

Magic Quadrant for Network Intrusion Prevention System Appliances, 1H08

Gartner RAS Core Research Note G00154849, Greg Young, John Pescatore, 4 February 2008, R2688 04022009

The network intrusion prevention system market continues to mature and evolve at a rapid pace as smaller vendors innovate and focus on specific markets. Vendors are starting to incorporate adjacent market features, but there is little progress in addressing emerging threats.

WHAT YOU NEED TO KNOW

This document is an updated version of the document published on 14 February 2008. Network intrusion prevention systems (IPSs) can detect and block attacks, and can act as pre-patch shields for systems and applications. IPS has long since eclipsed by multitudes the intrusion detection system (IDS) market (see Figure 1).

MAGIC QUADRANT

Market Overview

The network IPS market is the successor technology to the IDS market. 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. Essentially, network IPS adds “block attacks and let everything else through” security enforcement to the “deny everything except that what is explicitly allowed” policy enforcement that first-generation firewalls provide.

Although the market for separate network IPS and firewall devices will continue through at least 2008, most next-generation firewalls (NGFWs) will use common processing engines to support both functions in one product, even if there is limited interaction between the two products.

The network IPS market for stand-alone appliances continues to grow, from more than \$700 million in 2006 to a forecast \$1 billion in 2007. In 2007, there were challenges for market leaders, with Sourcefire off to a bumpy start with its initial public offering (IPO), Internet Security Systems working to integrate into IBM, and TippingPoint running into potential barriers to the acquisition of 3Com by Bain and Company and Huawei to foreign interests.

Firewall vendors have been lethargic in improving their in-the-firewall IPS offerings, enabling the stand-alone IPS market to expand faster than it would with competition from firewall vendors. This is mostly because the update cycles for firewalls and IPS appliances have been out of sync, but as enterprises look to replace first-generation IPS units, vendors with integrated capabilities have an opportunity to grow at the expense of stand-alone IPS vendors.

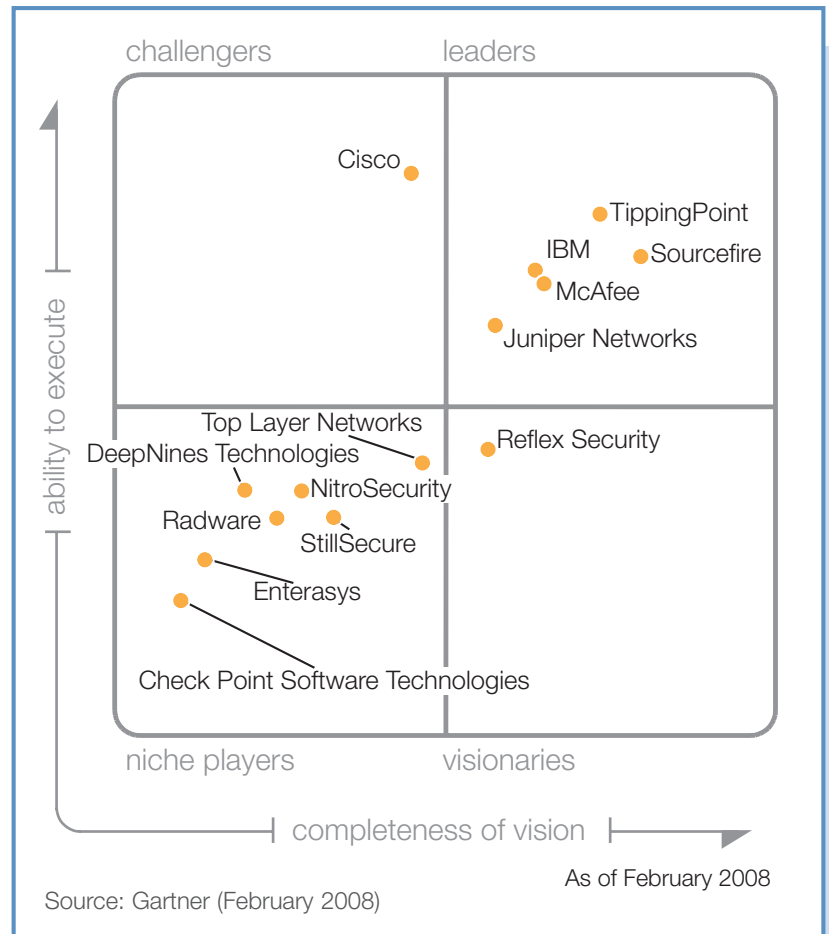
When enterprises compare products, signature quality remains the most weighted and competitive factor on shortlists. Most vendors employ some form of external vulnerability research as an input to signature creation. Some vendors, however, repurpose the open source Snort engine and/or signatures, or other third-party signatures, resulting in problems such as late or inaccurate signatures (owing to poor translations or failure to accommodate the detection signatures in an IPS role), or constraints in innovation, as they potentially must follow the technology direction of Snort. Vendors that invested in their own primary vulnerability research, detection engines and signature creation fared best in our evaluation. Sourcefire owns the copyright on the Snort license, putting the vendors that re-use Snort at a competitive disadvantage, because they can be seen as subordinating themselves to a competitor's road map and a potentially more-restrictive future license under Snort 3.0.

