Gartner

Research

Publication Date: 14 April 2009 **ID Number: G00167303**

Magic Quadrant for Network Intrusion Prevention System Appliances

Greg Young, John Pescatore

The network IPS market continues to mature and evolve, and has become a due-diligence safeguard. Evolving threats mean that vendors that stand still risk becoming irrelevant.

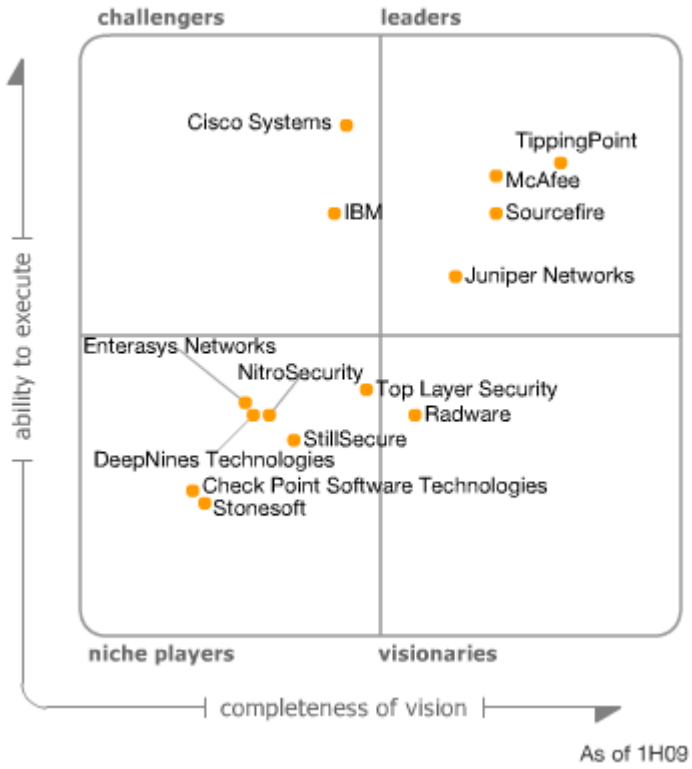
© 2009 Gartner, Inc. and/or its Affiliates. All Rights Reserved. Reproduction and distribution of this publication in any form without prior written permission is forbidden. The information contained herein has been obtained from sources believed to be reliable. Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information. Although Gartner's research may discuss legal issues related to the information technology business, Gartner does not provide legal advice or services and its research should not be construed or used as such. Gartner shall have no liability for errors, omissions or inadequacies in the information contained herein or for interpretations thereof. The opinions expressed herein are subject to change without notice.

WHAT YOU NEED TO KNOW

Network intrusion prevention systems (IPSs) can detect and block attacks, and can act as prepatch shields for systems and applications. IPSs include intrusion detection as a subset of capabilities, and have long since eclipsed the detection-only market (see Figure 1).

MAGIC QUADRANT

Figure 1. Magic Quadrant for Network Intrusion Prevention System Appliances



Source: Gartner (April 2009)

Market Overview

The network IPS market subsumed the intrusion detection system (IDS) market several years ago. IPS contains all the detection features of IDS, with two critical areas of improvement:

- Intrusion prevention moves beyond simple attack signature detection to add vulnerability-based signatures and nonsignature detection capabilities.
- Network IPS sensors operate at wire speeds to enable in-line automated blocking and attack handling.

© 2009 Gartner, Inc. and/or its Affiliates. All Rights Reserved.

Essentially, network IPS adds "block attacks and let everything else through" security enforcement to the "deny everything except that which is explicitly allowed" policy enforcement that first-generation firewalls provide.

IPS Benefits

The primary driver for network IPS remains protecting the enterprise from network-based attacks that target system and software vulnerabilities. The primary placement point is at the Internet edge, with secondary placements in branch offices, the data center and, less often, the internal network. IPS is used as a "prepatch shield" to provide positive protection from attacks seeking to exploit known vulnerabilities until patches have been deployed and verified. Most vendors issue vulnerability-facing IPS signatures within 24 hours of patch release, which is invariably faster than an enterprise's ability to patch systems in a measured manner. The reality is that not all vulnerable systems are patched, or new vulnerable systems join the network, and attackers continue to try to exploit vulnerabilities for which patches have long been available. For this reason, IPS signatures never really go away, and the ability of IPS products to maintain data throughput with large signature lists is critical.

The nature of the most damaging attacks on businesses continues to evolve. Financially motivated attacks don't simply go after unpatched PCs and servers; they increasingly are using targeted malware that does not seek to exploit vulnerable software. These targeted attacks (such as bot-net-based attacks) use social engineering techniques to trick users into installing malicious software, and then exploit systems from within the perimeter. Dealing with this changing threat requires more than simple, signature-based detection. IPS vendors have not made major advances in detecting and blocking these advanced attacks, sometimes called "arbitrary malware." The challenge in combating arbitrary malware is in better handling the "gray list," or suspicious traffic that is neither known good (white list) nor known bad (black list).

There have been some increases in "zero day" attacks, which take advantage of computer security holes with as yet no solutions. Approaches to deal with zero-day vulnerabilities are less controversial lately, but their value must be kept in perspective because they are considered in few product selections.

