G00226398

MarketScope for Wireless LAN Intrusion Prevention Systems

Published: 2 August 2012

Analyst(s): John Girard, John Pescatore, Tim Zimmerman

Wireless LAN intrusion prevention systems address evolving wireless security threats. WLAN IPS is a distinct market, but baseline security is increasingly satisfied by products and capabilities from WLAN infrastructure vendors.

What You Need to Know

This document was revised on 13 August 2012. The document you are viewing is the corrected version. For more information, see the Corrections page on gartner.com.

Wi-Fi support is a standard extension of corporate networks, and enterprises need wireless LAN (WLAN) intrusion prevention system (IPS) tools to ensure that vulnerability management and intrusion prevention processes are extended to cover wireless extensions to wired networks. WLAN IPS also plays an important role to ensure that supported WLAN performance is not impeded by interference or denial-of-service (DoS) attacks, WLAN traffic is kept private and secure, users are prevented from installing unauthorized WLANs, and unsupported/unauthorized WLAN technologies are barred from operation.

WLAN exploits require physical proximity to the target network and are thus much less likely to occur than threats that are delivered over the Internet. However, for the same reasons, WLAN exploits can be targeted to cause significant location-specific 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 IPSs.

Strong regulatory requirements in government and retail have influenced many WLAN IPS purchases. The WLAN IPS process continues to draw interest as a critical operational security concern for those companies that need the most rigorous wireless security measures for a variety of reasons, typically related to compliance with strict regulations involving privacy of classified or sensitive data.

WLAN IPS capabilities can be implemented by using the integrated monitoring functions provided by the WLAN infrastructure vendor as part of the access points, as separate "overlay" capabilities that require separate sensors, or the use of multiradio sensors that can be used simultaneously as access points (APs) and sensors. The former may be less expensive, while the latter almost invariably provides stronger security capabilities through full-time monitoring. Over this evaluation period, Gartner has seen that the majority of enterprises are looking at integrated IPS and infrastructure solutions to meet their WLAN risk requirements, with overlay demand continuing for specialized and high-security use cases.

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, active RFID, cordless phones and other non-Wi-Fi services. In particular, Gartner believes that "my Wi-Fi" devices (inexpensive bridges between Wi-Fi and 3G/4G services) will become the next rogue problem, requiring WLAN IPSs to add 3G/4G detection capabilities.

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 2011 through the first half of 2012. 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 APs are frequently misconfigured in ways that introduce vulnerabilities. A recent Gartner survey showed that, while 85% of enterprises already had or were adding wireless for mobile connectivity, they were not getting additional staff to manage the additional wireless components. Additionally, of those with a WLAN installed, only 2% were aware of the design parameters — including security — that were used for implementing the network (see "Use Best Practices to Implement a WLAN").

Just like wired networks, wireless networks need to be monitored to 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, and 4G/Long Term Evolution (LTE), 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, DoS attacks and unauthorized wireless networks. We believe that comprehensive intrusion prevention is only used by a small portion of the target market, but the ability to disconnect suspect connections is a minimum requirement.
- 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 and compliance verification: The ability to quickly detect and mitigate misconfigured or unmanaged (rogue) wireless APs. The latest 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 APs and weakly defended consumer-grade end-user devices.

WLAN IPS is an important and expected 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 the Wired and Wireless LAN Infrastructure"). 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 APs as monitors when they are not transmitting. This has some security shortcomings, because sensing may not be as aggressive on shared APs, and sensors are placed for production, rather than listening. However, this approach is often the least expensive in terms of installation, training and complexity, because no additional hardware needs to be procured and installed. Higher-end APs can include dedicated radios for IPS functions.
- Overlay: Deploying dedicated monitoring-only sensors that are separate from and in addition to the operational APs. 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) APs are deployed.
- Hybrid: These augment operational AP sensors with a number of dedicated sensors in high-risk areas. This can be done with dedicated receive-only sensors, or by using multiradio sensors

that can be used simultaneously as APs and sensors. This represents a compromise between security and cost. A typical hybrid scenario might only use a few WLAN IPS sensors per building, regardless of the number of operational APs.

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 or protocols, particularly cellular data services, such as 4G/LTE deployed in femtocells (see "Maximize Enterprise Mobile Security by Adding Femtocells"). 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 non-Wi-Fi signal monitoring, 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 of all or a part of the wireless spectrum 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. 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 were not historically 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 geography: North America, 64%; Latin America, 3%; Europe, 12%; Middle East and Africa, 3%; and Asia/Pacific, 13%.