The nature of the most damaging attacks on businesses has changed. Financially motivated attacks don't simply go after unpatched PCs and servers; they increasingly are using targeted malware that requires more than simple, signature-based detection. IPS vendors have not made major advances in detecting and blocking these advanced attacks. Although there has been some increase in "zero day" attacks (which take advantage of computer security holes with no solutions), zero-day signatures, which are signatures for vulnerabilities not yet publicly disclosed, remain controversial.

The risk of reverse-engineering signatures has led vendors that support these signatures to better obfuscate them in 2008. A small percentage (Gartner estimates less than 10%) of enterprises deploy zero-day signatures, and they do not represent a major competitive factor. The creation of custom signatures by end users is on the increase, although it is in place in less than 20% of deployments, mostly for custom applications or unusual protocols. If IPS vendors provide capabilities for easy offline testing of signatures or filters effective in detecting and/or blocking targeted attacks, then early adopter (Type A) enterprises would increase their use of these features.

IPS products are starting to incorporate features from other emerging security products. Early IPS product offerings include post-connect network access control (NAC) enforcement and data

Figure 1. Magic Quadrant for Network Intrusion Prevention System Appliances, 1H08



loss prevention (DLP). DLP is not a good fit for in-line blocking, because most DLP concerns are in e-mail and outgoing Web traffic, and effective DLP requires a tight connection to business-specific policies to reduce false positives. However, IPS products can provide simple features for detecting specific types of information (such as credit card and social security numbers) that may offer stopgap capabilities for organizations that are not yet able to deploy DLP.

The Magic Quadrant is copyrighted February 2008 by Gartner, Inc. and is reused with permission. The Magic Quadrant is a graphical representation of a marketplace at and for a specific time period. It depicts Gartner's analysis of how certain vendors measure against criteria for that marketplace, as defined by Gartner. Gartner does not endorse any vendor, product or service depicted in the Magic Quadrant, and does not advise technology users to select only those vendors placed in the "Leaders" quadrant. The Magic Quadrant is intended solely as a research tool, and is not meant to be a specific guide to action. Gartner disclaims all warranties, express or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

© 2008 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.

Encrypted traffic is increasing gradually, a significant problem for IPS. As the percentage of Secure Sockets Layer (SSL) and otherwise encrypted traffic increases, it presents a growing “blind spot” when SSL decryption is not in the product. A small proportion of IPS placement points are less subject to encrypted-traffic problems (for example, behind the analog-to-digital conversion or Web server); however, for most deployments, these difficulties are a growing concern. IPS vendors must include SSL inspection or similar capabilities to meet this challenge. 802.1AE/AF-based networks will support policy-based link encryption that can decrypt traffic on links where IPS devices are located.

