Gartner

Research

Publication Date: 12 July 2011 **ID Number: G00213850**

MarketScope for Wireless LAN Intrusion Prevention Systems

John Girard, John Pescatore, Tim Zimmerman

The WLAN IPS market shows signs of growth after two slow years in a weakened economy. Payment Card Industry requirements, as well as a rush of consumer devices into the workplace, 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 WLANs continue to be compromised. WLAN exploits are not headline news in the media anymore, but represent security incidents that can be difficult and expensive to remediate. Reasons for compromise include continued use of legacy equipment, weak authentication protocol choices, unencrypted guest networks and public hot spots, other configuration mistakes, and the onslaught of personal wireless devices. Since manual sniffing methods have proven to be operationally expensive and insufficient, enterprises deploying WLAN infrastructure must give due consideration to WLAN intrusion prevention systems (WLAN IPSs).

Wi-Fi support is 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 WLAN IPSs 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 increasing influence on WLAN IPS purchases.

WLAN IPS 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.

Further advances in other wireless technologies and general concerns about the use of smartphones have carried the scope of WLAN IPS beyond Wi-Fi, and vendors in this market are expanding into Bluetooth, mobile phones, wireless cameras, cordless phones and other non-Wi-Fi services. These additional wireless signals can cause interference, expose information, 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 WLAN IPS market from the second half of 2010 through the first half of 2011. 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.

During the evaluation time frame, wireless networking in general and wireless security continued to mature. However, wireless networks are still operated by people who sometimes make mistakes, and wireless network access points are frequently misconfigured in ways that introduce vulnerabilities. Just like wired networks, wireless networks need to be monitored to both proactively detect vulnerabilities to accelerate mitigation and to quickly detect security incidents to support rapid incident response. Also, while the basic Wi-Fi technology is mature, what Gartner calls the "consumerization of IT" is driving demand for increased use of employee-owned devices with wireless access, such as iPhones and iPads. This increases the need for WLAN monitoring to support network access control (NAC) functions for allowing wireless access to users who are

allowed to use unmanaged devices. Demands for increased mobility have also led to pressure to use technologies, such as 802.11n, Long Term Evolution (LTE) and third generation (3G)/fourth generation (4G), in data devices before equipment security capabilities and company security practices have matured. All this adds up to a continuing need for wireless monitoring and intrusion prevention to mitigate risk.

To deal with the risks of wireless use, the demand for WLAN IPS continues to evolve. Gartner continues to see buyer interest driven by the primary use cases for WLAN IPS:

- Intrusion detection and prevention: Active detection and detailed investigation of potential malicious actions, including actions such as man-in-the-middle attempts, denial-of-service attacks and unauthorized wireless networks.
- Overall WLAN health/operations infrastructure monitoring: WLAN vulnerability assessment integrated into efforts to ensure overall WLAN availability and performance (for example, the use of WLAN IPS data gathering for performance analysis, troubleshooting and interference analysis).
- Vulnerability management: The ability to quickly detect and mitigate misconfigured or unmanaged (rogue) wireless access points. The latest Payment Card Industry (PCI) and government security standards drive this requirement for many organizations. However, the ability to pull a compliance report from a successful implementation of WLAN IPS could lull enterprises into a dangerous sense of complacency. Companies must remember that compliance is not the end of vulnerabilities, and does not equate to security. We predict that most successful WLAN attacks will exploit misconfigured access points and weakly defended consumer-grade end-user devices.

This year, buyers are showing increasing interest in the enforcement of no-wireless zone policies to allow them to not only monitor, but also conditionally block wireless transmissions of all types in controlled areas to prevent the use of wireless devices that can record high-quality sound, audio and video. Schools are a growing market for this purpose due to privacy concerns, while government agencies and businesses have information leakage concerns. Gartner sees this use case as limiting access in specific areas, rather than creating total bans on wireless.