IPS Market Size Growth Continues

The market for separate network IPS and firewall devices grew at 11.7% in 2008, although the rate of growth is flattening to half of that seen 2007. The absence of innovation by firewall vendors in producing next-generation firewalls (NGFWs) that include full IPS capabilities has produced upward pressure on the growth rate, while the increased market penetration of IPS is a larger downward pressure on the growth rate. The macroeconomic condition had some impact on IPS sales, because many enterprises postponed refresh decisions. However, Gartner believes that more of the growth slowdown is due to lack of innovation by IPS vendors in addressing new high-visibility threats. Gartner observed an increase in U.S. government purchases in the last quarter of 2008, tied to spending on the Comprehensive National Cybersecurity Initiative deployment of intrusion detection at federal agency Internet connections.

The past 12 months have seen many vendors announce 10 gigabits per second (Gbps) IPS products. Sales of these products remain niche. These 10+ Gbps models more often act instead as "growth insurance" for customers purchasing lower-throughput models. That is, they want assurance that should their needs change, there are higher-end models they can step into.

Signature Quality Remains a Primary Selection Factor

When enterprises compare products, signature quality remains the most weighted and competitive factor on shortlists. Most vendors employ some form of external vulnerability research

© 2009 Gartner, Inc. and/or its Affiliates. All Rights Reserved.

as an input to signature creation. Gartner sees a widening gap in signature quality among vendors. For the leading IPS vendors, the staff and investments they have assigned to signature research are generally greater than the competition. There are no shortcuts to signature quality, and we believe vulnerability and malware research will continue to shape the market into tiers. Customers seeking best-of-breed protection will shortlist based on high protection quality, which includes signature quality, as well as capabilities for detecting and stopping new threats. Enterprises seeking "good enough" protection as a result of, for example, not having resources or the security profile to be able to enable new signatures quickly, will seek out the second tier of signature-quality products. Investment in purpose-built hardware will continue to buoy up performance under the immutable inspection pressure of new signatures being added to address new vulnerabilities, and older signatures staying in place to guard against older, yet still potent, attacks. Some vendors have already "blinked" in the face of this competitive pressure and are vague about inspection throughput. Enterprises are advised to avoid any vendor that doesn't provide third-party demonstration of appliance throughput rates with inspection enabled.

The creation of custom signatures by end users is slightly increasing, although it is in place in less than 20% of deployments, mostly for custom applications or unusual protocols. Most of these enterprises seek assistance from their IPS vendors in creating or troubleshooting these signatures.

Increasingly, selections will include correlation of alerts, including those from other safeguards, within the IPS itself. The use of source "reputation" inputs as part of the IPS blocking decision process will play an increasing role. As part of this enterprise requirement to reduce the gray list, IPS events can be valuable in building confidence in the risk of other events, or vice versa.

Most vendors include in their base pricing bypass unit modules enabling fail-open for copper ports, with bypass units for optical ports at an additional charge.

Recently, a higher number of IPS selections by Gartner customers have been from enterprises where there is neither an incumbent IPS nor IDS. These enterprises face the hurdle that deploying IPS is a new task for personnel, unlike migrations from IDS where a task is replaced. Infrastructure buying metrics such as port density, cost/port and physical appliance size are not generally seen as IPS selection criteria in enterprises. Rather, ease of deploying in-line and ease of administration are key selection criteria.

New Capabilities

Rate-limiting capabilities are in most IPS products. Some also have quality of service (QoS) that goes beyond respecting the external QoS tags and can prioritize bandwidth based on security criteria or protocol type. IPS operating as a post-connect network access control (NAC) enforcement point remains niche, mostly because most NAC implementations have yet to enable enforcement. Data loss prevention (DLP) in IPS also will continue to be niche — DLP is not a good fit for in-line IPS blocking. Only DLP vendors that also have IPS products are likely to have some correlative or other interaction. Most DLP in IPS today is limited to searching on credit card and Social Security numbers, bringing a high false-positive rate absent the context present in true DLP products.

Market Definition/Description

The network IPS appliance market is composed of in-line devices that perform full-stream assembly and deep inspection of network traffic, providing detection using several methods including signatures, protocol anomaly detection and behavioral or heuristics. This Magic Quadrant is for stand-alone network IPS appliances. Network IPS also is provided in an NGFW, which is the integration of an enterprise-class network firewall and network IPS, and can be an embedded function in network infrastructure equipment. NGFW capability (see "Magic Quadrant

© 2009 Gartner, Inc. and/or its Affiliates. All Rights Reserved.

for Enterprise Network Firewalls") and products not for the enterprise are the subjects of other research.

Inclusion and Exclusion Criteria

In this Magic Quadrant, we include only those products that meet Gartner's definition of network IPS. A product must:

- Operate as an in-line network device that runs at wire speeds
- Perform packet normalization, assembly and inspection
- Apply rules based on several methodologies to packet streams, including (at a minimum) protocol anomaly analysis, signature analysis and behavior analysis
- Drop malicious sessions and not simply reset connections; the session drop must not be merely a block of all subsequent user traffic
- Have achieved network IPS product sales during the past year of more than $4 million in a customer segment visible to Gartner

Gartner examined whether some firewall products that included IPS (for example, Fortinet) merited inclusion. However, we found that most firewalls that included IPS are being deployed for both capabilities.