IPS pricing has destabilized significantly during the past 12 months. In 2006, there was a consistent average of \$50,000 per gigabits per second (Gbps) of deep inspection. In 2007, there was considerable price variance. This change is attributed to new IPS features in some products (such as adding vulnerability management integration), making direct product price comparisons less possible, and to some vendors considerably increasing their prices without much change in their products. Thus, enterprises should weight price as a factor in product selections.

Performance, reliability and availability are key criteria for any in-line device. Most vendors include in their base pricing bypass unit modules enabling fail-open for copper ports. Several IPS products are advertised as having speeds of 10 Gbps, although none has any recognized third-party testing to support this claim. Sales of appliances with speeds of 5 Gbps and greater are still rare and often price-prohibitive, with many multi-Gbps placements served with load-balancing several IPSs rather than with one large appliance. As data center and switch IPS placements increase, so will the requirement for these higher-speed devices. Administrative console quality remains a competitive factor. This variance shows mostly in the managing, provisioning and correlating of data from large numbers of devices.

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 and products not for the enterprise are the subject of other research.

Inclusion and Exclusion Criteria

In this Magic Quadrant, we included only products that met Gartner’s definition of network IPS, which is that the 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 that don’t simply reset connections; the session drop must not be 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.
- They are in other NAC product categories. These are not IPS and are covered in other Gartner research.
- They are host IPS products – that is, software on servers and workstations rather than an in-line device on the network.

Added Vendors Added

Enterasys

Check Point Software Technologies

Dropped Vendors Dropped

NFR Security (acquired by Check Point)

Evaluation Criteria Ability to Execute

Ability to execute criteria are based on:

- **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 dollars 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 customers’ 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. Post-deployment 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 (see Table 1).

Completeness of Vision

Completeness of vision criteria include:

- **Market Understanding:** This includes providing the correct blend of detection and blocking technologies that meet and exceed customers' 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 short-cut detection technologies scored lower.
- **Sales Strategy:** This includes pre- and post-product 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 overreliant 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 (see Table 2).

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 have demonstrated 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 customers' 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, 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.

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	

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

Strengths

- Check Point Software Technologies completed the acquisition of NFR Security with the updating and renaming of NFR's stand-alone appliance IPS-1. Most customers find that the majority of support issues that would be expected in such transitions have passed. Thus, Check Point is a shortlist contender for incumbent firewall installations where enterprises seek only one invoice and support relationship.
- The operating system is robust and used in the Check Point SecurePlatform firewall product.
- The Hybrid Detection Engine has a blend of detection techniques, including the use of vulnerability signatures, protocol analysis, network changes and some behavioral aspects.
- Check Point's large installed base of firewalls and breadth of channel provide a potentially huge market execution advantage.

Cautions

- NFR customers report a decline in signature issue frequency and signature quality since the acquisition by Check Point.
- The IDS legacy of the product is apparent in that few customers use the product in in-line IPS mode. Customers often cite the IPS-1 interface as nonintuitive for tuning. One year after the acquisition, there is still no integration of the IPS-1 under the Check Point SmartCenter console.
- IPS-1 is rarely seen on Gartner customers' shortlists, and most customers' impressions are unfavorable. Check Point has an opportunity to gain a share of the IPS market by selling IPS-1 to its firewall customers but will not do so without increased marketing and product support.

Cisco

Strengths

- Cisco offers a wide range of IPS platform selections, with detection engine and signatures shared among stand-alone IPS 4200 series appliances, add-in modules for the Adaptive Security Appliances (ASA) firewall, and a software load and add-in module for Integrated Services Router products. Late in 2007, Cisco released the 4270 IPS appliance, rated for 4 Gbps of throughput.