WLAN IPS is an increasingly important component of WLAN infrastructure. Security has become "table stakes" for vendors in the WLAN infrastructure market — enterprises expect their WLANs to include some basic security monitoring capabilities (see "Magic Quadrant for Wireless LAN Infrastructure (Global)"). For many enterprises, what is built-in will be good enough, but just as in the wired network security market, many enterprises will require a separate security monitoring infrastructure. Enterprises have several architectural choices for WLAN IPS:

- Infrastructure-based: Using their operational access points as monitors when they are not transmitting. This has some security shortcomings, because sensing may not be as aggressive on shared access points, and sensors are placed for production, rather than listening. However, this approach is often the least expensive, because no additional hardware needs to be procured and installed. Higher-end access points can include dedicated radios for 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 and other physical features 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 a number of dedicated sensors in high-risk areas. This represents a compromise between security and cost. A typical hybrid scenario might only use WLAN IPS 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, particularly cellular data services, such as 3G/LTE. As metropolitan broadband wireless services become increasingly included with smartphones and laptops, enterprises will need to detect these wireless signals and determine whether their use represents a risk or exposure to devices on the network bridging directly to wireless Internet connectivity. Generally, there will be no enterprise infrastructure deployed for 3G/LTE or Evolved High-Speed Packet Access (HSPA+), and overlay solutions will be needed to monitor these other services. None of the offerings today fully support monitoring these signals, but Gartner believes this will be an important capability by 2H13.

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 determining the root cause of problems reported by users. WLAN system management capabilities continue to be important features evaluated by buyers. Gartner believes that the dual use of WLAN IPS across security and WLAN operations management will continue to increase during the next three years, but revenue growth will slow as infrastructure-based security monitoring capabilities become increasingly "baked in" features of WLAN infrastructure.

We have also seen some demand for managed WLAN securing monitoring services, driven mostly by merchants looking to satisfy PCI requirements for WLAN monitoring (see "Gartner Survey: Challenged U.S. Firms Seek Alternative PCI-Compliance Solutions"). Most of the demand exists only at very low price (cost/device/month) points, much lower than the traditional managed/monitoring firewall pricing. Price points of below $30/device/month support a profitable business model only for very lean, aggressive service providers (see "Using WLAN Managed and Professional Services to Expand Infrastructure Mobility").

Gartner estimates that global revenue in this market grew from $184 million in 2009 to more than $270 million in 2010. This represents a one-year growth rate of 50%, compared to growth of 14% in 2009. WLAN IPS market growth during this period was higher than the growth rate of the WLAN infrastructure market as a whole (see "Magic Quadrant for Wireless LAN Infrastructure (Global)").

We believe that the increase in market growth is due to two main factors:

- PCI requirements for Wi-Fi rogue monitoring are a primary demand driver in businesses that accept or process credit card payments. Average installation sizes have gotten smaller, but at the same time, there are an increasing number of deals and locations involved in both retail settings and in emerging markets, such as education. This part of the market is successfully served by the infrastructure vendors.

- Consistency, enforcement and reporting to maintain a solid wireless security posture at the high end of the market, which often favors overlay vendors.

At the same time, factors remain in play that could flatten WLAN IPS revenue growth in 2012:

- Enterprise perception of WLANs as mature technology, combined with acquisitions of WLAN IPS vendors by WLAN infrastructure vendors, will lead many companies to use operational access points or other work-arounds as monitoring solutions, instead of pursuing more-intensive, sensor-oriented strategies and sophisticated WLAN IPS installations.

- The sales of WLAN IPS into PCI environments could reach saturation in developed countries by 2013.

Considering the above factors, Gartner believes WLAN IPS market growth into 2012 will be approximately 25% to 30%, leading to an overall market size of $350 million.

Vendors in this market include WLAN infrastructure vendors that sell differentiated WLAN IPS 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 ability to fulfill the core requirements of WLAN IPS. Some WLAN IPS vendors also offer products or services for NAC, which is a related and complementary market; however, NAC solutions are typically not focused on wireless use cases. 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. WLAN IPS is a global market: average revenue by geographies breaks down as follows: North America, 66%; Latin America, 2%; Europe, 17%; Middle East and Africa, 4%; and Asia/Pacific, 12%.