We excluded products and vendors if:

- They are in other product classes or markets, such as network behavior assessment (NBA). These products are not in-line IPS, but focus instead on networkwide anomaly detection. IPS vendors are beginning to implement feeds from network anomaly detection as a means of having intelligence from across the network that can be used to prioritize blocking.
- The product is not an IPS and is covered in other Gartner research (for example, NAC).
- They are host IPS products — that is, software on servers and workstations rather than an in-line device on the network.
- The vendor has minimal or negligible apparent market share among Gartner clients or is not actively shipping products.
- The vendor is not the original manufacturer of the firewall product, which includes hardware OEMs, resellers that repackage products that would qualify from their original manufacturers and carriers and Internet service providers that offer managed services. We assess the breadth of OEM partners as part of the evaluation of the firewall and do not rate platform providers separately.

Added

Stonesoft has been added because its IPS product now meets the inclusion criteria.

Dropped

With a change of strategy, Reflex Security effectively exited the IPS market (see "Reflex Leaves the Physical IPS Market to Pursue Virtual Security Opportunities").

© 2009 Gartner, Inc. and/or its Affiliates. All Rights Reserved.

Evaluation Criteria

Ability to Execute

Ability to execute criteria are based on (see Table 1):

- Product/Service: This includes customer satisfaction in deployments; we gave high ratings for proven performance in competitive assessments, best-in-class detection and signature quality.
- Overall Viability: This addresses the overall financial health of the business and the prospects for continuing operations.
- Sales Execution/Pricing: This includes cost per Gbps, revenue, average deal size, installed base and use by managed security service providers (MSSPs).
- Market Responsiveness and Track Record: This means delivering on planned new features.
- Market Execution: This includes delivering on features and performance, customer satisfaction with the features and the features winning out over competitors in selections. We gave high ratings in this category to vendors that deliver products with low-latency and multi-Gbps, have solid internal security, behave well under attack, have high availability and are available ports that meet customer demands. Also highly rated are vendors whose products offer speed of vulnerability-based signature production, signature quality and dedicated internal resources to vulnerability discovery.
- Customer Experience: This includes management experience and track record, and depth of staff experience, specifically in the security marketplace. Also important are low-latency, rapid signature updates, overall low false-positive and false-negative rates, and how the product fared in attack events. Postdeployment customer satisfaction, where the IPS is actively managed, is a key criterion.
- Operations: This is the ability of the organization to meet its goals and commitments. Factors include the quality of the organizational structure, including skills, experiences, programs, systems, and other vehicles that enable the organization to operate effectively and efficiently on an ongoing basis.

Table 1. Ability to Execute Evaluation Criteria

Evaluation Criteria	Weighting
Product/Service	High
Overall Viability (Business Unit, Financial, Strategy, Organization)	Standard
Sales Execution/Pricing	Standard
Market Responsiveness and Track Record	Standard
Marketing Execution	Standard
Customer Experience	Standard
Operations	Standard

Source: Gartner (April 2009)

© 2009 Gartner, Inc. and/or its Affiliates. All Rights Reserved.

Completeness of Vision

Completeness of vision criteria are (see Table 2):

- Market Understanding: This includes providing the correct blend of detection and blocking technologies that meet and exceed customer requirements. Also included are an understanding of and a commitment to the security market and, more specifically, the network security market.
- Market Strategy: This criterion includes innovation, forecasting customer requirements, having a vulnerability rather than exploitative product focus, being ahead of competitors on new features and integration with other security solutions. Vendors that rely on third-party sources for signatures or that have weak or shortcut detection technologies scored lower.
- Sales Strategy: This includes pre- and postproduct support, value for pricing, and providing clear explanations and recommendations for detection events.
- Offering (Product) Strategy: This criterion emphasizes product road map, signature quality, NGFW integration and performance. Successfully completing third-party testing, such as the NSS Labs' group IPS tests and common-criteria evaluations, is important. Vendors that reissue signatures, are over-reliant on behavioral detection and are slow to issue quality signatures didn't score well.
- Business Model: This includes the process and success rate for developing new features and innovation, and R&D spending.
- Vertical/Industry Strategy: This criterion includes the ability to direct resources, skills and offerings to meet the specific needs of the market and a commitment to vertical markets (for example, MSSP and the financial sector).
- Innovation: This includes R&D and quality differentiators, such as performance, management interface and clarity of reporting. The road map should include moving IPS into new placement points and better-performing devices, as well as advanced techniques for detecting and blocking targeted attacks.
- Geographic Strategy: This includes the ability and commitment to direct resources to meet the specific needs of geographies outside the "home" or native geography directly or through partners, channels and subsidiaries as appropriate for the geography and market.

Table 2. Completeness of Vision Evaluation Criteria

Evaluation Criteria	Weighting
Market Understanding	Standard
Marketing Strategy	Low
Sales Strategy	Low
Offering (Product) Strategy	High
Business Model	Standard
Vertical/Industry Strategy	Low
Innovation	High

© 2009 Gartner, Inc. and/or its Affiliates. All Rights Reserved.

Evaluation Criteria	Weighting
Geographic Strategy	High

Source: Gartner (April 2009)

Leaders

Leaders demonstrate balanced progress and effort in all execution and vision categories. Their actions raise the competitive bar for all products in the market, and they can change the course of the industry. To remain leaders, vendors must demonstrate a track record of delivering successfully in enterprise IPS deployments and in winning competitive assessments. Leaders produce products that provide high signature quality and low latency, are innovating with or ahead of customer challenges (such as using endpoint intelligence to make more-efficient detections) and have a range of models. Leaders continually win selections and are consistently visible on enterprise shortlists. However, a leading vendor is not a default choice for every buyer, and clients should not assume that they must buy only from vendors in the Leaders quadrant.