- The use of Cisco's Security Monitoring, Analysis and Response System (CS-MARS) product for security information and event management (SIEM) is considered part of most Cisco IPS purchases, because it provides extended correlation and visibility of IPS alerts.
- Cisco has accrued a significant IPS market share and provides good international support. 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.
- 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.
- Cisco's TrustSec architecture provides an attractive approach to supporting network encryption without disabling in-line IPS.

Cautions

- The Cisco IPS management console, including CSM, does not score well in shortlist competitions against most leading IPS products.
- The Risk Rating feature setting can result in inexperienced IPS administrators reducing the protection provided by the IPS.
- Users' impressions are that Cisco focuses only on major vulnerabilities. The Cisco IPS signature set has fewer signatures than the industry average.
- Gartner customers often report that Cisco sales propose the ASA product instead of the more appropriate 4200 product for stand-alone IPS selections.

DeepNines Technologies

Strengths

- DeepNines has focused its IPS products vertically on the kindergarten through grade 12 (K-12) education segments. 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.

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
Geographic Strategy	high
Source: Gartner	

- The broad suite of DeepNines products, such as content filtering and NAC, provides choices for vertical education customers to expand their protection without having to deal with multiple vendors.
- Signature quality is reported as good to excellent.

Cautions

- Low visibility in the Gartner customer base makes increasing market and channel penetration difficult. The company's comparatively small size puts DeepNines at a disadvantage when competing for large-enterprise business.
- The absence of common-criteria certification is a showstopper for federal customers and other high-security vertical markets, such as finance.
- Not having performance validation testing by an external organization (such as NSS Group) lowers visibility and believability in the high-end market but is less relevant with the vendor's new focus on the education market.
- The time-for-signature release after the vulnerability announcement is somewhat longer than the industry average.

Enterasys

Strengths

- The networking background of Enterasys is evident in that the Dragon IDS/IPS product line has an overall small rack space footprint, making the products well-suited for deployments such as MSSP/carrier/ISP where detection is valued over blocking.
- Management features include log compression and NetFlow collection.

Cautions

- Gartner has observed that most customers are not using the Dragon IDS/IPS product in blocking mode, and Enterasys markets the IDS capabilities over prevention and blocking.
- An unusually large signature library (about five times the IPS market average) and overreliance on Snort signatures are indicative of low-fidelity or IDS-like signatures. Zero-day signatures are not protected against reverse engineering.
- Although there have been improvements, most enterprises do not have high confidence in the overall financial viability of Enterasys.

IBM

Strengths

- The new, purpose-built appliance from the acquisition of Internet Security Systems, such as the Proventia GX6116 model, marks the transition that Internet Security Systems made from software-based IPS to purpose-built appliances.
- The X-Force vulnerability research team continues to provide strong signature research quality. The Protocol Analysis Module enables the addition of new protocol inspection capabilities, such as shell code heuristics, without a product redesign.

- The integration at the console of the Anomaly Detection System NBA product with the Internet Security Systems IPS provides passive broad network coverage to complement IPS in correlation and network visibility.
- IBM provides the Internet Security Systems business unit with a wide sales and distribution network.

Cautions

- There has been a significant reduction on shortlists of Proventia IPS products subsequent to the acquisition of Internet Security Systems by IBM. IBM is not seen in the market as having network security as a core competence by network IPS buying centers, and the challenge of Internet Security Systems maintaining its previous focus as part of IBM is evident.
- For its newest product, IBM has listed the appliance throughput capacity without 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 customers often report that other IBM business units are unaware of Internet Security Systems IPS products and that the business units are as likely to push Cisco security products.

Juniper Networks

Strengths

- Customers of Juniper Networks intrusion detection and prevention products (Juniper Networks IDP) consistently rate post-sales support very highly. Juniper's sales have been competitive in pricing and creativity, such as the offer of free IPS migration assessments.
- Juniper Networks IDP includes support for up to 250 virtual IPS instances, rate limiting, integration with Juniper SSL virtual private network (VPN) products so that threat information can be linked to VPN sessions and user identity for action.
- The Juniper console and centralized NetScreen-Security Manager (NSM) rate highly in competitive assessments, particularly for NetScreen firewall customers.