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 forerunner 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 its 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, the loss of 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 at risk.

Inclusion and Exclusion Criteria

This MarketScope evaluates vendors that actively compete through recognition and sales of WLAN IPS 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:

- Declares its basic WLAN IPS capability and features clearly and competitively in its product/service descriptions, literature, white papers and website
- Is able to generate visibility, demand and competition solely on the basis of WLAN IPS (this applies to any company with a WLAN IPS capability, including infrastructure players)
- Is perceived by Gartner clients, as evidenced through inquiries, as an influential WLAN IPS vendor
- Provides evidence of revenue generation for WLAN IPS
- Competes in wireless markets by specific instances of leadership developed through its WLAN IPS capabilities
- Offers advanced and use-case-specific features, including aggressive intrusion tracing with NAC-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

All included vendors derive their largest percentage of income from business deals originating in North America, but also have reportable revenue in all other geographies, with the next largest percentages typically in Europe and Asia/Pacific. All included vendors have direct and/or reseller representation in all geographies.

Vendors that do not provide competitive evidence or otherwise cannot be gauged in Gartner analysis and third-party sources to have a competitive role in this market (as defined in the inclusion criteria) will be excluded.

Vendors Added or Dropped

Added

Bluesocket, Enterasys Networks, Meraki, Xirrus: These infrastructure companies offer viable WLAN IPS features that meet the inclusion criteria.

Dropped

AirPatrol: This vendor has stated that it has exited the WLAN IPS market and will focus on other areas.

Other Vendors

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

- **D-Link:** The vendor has a product in development, but it was not released during the survey period.
- **HP:** The vendor offers WLAN IPS, but did not meet the competitive requirements set forth in the inclusion criteria for this report. HP has a strategic partnership with AirTight Networks.
- **Meru:** The vendor launched a security and compliance suite that provides basic WLAN IPS and an optional PCI module, but did not meet the inclusion criteria set forth for this research.
- **Netgear:** The vendor did not have a differentiated product on the market during the study period covered by this research. Netgear is currently an OEM for AirTight.
- **Trapeze Networks/Juniper Networks:** This Wi-Fi infrastructure vendor was acquired by Juniper in 2010. Neither Trapeze nor Juniper has promoted a competitive WLAN IPS position.
- **Code Red Systems:** Code Red's AirMarshal Wireless Management Platform supports WLAN monitoring, and its AirStop agent can enforce WLAN security policies on laptops. However, Code Red does not support the centralized WLAN IPS functions required for inclusion, and Gartner has not seen the vendor in any WLAN IPS enterprise competitions.
- **WatchGuard:** The vendor offers basic WLAN IPS, but did not meet the competitive requirements set forth in the inclusion criteria for this research.

- **Zoho:** Its lightweight ManageEngine WiFi Manager was discontinued in 2010 and is no longer a supported product.

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 WLAN IPS investments for two to three more years, as well as continuing enhancements and innovations by the companies that show leadership in WLAN IPS. However, the viability of WLAN IPS to be sustained and tracked as a separate market is waning. Basic WLAN IPS features offered by WLAN infrastructure vendors will continue to improve and will become good enough for typical buyer needs by 2012. Stand-alone WLAN IPS 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 has found sufficient continuing interest in this area to conduct another MarketScope. WLAN IPS growth will be re-evaluated for 2012 to determine whether the market continues to stand alone or is regarded as a critical capability for WLAN infrastructure purchases.