Challengers

Challengers have products that address the typical needs of the market, with strong sales, large market share, visibility and clout that add up to higher execution than niche players. Challengers often succeed in established customer bases but do not yet fare well in competitive selections.

Visionaries

Visionaries invest in leading/bleeding-edge features that will be significant in next-generation products and that give buyers early access to improved security and management. Visionaries can affect the course of technological developments in the market, but they lack the execution skills to outmaneuver challengers and leaders.

Niche Players

Niche players offer viable solutions that meet the needs of some buyers. Niche players are less likely to appear on shortlists, but they fare well when given the right opportunities. Although they generally lack the clout to change the course of the market, they should not be regarded as merely following the leaders. Niche players may address subsets of the overall market (for example, the small or midsize business [SMB] segment or a vertical market), and they often do so more efficiently than leaders. Niche players frequently are smaller enterprises, produce only software appliances and/or do not yet have the resources to meet all enterprise requirements.

Vendor Strengths and Cautions

Check Point Software Technologies

Israel-based Check Point is a well-established security company known primarily for its firewall products. It has a well-established partner channel. Check Point had its initial entry into IPS with SmartDefense as part of its firewall products. Check Point acquired NFR Security in 2006, and released the stand-alone IPS product, IPS-1, which consists of six Check Point models and a version on Crossbeam Systems. With its laser-like focus on firewall/virtual private network (VPN) deployment, Check Point has had difficulty finding success in the majority of adjacent markets. Check Point has had considerable activity recently, with the continuing progression in producing its own branded appliances and the recent announcement of the intent to acquire the Nokia security appliance unit.

© 2009 Gartner, Inc. and/or its Affiliates. All Rights Reserved.

Strengths

- IPS-1 can be shortlisted by current Check Point firewall customers looking to deal with a vendor they already have a relationship with, or replace an on-firewall SmartDefense installation with more IPS functionality in a stand-alone appliance.
- Gartner believes that Check Point has moved more resources into its IPS product unit, which should result in a better rate of product advancement than has been seen during the past 24 months.
- The appliance operating system is the same as used in the Check Point SecurePlatform firewall products and is robust. The IPS software blade available on Check Point firewalls is partially based on the IPS-1 code.
- Gartner believes that the Nokia security appliance acquisition provides a good future path for potential purpose-built IPS appliances, although no road map announcements have been made.

Cautions

- Two years after the acquisition, IPS-1 cannot be run under a single Check Point SmartCenter console with other Check Point products. Gartner expects that Check Point will have a unified console by year-end 2009.
- With the release of the new software blade IPS for use on Check Point (and OEM) firewall appliances, the Check Point strategy regarding the futures of SmartDefense, IPS-1 and IPS Blade is unclear.
- IPS-1 is rarely seen on Gartner customer shortlists, and has a small market share. Signature quality is consistently reported as being low.

Cisco Systems

Cisco has stand-alone IPS available in the 4200 series appliances, and the IDS Services Module 2 switch blade when loaded with its IPS Sensor Software. Cisco also has IPS available via add-in hardware modules for the Adaptive Security Appliances (ASA) 5500 series firewalls, and software-based IPS within Internetwork Operating System (IOS)-based routers. Through the acquisition of IronPort Systems in 2007, and the acquisition of Protego Networks in 2004, Cisco has e-mail security, Web security and network behavior analysis/correlation products that can integrate with its IPS products as well as support reputation feeds.

Strengths

- Cisco offers a wide range of IPS platform choices.
- Cisco has wide international support, an extremely strong channel and broad geographic coverage. Enterprises that already have a significant investment in Cisco security products or that use Cisco Security Manager (CSM) are good shortlist candidates for Cisco IPS. The free IPS Manager Express (IME) was recently introduced for managing up to five IPS devices.
- Cisco IPS includes a Risk Rating feature that can be set to adjust alerts based on factors, such as the sensitivity of the asset being protected, providing context for detection and blocking.

© 2009 Gartner, Inc. and/or its Affiliates. All Rights Reserved.

- Cisco is one of the top five vendors for specialized IPS appliance market share in 2008, according to Gartner Dataquest (see "Market Share: Enterprise Network Security Equipment, Worldwide, 2008").

Cautions

- The Cisco IPS Device Manager (IDM) console and the multiproduct console CSM do not score well in shortlist competitions against most leading IPS products, and consistently score low in customer evaluations. Customers are effectively required to use Cisco Security Monitoring, Analysis, and Response System (CS-MARS) to view alerts, and CSM to push policy with (one console is browser- and the other Java-based).
- The Risk Rating feature setting can result in inexperienced IPS administrators unintentionally reducing the protection provided by the IPS.
- Improvements have been made in signature quality during the past year; however, users consistently report to Gartner that signature quality is an issue.

DeepNines Technologies

Founded in 1999, Texas-based DeepNines started out as a pure-play IPS company. DeepNines uses traffic flow tagging to ensure that IPS resources are prioritized. DeepNines narrowed its focus onto the K-12 education vertical, and subsequently expanded the product line to include an all-in-one SMB firewall, network analysis (Edge Security Profiler [ESP]) and URL filtering products.