WLAN IPS vendors fall into three groups:

- Specialty vendors that typically sell WLAN IPS as stand-alone products and services. Stand-alone WLAN IPS may be sold directly to be implemented as an independent overlay solution on top of an existing WLAN or without any WLAN at all as part of a "no wireless" policy. Vendors in this group may license their technology to companies in the other two groups. Overlay systems will provide the most flexible approach for rapidly incorporating monitoring and intrusion prevention, especially as new wireless signaling technologies appear that are not natively monitored by incumbent WLAN infrastructure; however, for many situations, the cost will be higher.
- WLAN infrastructure vendors that provide basic WLAN IPS capability only as part of their own infrastructure solutions. All of the WLAN infrastructure providers offer basic access controls and IPS detections in their product lines. For many companies, these included features will be good enough when combined with LAN access controls based on Wi-Fi Protected Access 2 (WPA2) and a basic guest networking policy. Vendors in this group may license their technology from companies in the first group.

- WLAN infrastructure vendors that sell WLAN IPS stand-alone and as part of their own infrastructure solutions. Vendors in this group typically acquired WLAN IPS technology that has a stand-alone buyer constituency. Vendors in this group may enjoy some success in selling their products to companies that own different infrastructures, as overlay solutions, and they can also use WLAN IPS as a sales tool to attract prospects to migrate away from other infrastructure vendors.

The continuation of WLAN IPS as a separate buying center and a distinct market is challenged by the fact that groups two and three substantially outnumber the specialty vendors in quantity and in terms of WLAN market share. As a result, it is difficult to obtain WLAN IPS unbundled market data separated from WLAN infrastructure. The bulk of innovation for new detection and mitigation methods no longer clearly rests with specialty vendors. The majority of buyers is looking for simple interference analysis and performance assistance, rather than sophisticated WLAN IPS, unless required to provide more-advanced protection by regulations or their own security risk profiles. Innovations requiring substantially new signal analysis might occasionally tip the advantage back to the first group, but the momentum will remain in favor of infrastructure vendors.

For a detailed description of the core capabilities of WLAN IPS products, see "What to Look for in a Wireless Intrusion Prevention System" (note: this document has been archived; some of its content may not reflect current conditions).

Gartner estimates that for 2012, the global revenue in this market will be approximately 350 million, up about 30% from 270 million in 2010. This is a deceleration from the 50% growth rate between 2009 and 2010, and is in line with our prediction last year.

High-security installations (for example, government use cases) and retail PCI requirements for Wi-Fi rogue monitoring are the major drivers for sophisticated WLAN IPS installations. WLAN IPS is being turned up in more locations as retail businesses expand storefronts in the current economy. However, we continue to believe that sales of WLAN IPS into PCI environments could reach saturation in developed Western markets by 2013. Two potentially interesting new competitive areas that can generally stimulate the market involve fast network access control responses to personal hot spots (generically known as my Wi-Fi) as well as unknown or misconfigured smartphones and tablets resulting from bring your own device (BYOD) activities. BYOD mitigation provides opportunities to partner with mobile device management vendors (see "Magic Quadrant for Mobile Device Management Software"). Also, the rise of competitive solutions, such as 4G/LTE femtocells can create demand for new monitoring categories that would be served most quickly by overlay vendors.

The majority of potential buyers perceive WLAN IPS as mature technology to be obtained from their WLAN infrastructure providers, and seek only basic intrusion monitoring as part of a larger effort to maintain good signal quality and performance. All vendors in this market have methods to identify rogues, and can limit connectivity to individual users and APs, as well as supply forensic information for more-detailed investigations. Companies that have implemented WPA2 security with Extensible Authentication Protocol — Transport Layer Security (EAP-TLS), for example, feel less pressured to identify rogue devices with urgency.

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 APs and wireless endpoints, and adjustments for quality of service and spectrum optimization. A vendor becomes *competitive* in this market when:

- It declares its basic WLAN IPS capability and features clearly and competitively in its product/ service descriptions, literature, white papers and website.
- Its WLAN IPS can be purchased by end-user companies under the vendor's brand name.
- It is able to generate competitive visibility, demand and competition solely on the basis of WLAN IPS. Evaluation factors include Gartner client interest, as evidenced through inquiries, as well as through public sources, including other published reviews, Gartner and non-Gartner conference presence, etc.
- It provides evidence of revenue generation from WLAN IPS.
- It competes in wireless markets by specific instances of leadership developed through its WLAN IPS capabilities.
- It demonstrates addition of unique and competitive value if providing WLAN IPS through a license with another vendor in the MarketScope.
- It 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 legislated mandates.