Evaluation Criteria

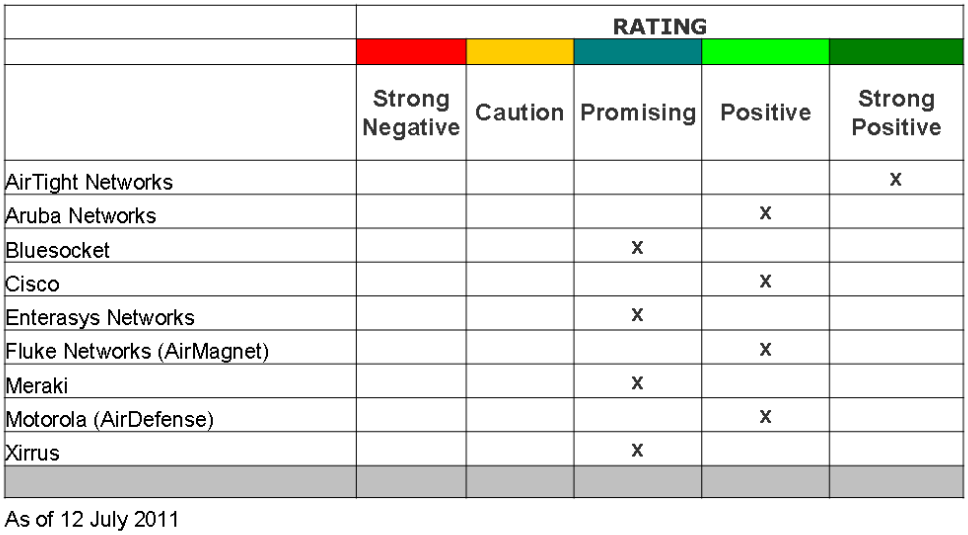
Table 1. Evaluation Criteria

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	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.	Standard
Overall Viability (Business Unit, Financial, Strategy and Organization)	Viability includes an assessment of the overall financial health of the organization and its commitment to the WLAN IPS 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.	High

Evaluation Criteria	Comment	Weighting
Marketing Execution	This entails the success and "mind share" of the product in the WLAN IPS 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 2011)

Figure 1. MarketScope for Wireless LAN Intrusion Prevention Systems



Source: Gartner (July 2011)

Vendor Product/Service Analysis

AirTight Networks

Description: Products include SpectraGuard Enterprise (WLAN IPS) and SpectraGuard Cloud Services, which now includes secure Wi-Fi Access, SpectraGuard Security Agent For Endpoints (aka SAFE, endpoint agent), and SpectraGuard Planner for planning WLAN and WLAN IPS deployments. Products are certified to Federal Information Processing Standard (FIPS) 140-2

and Common Criteria (CC) Evaluation Assurance Level (EAL) 2. AirTight's products are available as a hosted service, as a subscription service (SpectraGuard Cloud Services) and for direct purchase for on-site installation.

Strengths: AirTight has a multiyear history of strong revenue growth, and earns consistently positive user feedback. AirTight has done well by selling through partnerships with infrastructure vendors, licensing deals and go-to-market referral partnerships, because its ease of use minimizes third-party bundling and support problems. AirTight's drop-in software-as-a-service (SaaS) package is affordable and was well-timed to PCI law fortifications that became important in 2009. A typical, but not exclusive, example of use 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 monthly subscription costs are among the lowest available, and revenue from SaaS is growing fast.

AirTight holds several patents for a trademarked "marker packet" technology, a method of using tagged packets for tracing wireless activity to quickly determine 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.

Managed public Wi-Fi hot spot support is available and will allow AirTight's existing client base, particularly in retail, to add basic Internet access services without adding additional equipment. The price for sensors that double as hot spots becomes very low in quantity — not significantly different from a sensor alone. The hot spot feature will tap buyers who would like to have fully monitored Internet access in remote locations, but are otherwise not prepared to implement a full branch-office infrastructure.

Challenges: AirTight depends on security or compliance as buyer decision drivers, but is less competitively known for cost-benefits of cloud services and integrated, secure Wi-Fi access when network operations issues are the highest priority in a buying decision. AirTight must continue to maintain and grow customer service and support in line with its success rates.

Gartner believes that one of AirTight's best sales opportunities — namely, market demand for PCI-driven add-on solutions — could saturate in developing countries by 2013. 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, strong security overlay solution with minimal training/skill requirements from a separate security provider. AirTight is popular when companies need to add IPS and hot spot controls at a time when they are not upgrading their infrastructure. AirTight has sold particularly well in high security scenarios and to defend against PCI vulnerabilities. All products are available with cloud service administration, monitoring and control.