Strengths

- Moving from the broader market to a focused vertical approach is a good specialization for DeepNines, considering that all other IPS vendors are marketing to the wider market. Any K-12 customer should shortlist the DeepNines Security Edge System (SES) IPS.
- DeepNines users like its bandwidth management and cache of frequently used content.
- Signature quality is reported as good and users like the interface. Third-party signatures, such as Snort, can be imported.
- The SES IPS can run on a customer-sourced server or a DeepNines-provided appliance. Not having a better purpose-built appliance strategy would usually be a negative; however, within the K-12 target market, this flexibility in the absence of high throughput and low-latency requirements is a positive.

Cautions

- Low visibility in the market makes increasing share and channel penetration difficult. The company's comparatively small size puts DeepNines at a disadvantage when competing for large-enterprise business; however, its focus on K-12 usually removes this obstacle.
- The absence of common-criteria certification is a barrier for federal government customers and other high-security vertical markets, such as finance or government. Not having performance validation testing by an external organization (such as NSS Group) lowers visibility and believability in the high-end market.
- The time-for-signature release after the vulnerability announcement is somewhat longer than the industry average, and the inability to change the provided signatures is unpopular with users.

© 2009 Gartner, Inc. and/or its Affiliates. All Rights Reserved.

Enterasys Networks

U.S.-headquartered Enterasys has a long history in the IDS market through its 2000 acquisition of Network Security Wizards, but was a latecomer with IPS products. Enterasys effectively has five models of IPS appliances on a hardened Linux operating system, and the company also has NAC, network IDS, security information and event management (SIEM) and host IDS products. Its Dragon Security Command Console provides consolidated management of IPS appliances. The Dragon IPS can be placed in-line; however, the "distributed IPS" deployment of Enterasys takes an alternative approach of combining IDS-like detection, and using switches and other network infrastructure elements for blocking. Enterasys is emphasizing the combination of NAC, SIEM and IPS. The viability of Enterasys has improved now that it is part of Siemens Enterprise Communications Group (formed October 2008), a Gores Group company. The Gores Group and Siemens have pledged to invest up to €350 million in the joint venture.

Strengths

- The Dragon Distributed IPS is well-suited for internal deployments, and existing Enterasys customers of other network and security products should consider the Dragon IPS.
- Management features include log compression, integration with the Enterasys SIEM and netflow collection.
- Customers rate technical and overall support highly.
- Product and support pricing are frequently listed by customers as reasons for selecting Enterasys.

Cautions

- Many customers that Gartner speaks with are not using the Dragon IDS/IPS product in blocking mode.
- Its unusually large signature library is indicative of low-fidelity or threat (versus vulnerability-facing) signatures. Customer confidence in its signature base for blocking is generally low, however Enterasys has added new features for assisting with selecting in-line signatures.
- Most users Gartner speaks with report their dissatisfaction with the user interface, although they report there have been improvements during the past year. Gartner rarely sees Enterasys on shortlists.
- Enterasys does not have the reputation feeds that competitors with Web security gateway and e-mail security gateway products have.

IBM

Internet Security Systems (ISS) was one of the earliest entrants into the intrusion detection market. Its Proventia IPS is available in eight models, with the GX-series on purpose-built appliances. IBM also has a VMWare-certified software version, and is certified for use on a Crossbeam application blade. The acquisition of ISS by IBM has steadily moved ISS from a security pure-play to being increasingly integrated within IBM. The past year has seen considerable changes in ISS management, including the departure of its chief technology officer and the recent appointment of the former IBM CIO as head of the business unit.

© 2009 Gartner, Inc. and/or its Affiliates. All Rights Reserved.

Strengths

- Its X-Force vulnerability research team has a well-known brand. IBM is benefiting from the good initial design of the Protocol Analysis Module (PAM) deep inspection engine, which has more easily enabled the addition of new protocol inspection capabilities.
- IBM provides the ISS business unit with a wide sales and distribution network, and access to customers that already have a strong relationship with IBM.
- It is one of the top five vendors for specialized IPS appliance market share in 2008, according to Gartner Dataquest (see "Market Share: Enterprise Network Security Equipment, Worldwide, 2008"). Additionally, its IPS products have been in several editions of NSS IPS testing.

Cautions

- Since the acquisition by IBM, ISS presence on IPS shortlists of Gartner customers has been continuously declining. IBM is not seen in the market as having network security as a core competence by network IPS buying centers.
- IBM specifications are not clear on the appliance throughput capacity with deep inspection enabled. This has negated much of the positive impact of the new models and has given ground to competitors in higher-end placements.
- Gartner expects that as ISS continues to be integrated within IBM, there will be a shift from ISS's traditional pure-play focus on network security, to more of a role enabling IBM as a system integrator. This will continue to lower the presence of Proventia on best-of-breed shortlists and, instead, increase share within incumbent IBM customers.
- IBM was listed most often in the survey to vendors as the vendor they claim to most often replace.

Juniper Networks

Juniper has a long history in IPS, based on Netscreen's 2002 acquisition of OneSecure. Its intrusion detection and prevention (IDP) stand-alone IPS line has four models of purpose-built appliances running on a Linux kernel. IPS is also available within the Juniper SRX, and ISG firewalls (see "Magic Quadrant for Enterprise Network Firewalls"). One of the most significant changes in Juniper security is the plan to migrate all products using ScreenOS and Linux onto its JUNOS operating system.