All vendors included in this MarketScope 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 by Gartner analysis and third-party sources to have a competitive role in this market (as defined in the inclusion criteria) may be excluded.

Vendors Added or Dropped

Added

No vendors were added to this report.

Dropped

Dropped vendors did not report revenue associated with WLAN IPS or appear to use it for competitive differentiation in the selling process. These vendors are not meeting the general competitive visibility criteria of the inclusion requirements, nor providing other forms of evidence of WLAN IPS market presence. The three vendors dropped from this report are: Bluesocket (acquired by Adtran), Enterasys Networks, and Xirrus.

Other Vendors

Several vendors are known historically in the context of this MarketScope, but are not ranked.

- AirPatrol exited the WLAN IPS market in 2010 to work on specialized federal markets, and in 2011 began to developed context-aware mobility security products. The AirPatrol ZoneDefense product provides wireless monitoring for WLAN and cellular signals, but does not meet the functional requirements to be included in the WLAN IPS MarketScope.
- D-Link has developed some in-house capability, but had not generated competitive visibility during the study period.
- HP has a strategic partnership with AirTight Networks, but does not separately meet the competitive visibility requirements for inclusion.
- Meru Networks launched a security and compliance suite that provides basic WLAN IPS and an optional PCI module, but did not meet the visibility and evidence inclusion criteria set forth for this research.
- Netgear does not have a differentiated WLAN IPS capability that would meet the competitive visibility requirements for inclusion.
- Juniper Networks acquired Trapeze Networks in 2010. Neither Trapeze nor Juniper has promoted a competitive WLAN IPS position.
- Code Red Systems does not support the centralized WLAN IPS functions required for inclusion.
- WatchGuard Technologies offers basic WLAN IPS, but did not meet the visibility and evidence inclusion requirements set forth in the inclusion criteria for this research.
- Zoho's lightweight ManageEngine Wi-Fi 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 because basic WLAN IPS features offered by WLAN infrastructure vendors will continue to improve and will become good enough for typical buyer needs by 2013. 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 APs. Therefore, the opportunity for new stand-alone vendors to enter the market will be difficult. In 2012 research, Gartner has found sufficient continuing interest in this area to publish another MarketScope. WLAN IPS growth will be re-evaluated for 2013, 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, 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
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 (August 2012)

Figure 1. MarketScope for Wireless LAN Intrusion Prevention Systems

	RATING				
	Strong Negative	Caution	Promising	Positive	Strong Positive
AirTight Networks					x
Aruba Networks				x	
Cisco				x	
Fluke Networks				x	
Meraki			x		
Motorola				x	

As of August 2012

Source: Gartner (August 2012)

Vendor Product/Service Analysis

AirTight Networks

AirTight has a multiyear history of strong revenue growth, mostly in North America, and sells well in high-security shops. Significant revenue, however, comes from retailers with large numbers of locations with limited budget for equipment and little or no distributed IT staff. In these situations, operations funds can often be obtained for retail service-based compliance-monitoring tools that require minimal training, which can be satisfied by AirTight's extensive and easy-to-read product and technology tutorials. Products include SpectraGuard Enterprise (WLAN IPS) and AirTight Cloud Services, including AirTight Secure Wi-Fi Access, SpectraGuard Security Agent for Endpoints (Safe), and SpectraGuard Planner for planning WLAN and WLAN IPS deployments. AirTight's products are available as a hosted service, as a subscription service (AirTight Cloud Services) and for direct purchase for on-site installation. Managed service now accounts for over 50% of company revenue. Several WLAN infrastructure providers license AirTight as a private-label IPS. Products are certified to Federal Information Processing Standard (FIPS) 140-2 and Common Criteria (CC) Evaluation Assurance Level (EAL) 2. AirTight has added BYOD support to SpectraGuard through its device fingerprinting techniques and third-party mobile device management (MDM) agent feedback to enhance wireless network access controls for roaming mobile devices. It explains BYOD options prominently on its website.[1]

Strengths

- AirTight's Marker Packet technology is a fast way to identify rogue traffic over the air, providing a high-confidence means to associate traffic with wireless senders.
- Packet frames are transmitted with signatures that are preserved as traffic moves through wired and wireless networks. This method is a strong network-independent solution in terms of the primary goal of a WLAN IPS product to swiftly categorize devices and take IPS actions.