Rating: Strong Positive

Aruba Networks

Description: Aruba Networks is an established WLAN infrastructure and IPS vendor that successfully competes with major WLAN vendors by offering a complete solution, as well as separate sales for infrastructure and overlays. Aruba emerged from the economic slowdown of the past several years with healthy growth. Aruba's wireless product portfolio is based on access points that can be configured as dedicated sensors or hybrid access points/sensors. Aruba's WLAN IPS 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 WLAN IPS functionality as well. Aruba products are certified to FIPS 140-2 and CC EAL 2, with CC EAL 4 certification in progress.

Strengths: Aruba's infrastructure-based WLAN IPS capabilities are enhanced by the controller's firewall and by earlier acquisitions that have integrated into a fairly seamless system with strong security capabilities. Aruba's hybrid access point rogue scanning extends over a wide range of channels, with a small dwelling time per channel. Aruba is a good choice for wireless guest networks, where its NAC and WLAN IPS 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. References praise quality service and support, ease of deployment, and ease of management.

Low-cost remote access points that fully link enterprise security policy to remote small and home offices are available at prices below $100. These branch access points may 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.

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 WLAN IPS products. Aruba can partially manage third-party access points, but doing so with reduced functionality is not a strong selling point.

Aruba's 2010 foray into virtual private network (VPN) and remote access technologies has not generated competitive visibility against incumbent network infrastructure vendors tracked in Gartner forecasts and the "Magic Quadrant for SSL VPNs." Because these new investments were called out in last year's competitive road map, their lack of impact indicates that Aruba should seek other directions to expand beyond its historical product areas.

Optimal use case: Aruba's WLAN IPS 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. Aruba also is competitive and suitable for providing WLAN IPS separately from a company's main WLAN infrastructure provider.

Rating: Positive

Bluesocket

Description: Founded in 1999, Bluesocket began as a pioneer for overlay WLAN management. Bluesocket BlueSecure includes an integrated WLAN intrusion detection system (IDS) application that works in conjunction with Bluesocket's Virtual Wireless LAN (vWLAN) as a virtualized application or separately on a BlueSecure Controller. vWLAN itself combines a scalable overlay management system that combines with Bluesocket's own brand of dual-radio infrastructure Access Points to provide centralized network security monitoring and access controls in a manner positioned by the company to be similar in concept to NAC, providing features for wired, wireless and guest users. BlueSecure is primarily an alerting system: It provides more than 50 wireless alerts to inform enterprises of potential threats and also provides behavioral-based analysis. Access points can be configured to be sensors only or have the ability to time-slice while serving client traffic. Bluesocket access points are autodiscovered on the network and automatically configured based on the application policy. Target market segments include education, healthcare, public sector, enterprise, hospitality and financial services.

Strengths: Bluesocket has a solid security solution with a good following for BlueProtect and BlueSecure applications, as well as a software-based high-availability solution based on its vWLAN architecture. Architecturally, the BlueSecure application can be deployed as an

integrated solution or stand-alone with the ability to address compliance reporting requirements, such as PCI. As a key differentiator for scalability and customer growth, Bluesocket is relying on the virtualization of management and control on its software-based vWLAN solution that can run on a variety of server, blade or hypervisor platforms (for example, vWLAN is certified as "VMware-Ready"). Bluesocket maintains a "standards-agnostic" policy that is meant to allow it to monitor and manage infrastructure access points from any vendor. However, all known installations for BlueSecure are operating on an existing Bluesocket wireless network.

Challenges: Although it has been in the market for a long time, Bluesocket is a relatively small vendor that depends heavily on channels. The company needs to be more vocal about its overall differentiation, including this wireless network service application. In particular, it needs to release more high-value publicly accessible case studies. Bluesocket needs to leverage its capabilities to expand its market share as wireless intrusion detection system (WIDS) becomes table stakes functionality for enterprises deploying access layer wireless solutions.