Strengths

- Customers of Juniper Networks IDP products consistently rate postsales support very highly.
- Juniper Networks IDP supports a high number of virtual IPS instances, six third-party vulnerability assessment (VA) engines, have rate limiting, and integrate with Juniper Secure Sockets Layer (SSL) VPN products so that threat information can be linked to VPN sessions and user identity for action.
- The Juniper console and centralized Network and Security Manager (NSM) rates highly in competitive assessments, particularly where other Juniper security products are already in place.

© 2009 Gartner, Inc. and/or its Affiliates. All Rights Reserved.

- It is one of the top five vendors for specialized IPS appliance market share in 2008, according to Gartner Dataquest (see "Market Share: Enterprise Network Security Equipment, Worldwide, 2008").

Cautions

- During the past year, Juniper IPS has had less visibility in the market, which is likely due to Juniper having made advances in its firewall products, and positioning those instead with customers and partners, and focusing on competing primarily with Cisco, rather than with a broader security field.
- Juniper has done well in maintaining a low rate of vulnerabilities for JUNOS; however, it must maintain or improve on this record if it is to move the IDP and other security products onto this single operating system.
- Juniper does not have the reputation feeds that competitors with Web security gateway and e-mail security gateway products have.

McAfee

U.S.-based McAfee is a security brand well-known for its host-based products, and it is one of the few security companies to have successful network security products. It has invested considerably in hardware improvements, which is noteworthy for a company with a software lineage. This year, the former Intrushield product was renamed to the McAfee Network Security Platform (NSP). There are eight models of NSP appliances. McAfee recently acquired Secure Computing, obtaining a line of firewall, Web security and e-mail security products.

Strengths

- Its high throughput, low replacement rate, and good scores in client performance testing are directly a result of the hardware investments in purpose-built appliances. Its IPS console scores well in competitive selections. Gartner has observed an increase in the visibility of the McAfee NSP on shortlists
- NSP can make a good shortlist contender for enterprises using other McAfee security products — such as NAC, vulnerability management, ePolicy Orchestrator (ePO) or host IPS.
- McAfee has a strong presence in federal government markets.
- It is one of the top five vendors for specialized IPS appliance market share in 2008, according to Gartner Dataquest (see "Market Share: Enterprise Network Security Equipment, Worldwide, 2008").

Cautions

- McAfee is known more for host security offerings and often isn't yet considered widely by enterprises and channel partners as a strong network security provider.
- The acquisition of Secure Computing will likely divert some network security engineering and management resources.

© 2009 Gartner, Inc. and/or its Affiliates. All Rights Reserved.

NitroSecurity

U.S.-based NitroSecurity entered the market early with in-line with IPS. It also has products in the SIEM, log management, and database monitoring markets. The NitroGuard IPS is available in six models of Intel-based appliances running a hardened Linux operating system.

Strengths

- FIPS 140-2 level 2 and Common Criteria EAL 3+ certifications are of interest to federal government customers, and demonstrate a significant commitment to third-party evaluations and the security of their products.
- The NitroView console is rated very highly by users, has good correlation, handles large numbers of events, and conducts real-time updating even during pivot views.
- The console capabilities of NitroSecurity products makes it a choice for SMBs or enterprises that want to detect large numbers of events. Users generally report a high level of satisfaction with NitroSecurity support responses.

Cautions

- NitroGuard IPS visibility within the Gartner customer base is low.
- Enabling all signatures by default is not popular with some users, and although the product has a command line interface, it is disabled in Federal Information Processing Standards (FIPS) 140 mode.
- NitroSecurity does not have the reputation feeds that competitors with Web security gateway and e-mail security gateway products have.

Radware

Israel-based Radware's primary business is in network infrastructure products for the data center, such as application delivery controllers. Radware has seven models of IPS across three platforms running a VxWorks operating system. The DefensePro IPS has well-advanced safeguards for rate limiting and Session Initiation Protocol (SIP) protection.

Strengths

- Its use of application-specific integrated circuits (ASICs) and network processors in a purpose-built appliance has shown low latency and high performance in deployments.
- Radware offers low product and maintenance costs, as compared with most competitors.
- Radware has a focus on behavioral assessment, which is unique in the IPS market. When combined with traditional detection mechanisms, this puts Radware in a strong position to address emerging threats.

Cautions

- The IPS console is limited in graphical user interfaces (GUIs) when compared with leading products.
- Radware has low visibility on IPS shortlists, notwithstanding that the product has features competing well with much larger companies. Gartner has seen most sales go to customers that already have Radware products.

© 2009 Gartner, Inc. and/or its Affiliates. All Rights Reserved.

Sourcefire

U.S.-based Sourcefire originated eight years ago as the commercial enterprise created to market and support the open-source Snort IDS product. The Sourcefire IPS is available in 11 appliance models and is also certified to run on a Crossbeam appliance blade and VMWare. The Sourcefire Vulnerability Research Team (VRT) develops all of Sourcefire's IPS rules, notwithstanding the common misconception that only community Snort rules are used. In 2007, Sourcefire acquired the Clam open-source antivirus technology.

Strengths

- Sourcefire has expanded from being primarily add-ons to its IPS products: Real-time Network Awareness (RNA), which provides knowledge of endpoints; Real-time User Awareness (RUA), which provides links to Lightweight Directory Access Protocol (LDAP) directories for policy decisions based user roles; and the Sourcefire Security Network. Sourcefire has extended its appliance range, moving it into a better competitive position against other purpose-built IPS vendors.
- Sourcefire runs the Snort open-source project, which gives it a significant competitive advantage over competitors that use the Snort detection engine or rules.
- Customers like the visibility of what is inside the rules, being able to customize the workflow, and support generally isn't tiered — meaning quick access to advanced technical support. The Sourcefire IPS has deep customization capabilities, making it popular with expert users.
- Sourcefire's education and consulting services receive strong marks and enhance customer loyalty.
- Sourcefire has a strong presence in federal government markets.