- Managed public Wi-Fi hot spot support was made available as a software enhancement during the last reporting period and is available in hybrid APs at a price point, in quantity, similar to the basic sensor, which is among the lowest in the market.

Challenges

- AirTight depends heavily on high security and/or PCI compliance as buyer decision drivers where scalable network operations issues are a critical business decision.
- Buyers are less likely to know of AirTight when making competitive decisions for cloud services and integrated, secure Wi-Fi access.
- With the addition of hot spot service, AirTight is no longer a pure WLAN IPS overlay player. On the other hand, AirTight is not equipped to become a full-feature infrastructure player that can compete head-on with WLAN infrastructure leaders.

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 a good choice 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. Retail use cases continue to be popular. All products are available with cloud service administration, monitoring and control.

Rating: Strong Positive

Aruba Networks

Aruba Networks is an established WLAN infrastructure and IPS vendor that competes strongly with the oldest incumbents, offering all combinations of wireless infrastructure, hybrid systems and overlays. Aruba's access points can be configured as dedicated sensors or hybrid APs/sensors. Aruba can utilize third-party APs as sensors, and provides wired-side NAC overlays. Aruba's WLAN IPS product line includes three categories of APs, the Mobility Controller for real-time AP and sensor coordination, the AirWave wireless management suite that manages rogue containment, reporting, visualization and other core security and administration functions, and the Aruba Wireless Intrusion Prevention module for use with the Aruba Controller's ArubaOS software (the infrastructure solution). Aruba continues to be responsive to the needs of government and other high-security industries. Since last year, Aruba obtained CC EAL 4 certification for the Aruba Mobility Controller[2] and all series of Aruba APs. All products offer encryption certified to FIPS 140-2. Aruba also has access management and BYOD support functions to the APs and mobility controller. These allow an Aruba network to identify the types of devices connecting and then leverage Aruba's ClearPass product for NAC support.

Strengths

- Aruba's hybrid access points are efficient at channel scanning, needing only a small and adjustable dwelling per channel.
- In addition to hybrid AP/sensors and a traditional security sensor, Aruba also offers a spectrum monitor sensor for dedicated network health and performance management.
- 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.
- The entire product line has a clear continuity of design, and the management interfaces have continually improved and set good examples for ease of use.
- The management console summarizes critical events and actions, minimizing the need for manual data mining. For example, the default rogue dashboard combines simple graphical elements with small detail tables that display only need-to-know data.

Challenges

- Aruba makes it easy for users to review and tune detection rules, in dynamic environments, but administrators must take care to review intrusion detection system (IDS) profiles to classify dangerous versus nondangerous neighboring devices.
- Aruba's "instant" mode allows operational simplification by placing controller functions to be virtualized in the access points, but buyers must monitor to maintain parity of policy between instant and controller-based AP operations.
- In 2009, Aruba started offering remote IPS extensions through its VPN gateways and low-cost remote office VPN APs. User feedback suggests that the VPN products have not broadly enhanced buying decisions for WLAN IPS.

Optimal Use Case

Aruba is well-suited for companies that want fast rogue detection and comprehensive reporting as part of a complete infrastructure purchase. Aruba also is competitive and suitable for providing WLAN IPS separately from a company's main WLAN infrastructure provider. Aruba is a good choice for wireless guest networks, where its NAC and WLAN IPS combine for a consistent defense against wired and wireless visitors.

Rating: Positive

Cisco

Cisco is the largest vendor and market share leader in the enterprise wired and wireless infrastructure market. Cisco has two wireless IPS applications. First, Cisco has a basic WLAN IPS application that is unlicensed and exists as part of WLAN controller (WLC) functionality. This