Optimal use case: BlueSecure should be used for wireless IDS as part of all Bluesocket installations. Bluesocket is not a competitive choice for companies that seek a WLAN IPS vendor to be separate from their infrastructure provider or that want WLAN IPS as a cloud service.

Rating: Promising

Cisco

Description: Cisco has two wireless IPS applications. First, an unlicensed application that exists as part of WLAN controller (WLC) functionality that is used by 70% of the installed base, and second, an adaptive WLAN IPS (aWIPS) with advanced capabilities and reporting that is implemented in conjunction with the Mobility Services Engine. The aWIPS application provides an easy-to-use console that incorporates monitoring and stateful analysis of WLAN traffic. Historically, both applications were deployed using dedicated sensors for spectrum input to the applications. These were typically access points that were configured for "Monitor Mode" functionality. Cisco recently announced "Enhanced Monitor Mode" functionality as an upgrade for all access points that allow them to time-slice spectrum monitoring with client communications. Cisco products are individually certified to FIPS 140-2. Common Criteria certification is in process.

Strengths: As a leader in wireless networking, Cisco is well positioned to address customer requirements for overlay or integrate WLAN IPS with the Enhanced Local Mode (ELM) announcement, which meets PCI 1.2 recommendations. The aWIPS application provides scalability, as well as the ability to detect, locate, analyze and mitigate more than 200 attacks, vulnerabilities and rogue profiles. If needed, CleanAir provides that ability to scan in-band as well as non-Wi-Fi spectrum and non-Wi-Fi bands for threats. aWIPs provides the ability not only to detect, but also to apply countermeasures, as well as extensive reporting. Reference users report excellent management capabilities and integration for aWIPS.

Challenges: Cisco's WLAN IPS 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 understand how to take advantage of the aWIPS capabilities, and they often confuse aWIPS functionality with the integrated WLC capabilities. Clients report that they 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; we feel that the addition of ELM will make the discussion easier, since the solution can be implemented with the existing access points.

Optimal use case: Cisco is a strong choice for production wireless-access infrastructure-based monitoring for integrated and overlay solutions and should be deployed as an integral part of any

Cisco WLAN installation. Cisco can be used as an independent WLAN IPS overlay vendor, although typically its WLAN IPS is combined with infrastructure sales. Cloud-based WLAN IPS services are not currently available.

Rating: Positive

Enterasys Networks

Description: Enterasys WLAN IPS functionality is integrated into its wireless Advanced Services application, which is marketed as Wireless Management Suite, which also includes a network management module. The physical WLAN IPS implementation can be deployed in standard mode, which provides scanning when the access points are not serving clients, and hybrid solution or overlay sensor mode where dedicated sensors work in conjunction with the installed access points. Sensor mode access points allow the enterprise to simultaneously scan 2.4GHz and 5GHz bands for wireless threats. The WIDS functionality not only includes threat detection, auto classification and mitigation, but also provides location information while integrating with the wired intrusion detection application, which provides a seamless wired and wireless solution, as well as extends the functionality for integrated behavioral analysis.

Strengths: Enterasys has an extensive WLAN IPS solution that can be integrated into a multilayer holistic security posture. Enterprises can choose to deploy WLAN IPS with time-slicing or dedicated sensors, as well an extensive reporting capability that can be integrated into the Enterasys wired IDS where protection is extended to deep packet inspection and signature-based pattern matching. Finally, the end-to-end physical layer can be integrated into the Enterasys NAC application for additional functionality.

Challenges: Enterasys is successful at selling WLAN products into its existing customer base, but is typically not mentioned in open competition with other WLAN vendors, even though its wireless security solutions have been offered for more than six years. While the Enterasys solution can be implemented as a stand-alone solution with dedicated sensors, it is rarely deployed as an overlay and is only seen as part of an Enterasys infrastructure offering. With a strong offering, Enterasys needs to use this solution to open doors and increase market share as WLAN IPS functionality becomes table stakes for 802.11n enterprise installations.

Optimal use case: Enterasys should be used for wireless IPS as part of all Enterasys installations, and is appropriate for enterprises in education, hospitality and healthcare. Enterasys is not a competitive choice for companies that seek a WLAN IPS vendor to be separate from their infrastructure provider or that want WLAN IPS as a cloud service.