Cautions

- The options in the Sourcefire interface can easily overwhelm newer and even technically skilled users. The user interface has improved greatly, but is not highly intuitive when compared with competitive offerings.
- The offering of Sourcefire on an OEM Nokia appliance has been effectively removed by the Check Point acquisition of the Nokia security appliance unit. Gartner does not, however, believe that this was yet a significant revenue source for Sourcefire, so the effect will be minimal.
- Despite having very competitive IPS products, Sourcefire has much less channel strength and visibility than major competitors, and is often left off shortlists as competitive pressures increase.

StillSecure

StillSecure is a U.S.-based pure-play security company. The Strata Guard IPS has six models, and is also available in a VMWare-certified software version, and a freeware version (Strata Guard Lite) capped at 10 Mbps named. StillSecure has found a good niche serving nonenterprise placements where price is highly weighted. StillSecure also produces an NAC (which has integration with its IPS product) and vulnerability management products.

© 2009 Gartner, Inc. and/or its Affiliates. All Rights Reserved.

Strengths

- Strata Guard is a low-cost, software-based product, making it a good choice for SMBs or sub-Gbps placement points. Strata Guard has one of the lowest-priced products on the market in terms of cost per Gbps of throughput.
- Users like StillSecure's viewable rules content, and the integration with the VAM vulnerability management platform product provides a link between vulnerabilities and remediation.
- Users of other StillSecure products are good candidates to shortlist the StrataGuard IPS.

Cautions

- The Strata Guard detection engine is based on Snort, and the majority of signatures are from third-party sources, such as Snort-variants, and are highly exploit-based. This keeps the cost low, but does not fare well in selections where best-of-breed signatures are required.
- StillSecure's visibility in the enterprise is low. The Strata Guard does not have the higher-end certifications, such as Common Criteria, which can be a barrier for federal government buying.

Stonesoft

Finland-based Stonesoft has been in the firewall market for many years, and introduced stand-alone IPS in 2006 after introducing IPS within its firewalls. Although the majority of its customers are in Europe and Africa, Stonesoft has been expanding sales and support within North America. Stonesoft is known for building its High-Availability (HA) feature into products, as opposed to using external high-availability products. Stonesoft has four models of IPS appliances, and a VMWare software version, running under the same management console as its firewall and SSL VPN products. Stonesoft's Magic Quadrant placement reflects its new entry to the market.

Strengths

- The HA feature will be of interest to deployments where a third-party high-availability feature or failure to bypass mode is not desired.
- Clients report high satisfaction with pre- and postsales technical and sales support. Current customers of other Stonesoft products can shortlist the IPS.
- Certifications for the Russian market (FSTEK and GOST).

Cautions

- Customers have reported mixed experience on ease-of-install. More reliance on purpose-built hardware may be required in the future to gain larger enterprise market share and remain competitive, although this has not yet been a significant barrier.
- Being late to the market, the IPS is missing a few features such as links to vulnerability assessment engines; however, Gartner believes that these are on the road map.
- There is limited coverage for geography outside of Europe and North America.

© 2009 Gartner, Inc. and/or its Affiliates. All Rights Reserved.

TippingPoint

TippingPoint is primarily a pure-play IPS vendor (it also has NAC products) and has been shipping IPS appliances since 2002. In early 2005, TippingPoint was acquired by 3Com. By mid-2007, 3Com announced it would spin-off TippingPoint as a separate company. Before that could proceed, 3Com became engaged in a potential acquisition by Huawei and Bain Capital, which did not occur. 3Com has recently announced that TippingPoint will remain within the company, albeit as a separate business unit. However, the long-term 3Com strategy for TippingPoint is unclear as to what this arrangement will mean to both entities. Despite this, TippingPoint has showed discipline in continuing to successfully compete and operate as a de facto stand-alone company. The company has 10 models of IPS, and its Core Controller product, which load-balances multiple IPS devices on the internal network, versus having a single large appliance placed at multiple links.

Strengths

- TippingPoint has the benefit of a large installed base and significant investment in signature development and vulnerability research teams. These investments have enabled TippingPoint to compete effectively on the basis of signature quality. The Zero Day Initiative (ZDI) is the TippingPoint program to attract first notice of undisclosed vulnerabilities from independent security researchers. This was controversial, but has subsequently been well-managed and matured, and now gives an advantage for selections where zero-day signatures are weighted highly.
- TippingPoint has strong channel support and is highly visible on Gartner customer shortlists. TippingPoint's IPS products have a broad model range of purpose-built appliances and are known for low latency and high throughput. TippingPoint was listed by the most IPS vendors as their primary competitor.
- Customers often cite ease of installation as a positive in product evaluations, especially for deployments with many devices. Clients also report that TippingPoint's IPS products require less effort to deploy and manage than competitive offerings.
- It is one of the top five vendors for specialized IPS appliance market share in 2008, according to Gartner Dataquest (see "Market Share: Enterprise Network Security Equipment, Worldwide, 2008").