solution is used by 70% of Cisco's installed base and can be managed through the WLC interface or through Prime NCS, Cisco's network management application. The second solution is an adaptive WLAN IPS (aWIPS) application with advanced capabilities and reporting that is licensed separately and sold in conjunction with or runs on an existing Mobility Services Engine (MSE) appliance. The aWIPS application is a more comprehensive solution that provides an easy-to-use console that incorporates monitoring and stateful analysis of WLAN traffic for users that need more-advanced capabilities. Prime NCS offers management capabilities for wired and wireless infrastructure, as well as aWIPS functionality. Historically, both applications were deployed using dedicated sensors for spectrum input to the applications, these were typically APs that were configured for monitor mode functionality. Cisco now has Enhanced Local Mode (ELM) functionality as an upgrade for all APs that allow them to time-slice spectrum monitoring with client communications or can use the Clean Air input from APs that have the dedicated spectrum analysis functionality in the AP. The Cisco 3600 series APs include a modular design, and the first module Cisco plans to release (4Q12) will include full-spectrum RF visibility and dedicated monitor mode capability.

Strengths

- Cisco can address a diverse set of customer requirements for overlay or integrated wireless IPS with monitor mode, ELM or Clean Air.
- CleanAir is especially helpful for enterprises to detect and mitigate Wi-Fi and non-Wi-Fi threats while simultaneously serving clients in both the 2.4GHz and 5GHz bands.
- The aWIPS application provides scalability, as well as the ability to detect over 200 attacks, vulnerabilities and rogue profiles. aWIPS provides not only the ability 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 unless they have a specific need for defined functionality.
- Gartner clients still do not recognize nor understand how to take advantage of the aWIPS capabilities, and they often confuse aWIPS functionality with the integrated WLC capabilities. As a result, the opportunity to upsell to the aWIPS over basic functionality is often lost, and buyers are not getting the full advantage of WLAN IPS, even though Cisco has done an excellent job marketing CleanAir.
- Buyers will need to do their own research and homework to understand the range and extent of available options for WLAN IPS, and related areas such as wireless BYOD security, rather than expect to get the full message from Cisco and Cisco's sales channel.

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.

Rating: Positive

Fluke Networks

Fluke Networks' AirMagnet Enterprise is a dedicated sensor overlay system aimed at enterprises that want strong spectrum analysis combined with security monitoring, as compared to using operational APs as security sensors. The AirMagnet architecture uses smart sensors to allow collections and analysis to continue during interruptions in connectivity to the management server, and supports a distributed "manager of managers" approach often needed in large-scale, global deployments. Sensors perform local processing, reducing the traffic load on the network and minimizing central points of failure. With v10, PC software sensors are available to extend rogue detection, and to monitor client performance and health. Fluke Networks offers other AirMagnet modules for planning and managing WLANs, such as AirMagnet Spectrum XT, Survey/Planner, VoFi Analyzer and Wi-Fi Analyzer. Cisco includes a subset of AirMagnet Enterprise, and offers a version of AirMagnet Planner to Cisco Small Business customers. AirMagnet has obtained CC EAL 2 and FIPS 140-2 certification, which are often required for government installations.

Strengths

- The solution supports full-packet capture, spectrum analysis and attack blocking, as well as compliance reporting and step-by-step explanation and configuration.
- All threats and devices detected by AirMagnet Enterprise are correlated on the wired infrastructure.
- The management console provides a rich mix of drill-down data views and high-level graphic dashboards. Users that selected AirMagnet generally report these factors as the primary reasons for selection.

Challenges

- Fluke Networks is not in the WLAN infrastructure business, and is generally perceived as a network certification, troubleshooting and monitoring company, rather than an IPS provider.
- Because Fluke Networks is the last of the pure-overlay vendors in the market study, AirMagnet Enterprise can only compete where an overlay solution is desired.
- Buyers comparing road maps for wireless BYOD security will note that Fluke has only a limited presentation on this subject,[3] involving a partnership with Cisco.

Optimal Use Case

AirMagnet is a strong choice where dedicated WLAN monitoring solutions are required for high-security needs. The sensor architecture also supports distributed scenarios where connectivity back to a management server may be intermittent. Environments where Fluke monitoring equipment is in use on the wired network may also see advantages in using AirMagnet as the WLAN IPS solution.

Rating: Positive

Meraki

Meraki is an innovative vendor that offers its solution globally. It is heavily installed in North America and has good references for Latin America. The Meraki WLAN IPS solution is an embedded capability of its cloud-hosted management platform. The Cloud Controller receives information from time-slicing APs at each location. Correlating data for each site provides centralized, multisite management. Meraki has a multitenant architecture to isolate production networking, management and security functions between its customers. Meraki APs can also be tagged as dedicated wireless intrusion detection system (WIDS)/Wi-Fi Protected Setup (WPS) radios. A radio's state can be toggled at any time via the dashboard. Each node on a customer network has full-spectrum scanning capabilities, because it maintains a persistent connection, over the Internet via SSL, to the Cloud Controller. Network administrators monitor and manage their entire networks — including distributed sites — via a secure browser-based interface. Meraki also offers Systems Manager, a cloud-based MDM service[4] that can interoperate with Cloud Controller.