Rating: Promising

Fluke Networks (AirMagnet)

Description: AirMagnet Enterprise provides an overlay solution that uses dedicated sensors for data collection and provides an easy-to-use console that incorporates monitoring and stateful analysis of WLAN traffic. Sensors perform local processing, reducing the traffic load on the network and minimizing central points of failure. The 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. All threats and devices detected by AirMagnet Enterprise are correlated on the wired infrastructure and can be integrated into enterprise network and log management systems, as well as security information and event management (SIEM) platforms. AirMagnet has obtained CC EAL 2 and FIPS 140-2 certification, which are often required for government installations.

Strengths: AirMagnet is a full-featured product offering and provides differentiation in businesses with high security needs that deploy WLAN IPS as an overlay. AirMagnet sensors can perform full-time traffic and security analysis, even if they are disconnected from the centralized server. For large multinational installations, AirMagnet can also aggregate data from upstream distributed local servers for centralized compliance and security reports. Users that selected AirMagnet generally report these factors as the primary reasons for selection. As part of Fluke Networks, AirMagnet has been able to leverage the Fluke sales organization and has grown more than 70% in the last two years.

Challenges: Some usage scenarios do not require full-time security monitoring, and because AirMagnet is not a WLAN infrastructure product, it does not show up in competitions where time-slicing implementations meet the business requirements. In addition, other vendors are improving their radio technologies to allow for faster scans. For enterprises with high security postures, Fluke's AirMagnet is a prime candidate because of its dedicated and single focus on intrusion detection, mitigation and reporting within the wireless spectrum, whereas WLAN vendors may have differing core competencies.

Optimal use case: AirMagnet is viable for WLAN IPS scenarios where full-time scanning is needed or the enterprise has a high security posture that we often find in government or financial markets. It is also a candidate 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. AirMagnet is competitive and suitable to provide WLAN IPS separately from a company's main WLAN infrastructure provider, but is not available as a cloud service.

Rating: Positive

Meraki

Description: Founded in 2006 by academics from MIT, Meraki offers WLAN IPS as an embedded capability of its cloud-hosted management platform. The Cloud Controller receives information from time-slicing access points at each location and, while correlating data for each site, provides centralized, multisite management. Each node on a customer network maintains a persistent connection over the Internet via Secure Sockets Layer (SSL) to the Cloud Controller. Network administrators monitor and manage their entire network — including distributed sites — via a secure browser-based interface.

Strengths: Meraki's WLAN IPS solution is included with every installation; access points have the ability to scan both 2.4GHz and 5GHz channels while serving clients. One of the benefits of a cloud-based, vendor-hosted controller is continual and automatic update of rogue signatures. Additionally, the solution maintains activity logs, and Meraki has the ability to provide specific reporting — as needed — for troubleshooting or regulation-specific reports, such as PCI.

Meraki has improved its auditing capabilities since the publication of the "Magic Quadrant for Wireless LAN Infrastructure (Global)," although the changes were not available as standard in the product until the end of the evaluation period of this MarketScope. Third-party audits and penetration tests are performed on cloud-hosted services. New security tools for administrators include two-factor authentication; fine-grained, role-based administration; IP-restricted logins; password strength enforcement; and change management.

Challenges: Meraki provides WLAN IPS capabilities as part of its Cloud Controller platform, but buries this important wireless network service. Lack of competitive visibility to the Cloud Controller's security features reduces opportunities for potential buyers to consider Meraki's service options.

Meraki is one of the smallest and youngest vendors in the WLAN IPS market. Buyers will need to weigh interests in cloud service innovation against the company's time in the market and its ability to compete with many mature players.

Optimal use case: Meraki can provide a complete solution (infrastructure and security) that is appropriate for enterprises in higher education, K-12, hospitality and healthcare that are interested in cloud-based solutions.