Cautions

- Since our 2007 IPS Magic Quadrant, Juniper has not been competitive in introducing updates and new features for its IPS products, and its presence on shortlists has reduced accordingly.
- Users of Juniper Networks IDP report that it can be difficult to determine which signatures are enabled.

McAfee

Strengths

- McAfee has a good variety of seven purpose-built IntruShield appliances ranging in throughput from 100 Mbps to 2 Gbps, with a new multi-Gbps platform expected in first-quarter 2008.
- McAfee IPS is currently the only stand-alone IPS product that provides inspection of SSL-encrypted traffic and supports a high number of virtual IPS instances.
- The McAfee network IPS can make a good shortlist contender for enterprises using other McAfee security products – such as NAC, vulnerability management (for example, Foundstone) and ePolicy Orchestrator – or host IPSs.

Cautions

- McAfee is known more for host security offerings and often isn't considered by enterprises and channel partners as a strong network security provider.
- McAfee has been acquiring small security software providers, which diverts engineering and management resources from the network security side of its business.

NitroSecurity

Strengths

- IPS vendor NitroSecurity has included network flow analysis (sFlow and NetFlow) for some NBA-like, behavior-based detection in the NitroGuard IPS.
- The NitroView console is the nearly singular reason for customers' selections, with console capabilities, including good correlation, handling large numbers of events and maintaining real-time updating, even during pivot views. This has led NitroSecurity closer to SIEM capability and to the introduction of the NitroView SIEM product, which has expanded the customer base and has created specialization in the IPS market.
- The low cost of NitroSecurity products makes them viable choices for SMBs or enterprises that want to detect large numbers of events.

Cautions

- As a smaller company, NitroSecurity has struggled for market share against larger competitors and has had slow growth
- The migration to SIEM capability will further move NitroSecurity from traditional IPS competitions toward single-vendor deals at the lower end of the IPS market. The NitroGuard IPS detection engine is based on Snort_Inline (which is a modified version of Snort), putting NitroGuard at a competitive disadvantage against Snort's de facto manager, Sourcefire.
- Nitro's visibility in the Gartner customer base is low.

Radware

Strengths

- The Radware DefensePro is a purpose-built IPS appliance that uses a custom application-specific integrated circuit (ASIC) and network processors.
- Radware offers low product and maintenance costs, as compared with most competitors.
- Radware's focus on behavioral assessment is unique in the IPS market. When combined with traditional detection mechanisms, this puts Radware in a strong position to address emerging threats.
- Radware recently reorganized to put more sales, marketing and product management focus on its security business.

Cautions

- Radware's background in denial of service protection and its focus on rate-based behavioral detection goes counter to the IPS market and customers' requirements.
- Radware has low visibility on shortlists, and Gartner has seen most sales go to customers that already have Radware products.

- Radware asserts that IPS should operate in Layer 2 transparent mode, but its product does have a Layer 3 mode, although this not advertised widely.

Reflex Security

Strengths

- Reflex Security has made the migration from SMB-only installations to more upper-midsize and enterprise deployments with greater throughput appliances, including a model advertised at a speed of 10 Gbps.
- The virtual security appliance IPS product can be installed in VMware products offering network layer IPS for network traffic entering the virtual machine, with installation in multiple partitions by "drag and drop" rather than by manual installation.
- Clients report high satisfaction with pre-sales and post-sales technical and sales support.
- Reflex Security's architecture and design enable it to compete where the IPS deployment must operate as a "security switch."

Cautions

- As a smaller privately held company, Reflex will face increasing challenges as it tries to compete against larger publicly traded vendors.
- Reliance on Snort signatures puts Reflex at a disadvantage when competing with Sourcefire and other IPS vendors that create their own signatures.
- Reflex Security is a single-product company, which limits its ability to attract channel partners and to respond to customer "security solution" needs.