Strengths

- Meraki's IPS solution is included with every service installation.
- APs have the ability to scan both 2.4GHz and 5GHz channels while serving clients.
- No on-site controllers are required, regardless of the size of individual site WLAN installations or the number of distributed locations.
- Sensors are easy to deploy and automatically discover the Meraki cloud application. Core security features such as rogue signatures are continuously updated.

Challenges

- Buyers of Meraki infrastructure services may be unaware of and lose opportunities to deploy Meraki's WLAN IPS capabilities because the features are not promoted. For similar reasons, buyers seeking dedicated WLAN IPS services may overlook the ability to deploy the solution as a stand-alone offering.
- High-security users should note that Meraki has not released a FIPS-validated solution.
- Meraki is a small (compared to others in this report), private company, so prospective customers should verify Meraki's local support capabilities within emerging markets as part of their evaluation processes.

Optimal Use Case

Meraki can be used for WLAN IPS as part of all Meraki installations, and is strongly represented in the education, retail, distributed enterprises, healthcare and hospitality industries.

Rating: Promising

Motorola

Acquired by Motorola in 2008, AirDefense is now part of Motorola Solutions. Motorola now offers AirDefense technology in versions oriented for WLAN operations (AirDefense Infrastructure Management and AirDefense Network Assurance), along with AirDefense Security and Compliance as the WLAN IPS offering. Within this product line, the AirDefense Services Platform can use any of the Motorola AP platforms as a sensor, in dedicated mode or hybrid mode for dual- and tri-radio hardware. There are three management server appliances models, as well as virtual and cloud-based management platform options. A software version, AirDefense Mobile, is also available for monitoring and enforcing WLAN policy locally on laptops. AirDefense has a number of modules, such as Advanced Forensics and Vulnerability Assessment. Motorola also has managed services and software as a service (SaaS) offerings built around the AirDefense Service Platform. Motorola has submitted a FIPS evaluation application for the ADSP software, which, as of the end of the study period, was in the initial user test phase. Buyers with specific regulatory needs should monitor test progress. The AP-7131N is FIPS 140-2 validated and can be used as a sensor, and AirDefense can monitor for use of other FIPS 140-compliant products.

Strengths

- Gartner continues to rate Motorola as a leader in the WLAN infrastructure market, allowing AirDefense to address the demand in infrastructure WLAN IPS sales.
- Since AirDefense also provides a stand-alone sensor, it is a strong competitor when overlay WLAN IPS capabilities also are required.
- The AirDefense architecture and sensor line support scaling from large to small environments. While Gartner has yet to see major demand for managed services around WLAN IPs, Motorola's offering does support early movers in that area and has met with success.

Challenges

- Where Motorola is the WLAN provider, AirDefense is in a strong position; however, most Gartner clients have large Cisco or Aruba WLANs, where AirDefense can only compete for overlay needs.
- When buyers select other products instead of AirDefense, the major reasons are cost and/or complexity in environments where scale is not a major issue.

Optimal Use Case

AirDefense continues to be a strong choice for users of Motorola 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. Enterprises moving to WLAN monitoring, but concerned about staffing, should investigate Motorola's managed service offering or new WLAN cloud services that include WLAN IPS as a service.

Rating: Positive

Recommended Reading

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

"Use Best Practices to Implement a WLAN"

"Maximize Enterprise Mobile Security by Adding Femtocells"

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

"Magic Quadrant for the Wired and Wireless LAN Infrastructure"

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

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

Evidence

[1] AirTight's BYOD solution.

[2] Aruba mobile device access control.

[3] Fluke's mention of BYOD for small businesses.

[4] Meraki mobile device management.

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.

In the below table, the various ratings are defined:

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
USA
+1 203 964 0096

Japan Headquarters
Gartner Japan Ltd.
Atago Green Hills MORI Tower 5F
2-5-1 Atago, Minato-ku
Tokyo 105-6205
JAPAN
+ 81 3 6430 1800

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

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

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