Rating: Promising

Motorola (AirDefense)

Description: In 2011, Motorola Solutions, having separated from Motorola Mobility, continues to provide AirDefense, a strong and mature wireless LAN security and management offering in a WLAN IPS overlay solution. The WLAN IPS product line consists of the AirDefense Security and Compliance line of products and AirDefense Mobile, a software agent for laptop WLAN policy enforcement and monitoring. The AirDefense Services Platform provides the administrative and management console, and supports the WLAN Vulnerability Assessment Module and a variety of compliance reports. The Advanced Forensics module supports replay and analysis of past events, while the Mobile Workforce Protection Agent provides local policy enforcement when installed on laptops.

Motorola also offers the AirDefense Infrastructure Management, Network Assurance and Mobile products for management and troubleshooting of WLAN networks. The AirDefense products can be procured stand-alone or bundled with Symbol WLAN infrastructure products.

Strengths: Motorola is a leader in the WLAN infrastructure market, putting it in a strong position for AirDefense infrastructure WLAN IPS sales. It can leverage its strong sales channels and relationships in its traditional markets (including some very large retailers) into an advantage in the fast-growing K through 12 education market and federal government markets. The product line has a wide range of sensors and rack-mount appliances to scale across large and small deployments. AirDefense shows strength in large and distributed deployments. High-end users continue to rate AirDefense as having the most complete set of security and management capabilities. User feedback has improved, indicating that buyers are finding the product easier to install and understand than in past reviews. New ways to share workloads between individual radios in multisensor installations will reduce IPS scan times and help to prioritize scan orders for busy versus quiet channels. AirDefense is now available in a cloud service offering, but the rollout occurred too late to influence the ratings in this research.

Challenges: AirDefense's strengths can be weaknesses at the lower end of the market, as features and product line structure increase complexity. While Gartner has seen more aggressive pricing recently from Motorola, AirDefense usually is the highest priced in competitive procurements. Despite recent efforts, Motorola has little traction and few end-to-end solutions outside its traditional vertical industries, and has been under competitive attack in those traditional industries. While AirDefense earns some very large wins, Gartner inquiries regarding AirDefense are not frequently combined with Motorola WLAN or competing infrastructure products.

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. Buyers should investigate the new cloud service.

Rating: Positive

Xirrus

Description: Founded in 2004, Xirrus has an internally developed wireless IPS that is integrated into the access points that are used with its own phased array architecture. It is not intended to be sold as an overlay solution. For wireless intrusion events, each array has a dedicated radio that monitors the 2.4GHz and 5GHz spectra. The solution provides full-time monitoring, classification and mitigation.

Strengths: The strength of the Xirrus solution is the dedicated monitor in the array that allows not only for classification, but also for the mitigation of threats, as well as a built-in firewall, spectrum analyzer and other performance tools. In conjunction with its phased array architecture, which provides an additional coverage footprint, the implementation can be deployed using fewer sensors. The management interface allows for individual or group classification of all devices that attach, as well as management distribution of rogue profiles.

Challenges: The integrated IPS functionality of the multiradio Xirrus access point would create both price and logistics barriers to a broad coverage rollout intended as a pure overlay solution. The rest of the WLAN IPS industry is in a price war to lower the per-location cost of monitoring equipment.

While the solution provides reporting about rogues and attacks, it is light on reporting for regulation requirements, such as PCI. Additionally, the embedded nature of the solution, where the sensor may coreside with a four-,eight- or 16-radio array, means that the solution is limited to Xirrus installations. While the integrated nature of the solution may be construed as a benefit to Xirrus customers, the market has shown that the functionality is table stakes as a WLAN requirement, and clients do view that it has value.

Optimal use case: Xirrus should be used to provide its own WLAN IPS as part of all Xirrus installations. Xirrus is not a competitive choice for companies that seek a WLAN IPS vendor to be separate from their infrastructure provider or that want WLAN IPS as a cloud service.

Rating: Promising

RECOMMENDED READING

Some documents may not be available as part of your current Gartner subscription.

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

"Magic Quadrant for Wireless LAN Infrastructure (Global)"

"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.

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 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

Gartner