Cautions

- With the decision to retain the TippingPoint business unit within 3Com, the perceived 3Com relationship with Huawei can be a barrier for some U.S. government sales.
- The advantages of being primarily a pure-play IPS vendor comes with the disadvantage that TippingPoint cannot expand its wallet share with customers much beyond IPS products.
- TippingPoint does not have the reputation feeds that competitors with Web security gateway and e-mail security gateway products have.

Top Layer Security

Top Layer Security is a U.S.-based pure-play IPS company whose lineage in denial-of-service (DoS) prevention gave it a segue into the IPS market. Top Layer has a purpose-built appliance in three models, and has shown a high degree of specialization in hardware and ASIC design. Top Layer has recently begun to use multiple paths of appliance improvement. Top Layer has a

© 2009 Gartner, Inc. and/or its Affiliates. All Rights Reserved.

managed security service (MSS) offering for its own product. Top Layer has benefited from senior management having longevity in their positions (a rare quality in the IPS market).

Strengths

- Top Layer's 5500 IPS has strong capabilities in DoS prevention and multidevice management. Changes to its appliance improvement strategy likely means pushing out end of life (EoL) for incumbent products and improved total cost of ownership (TCO).
- Users like the company's focus on IPS and report strong postsales and technical support. The IPS is in evaluation for Common Criteria EAL-4 (but not yet certified at the time of publication).
- The Network Security Analyzer reporting and forensics tool provides capability that, for many competing solutions, requires an additional SIEM or correlation product purchase.
- Very low-latency hardware performance makes for a good choice for selections where this is a concern such as protecting trading networks, internal deployments or near-real-time systems.

Cautions

- Top Layer has managed its business well to profitability; however, it has not been able to break into the majority of shortlists and keep up with the leaders in terms of market share.
- Top Layer is a single-product company, which limits its ability to attract channel partners and to respond to customer security solution needs.

RECOMMENDED READING

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

"Magic Quadrant for Enterprise Network Firewalls"

"Reflex Leaves the Physical IPS Market to Pursue Virtual Security Opportunities"

"Market Share: Enterprise Network Security Equipment, Worldwide, 2008"

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.

© 2009 Gartner, Inc. and/or its Affiliates. All Rights Reserved.

Evaluation Criteria Definitions

Ability to Execute

Product/Service: Core goods and services offered by the vendor that compete in/serve the defined market. This includes current product/service capabilities, quality, feature sets, skills and so on, whether offered natively or through OEM agreements/partnerships as defined in the market definition and detailed in the subcriteria.

Overall Viability (Business Unit, Financial, Strategy, Organization): Viability includes an assessment of the overall organization's financial health, the financial and practical success of the business unit, and the likelihood of the individual business unit to continue investing in the product, to continue offering the product and to advance the state of the art within the organization's portfolio of products.

Sales Execution/Pricing: The vendor’s capabilities in all pre-sales activities and the structure that supports them. This includes deal management, pricing and negotiation, pre-sales support and the overall effectiveness of the sales channel.

Market Responsiveness and Track Record: Ability to respond, change direction, be flexible and achieve competitive success as opportunities develop, competitors act, customer needs evolve and market dynamics change. This criterion also considers the vendor's history of responsiveness.

Marketing Execution: The clarity, quality, creativity and efficacy of programs designed to deliver the organization's message to influence the market, promote the brand and business, increase awareness of the products, and establish a positive identification with the product/brand and organization in the minds of buyers. This "mind share" can be driven by a combination of publicity, promotional, thought leadership, word-of-mouth and sales activities.

Customer Experience: Relationships, products and services/programs that enable clients to be successful with the products evaluated. Specifically, this includes the ways customers receive technical support or account support. This can also include ancillary tools, customer support programs (and the quality thereof), availability of user groups, service-level agreements and so on.

Operations: The ability of the organization to meet its goals and commitments. Factors include the quality of the organizational structure including skills, experiences, programs, systems and other vehicles that enable the organization to operate effectively and efficiently on an ongoing basis.

Completeness of Vision

Market Understanding: Ability of the vendor to understand buyers' wants and needs and to translate those into products and services. Vendors that show the highest degree of vision listen and understand buyers' wants and needs, and can shape or enhance those with their added vision.

Marketing Strategy: A clear, differentiated set of messages consistently communicated throughout the organization and externalized through the Web site, advertising, customer programs and positioning statements.

Sales Strategy: The strategy for selling product that uses the appropriate network of direct and indirect sales, marketing, service and communication affiliates that extend the scope and depth of market reach, skills, expertise, technologies, services and the customer base.

© 2009 Gartner, Inc. and/or its Affiliates. All Rights Reserved.

Offering (Product) Strategy: The vendor's approach to product development and delivery that emphasizes differentiation, functionality, methodology and feature set as they map to current and future requirements.

Business Model: The soundness and logic of the vendor's underlying business proposition.

Vertical/Industry Strategy: The vendor's strategy to direct resources, skills and offerings to meet the specific needs of individual market segments, including verticals.

Innovation: Direct, related, complementary and synergistic layouts of resources, expertise or capital for investment, consolidation, defensive or pre-emptive purposes.

Geographic Strategy: The vendor's strategy to direct resources, skills and offerings to meet the specific needs of geographies outside the "home" or native geography, either directly or through partners, channels and subsidiaries as appropriate for that geography and market.

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

© 2009 Gartner, Inc. and/or its Affiliates. All Rights Reserved.

Gartner