Sourcefire

Strengths

- Sourcefire has expanded from its IPS product line to new products that extend IPS functionality. Real-time Network Analysis (RNA) provides knowledge of endpoints, Real-Time User Awareness (RUA) provides links to LDAP directories for policy decisions based on the role users have. Sourcefire has extended its appliance range, moving it into a better competitive position against other purpose-built IPS vendors.
- The acquisition of ClamAV extends Sourcefire's commitment and visibility to the open-source community. Sourcefire runs the Snort open-source project, which gives it a significant competitive advantage over competitors that use the Snort detection engine and/or rules.
- Customers like the visibility of what is inside the rules, the interface provides considerable capability for customization and tuning, and support generally isn't tiered, which means quick access to advanced technical support.
- Sourcefire's education and consulting services receive strong marks and enhance customer loyalty.

Cautions

- The options in the Sourcefire interface can overwhelm newer or less-technical users.
- Although the Sourcefire Vulnerability Research Team (VRT) develops most of Sourcefire's IPS rules, users' perceptions are that only community Snort rules lead to exclusion from some shortlists.
- Sourcefire's stock is trading well below its IPO, which generally causes distractions for management and the workforce.

StillSecure Strengths

- Strata Guard is a low-cost, software-based product, making it a good choice for SMBs or sub-Gbps placement points.
- Users like StillSecure's viewable rules content, and the integration with the VAM vulnerability management platform product provides a link between vulnerabilities and remediation.
- StillSecure also offers products for NAC and vulnerability management, as well as a software network platform that includes modules for firewall and router/DHCP. StillSecure offers Strata Guard Free as a free-of-charge IPS software product that has capped throughput at 5 Mbps and can run in VMware.

Cautions

- The Strata Guard detection engine is based on Snort. This, combined with a reliance on Snort signatures, puts Strata Guard at a competitive disadvantage to Snort's de facto manager, Sourcefire. However, StillSecure does not often compete directly with Sourcefire and has better opportunities in the SMB sector.
- Some users report that Strata Guard requires greater ability for customization. NAC has become the primary focus of StillSecure, reducing its focus and competitive presence in IPS.
- StillSecure's visibility in the Gartner client base is low.

TippingPoint Strengths

- TippingPoint, a unit of 3Com, has the benefit of a large installed base and significant investment in signature development and vulnerability research teams. These investments have enabled 3Com to close the gap and compete aggressively with other leaders in signatures.
- The TippingPoint unit of 3Com has significant experience in the IPS market and is highly visible on Gartner customers' shortlists. TippingPoint's IPS products have a broad model range of purpose-built appliances, including high-throughput options, and are known for low latency.
- 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 required to deploy and manage than competitive offerings.

Cautions

- The TippingPoint IPS business unit will change under the proposed planned acquisition of 3Com by Bain and Company and Huawei, with TippingPoint spinning out in an IPO or becoming part of 3Com under Bain/Huawei ownership.
- 3Com has emphasized zero-day signatures, and although this is valuable to a small percentage of enterprises, it alienates others that don't view this factor as valuable or that see it as overshadowing the product's other features.

Top Layer Networks Strengths

- Top Layer Networks is a pure-play IPS vendor with a purpose-built appliance. The 5500 IPS, recently updated to the 5500E version, has good capabilities in denial-of-service prevention and multidevice management.
- Users like the company's focus on IPS and report strong post-sales and technical support.
- The Network Security Analyzer reporting and forensics tool provides capability that, for many competing solutions, requires an additional SIEM or correlation product purchase.

Cautions

- Performance and low latency have been strong feature issues in Top Layer's deployments; however, the ASIC and platform limit the ability of Top Layer to make significant changes to the base product in the long term.
- Top Layer has lower visibility than other, purpose-built appliance IPS makers on Gartner customers' shortlists.
- Top Layer is a single-product company, which limits its ability to attract channel partners and to respond to customer security solution needs.

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.

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.

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.