RAPIDS 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

Cisco

Description: Cisco's wireless IPS function consists of its unlicensed adaptive Wireless Intrusion Prevention System (aWIPS) solution, Mobility Services Engine (MSE) and CleanAir. The wireless IPS capabilities integrated into the Cisco WLAN controllers and wireless control system (WCS) are unlicensed functionality that is used by 70% of the Cisco wireless installed base over existing access points. Its aWIPS solution is an overlay implementation using MSE that requires standard Cisco access points used as dedicated sensors/monitors. aWIPS provides an easy-to-use console that incorporates monitoring and stateful analysis of WLAN traffic. Cisco products are individually certified to FIPS 140-2. Common Criteria certification is in process. CleanAir is a newly released solution that incorporates spectrum analysis.

Strengths: Cisco's position in wired and wireless infrastructures and the breadth of its products mean it is automatically on the shortlists of enterprises of all sizes looking for an integrated wireless IDS or overlay solution. Cisco's aWIPS can be deployed using only operational access points as part-time sensors, or using extra access points as receive-only sensors, or a combination of both. The release of CleanAir in its 3500 series access point enables enterprises to deploy a spectrum analysis solution with not only an enhanced number of signatures but also better resolution than solutions that use existing chipsets, or time slice the data collection algorithm looking for rogue devices. Reference users report excellent management capabilities and integration for aWIPS.

Challenges: Cisco's WIPS communication continues to get lost in the breadth of Cisco's product family and is sometimes dismissed by clients that may not realize the significant progress and improvements that have been made. Gartner clients still do not recognize or understand how to take advantage of the aWIPS capabilities, and they often confuse aWIPS functionality with the integrated WLAN controller capabilities. For example, in a unified network scenario that is often proposed by Cisco as part of a new wireless network build-out, the user might have to deal with cross-configurations of standard and lightweight access points used in production and hybrid modes, WLAN controllers, a WCS console, MSEs and others. Cisco recommends that buyers use a combination of dedicated access points and production access points for monitoring 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.

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.

Rating: Promising

Motorola (AirDefense)

Description: Motorola acquired AirDefense in 2008, adding to its previous acquisitions of Symbol Technology and Wireless Valley to create an enterprise mobility portfolio. Motorola has branded the product line the AirDefense Services Platform, which consists of three models of management and storage appliances, one sensor-only model and four models of dedicated sensors that are combined with operational access points. AirDefense products may be purchased in a stand-alone manner or in a bundle with Symbol infrastructure.

Strengths: Motorola's (Symbol's) strength in the retail market gives AirDefense a strong position in being used to meet the PCI's requirements for WLAN security and rogue detection. Motorola has begun to aggressively attack the WLAN market, which should increase AirDefense's visibility in WLAN infrastructure deals outside the PCI space. AirDefense deployments have spanned the range from some of the highest sensor counts in the industry to smaller, stand-alone deployments, demonstrating a high degree of scalability and survivability. Motorola's design for combined access port/sensors supports more-complete monitoring. Sophisticated users rate AirDefense as having the most complete set of security and management capabilities.

Challenges: For less-sophisticated users, AirDefense's wide range of features increases the complexity of deployment and management. AirDefense's graphical user interface (GUI) has improved but is still complex for simple use cases. AirDefense's pricing generally comes in at the high end and requires buyers to value the detailed features.

Optimal-use case: AirDefense continues to be a strong choice for users of Motorola/Symbol WLAN products, such as in the retail industry, as well as for buyers with large-scale monitoring needs and with high-end WLAN security and performance monitoring needs.

Rating: Positive

RECOMMENDED READING

"Wireless Security Trends: Planning Principles for a New Decade"

"Magic Quadrant for Wireless LAN Infrastructure"

"What to Look for in a Wireless Intrusion Prevention System"

"Magic Quadrants and MarketScopes: How Gartner Evaluates Vendors Within a Market"

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.

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 with 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.

REGIONAL HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters
Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters
Gartner Australasia Pty. Ltd.
Level 9, 141 Walker Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Japan Headquarters
Gartner Japan Ltd.
Aobadai Hills, 6F
7-7, Aobadai, 4-chome
Meguro-ku, Tokyo 153-0042
JAPAN
+81 3 3481 3670

Latin America Headquarters
Gartner do Brazil
Av. das Nações Unidas, 12551
9° andar—World Trade Center
04578-903—São Paulo SP
BRAZIL
+55 11 3443 1509