LICENSED FOR DISTRIBUTION

**Magic Quadrant for Intrusion Detection and Prevention Systems**

**Published:** 16 January 2017 **ID:** G00295470

Analyst(s):

Craig Lawson, Adam Hils, Claudio Neiva

**Summary**

Security and risk management leaders should know that while IDPSs are being absorbed by firewall placements at the perimeter, they give the best protection. They're also responding to pressure from uptake of other threat defense solutions, and providing credible internal and cloud placement options.

**Strategic Planning Assumption**

In 2020, 30% of new stand-alone intrusion detection and prevention system (IDPS) placements will be cloud-based (public or private) or deployed for internal use cases.

**Market Definition/Description**

The network IDPS market is composed of stand-alone physical and virtual appliances that inspect defined network traffic either on-premises or in the cloud. They are often located in the network to inspect traffic that has passed through perimeter security devices, such as firewalls, secure web gateways and secure email gateways. While detection only (IDS) is still often used, a large number of appliances are deployed in-line and perform full-stream reassembly of network traffic. They provide detection via several methods — for example, signatures, protocol anomaly detection, behavioral monitoring and heuristics, advanced threat defense (ATD) integration, and threat intelligence (TI) to uncover unwanted and/or malicious traffic and report or take action on it.

All of the aforementioned methods augment IDPS capabilities with more context to reduce both the number of alerts as well as false-positives. False-positives are still a concern for clients when IDPSs are in blocking mode. When deployed in-line, IDPSs can also use various techniques to detect and block attacks that are identified with high confidence; this is one of the primary benefits of this technology. The capabilities of leading IDPS products have adapted to changing threats, and next-generation IDPSs have evolved incrementally in response to advanced targeted threats that can evade first-generation IDPSs (see "Defining Next-Generation Network Intrusion Prevention" ).

This Magic Quadrant focuses on the market for stand-alone IDPS appliances; however, IDPS capabilities are also delivered as functionality in other network security products. Network IDPSs are provided within a next-generation firewall (NGFW), which is the evolution of enterprise-class network firewalls, and include application awareness and policy control, as well as the integration of network IDPSs (see "Magic Quadrant for Enterprise Network Firewalls" ). IDPS capability is available in unified threat management (UTM) "all in one" products that are used by small or midmarket businesses (see "Magic Quadrant for Unified Threat Management" ). We have also begun to see basic IDPS functionality provided by a small number of network ATD vendors. Gartner observes that the maturity of IDPS modules embedded with ATD solutions has yet to be proven.

So, while the stand-alone IDPS market is forecast to start shrinking from 2017 (see [Forecast: Information Security, Worldwide, 2014-2020, 3Q16 Update](https://www.gartner.com/document/3512217) ), the technology itself is more widely deployed than ever before on various platforms and in multiple form factors. The technology is increasingly ubiquitous in technology like NGFW and UTM. IDPS vendors need to move to delivering internal and virtualized/cloud deployments if the market is to continue to grow. That said, it needs to be stated that in general, the IDPSs that are available in firewalls and UTM solutions are not up to the same standard as those from leading dedicated providers.

In addition, some vendors offer functionality in the public cloud in order to provide controls closer to the workloads that reside there. Gartner is tracking the growth of these deployments carefully, and will monitor their efficacy.

Stand-alone IDPSs are most often deployed for the following use cases:

* When the staff managing the IDPS does not manage the firewalls
* When best-of-breed protection is required or preferred
* As an IDPS on the internal network
* When high IDPS throughput and low-latency performance is required
* To provide network security on parts of the internal network where it's easier to deploy IDPS than technology like firewalls
* To provide additional visibility and detection capabilities in the public or private cloud

**Magic Quadrant**

**Figure 1.** Magic Quadrant for Intrusion Detection and Prevention Systems



Source: Gartner (January 2017)

**Vendor Strengths and Cautions**

**AhnLab**

AhnLab, founded in 1995 and headquartered in South Korea, is a network and endpoint security vendor. TrusGuard IPX was released on 2012. The AhnLab product portfolio includes firewalls, ATD, distributed denial of service (DDoS) attack mitigation and endpoint security solutions. It is shipping three IPX appliances between 5 Gbps to 40 Gbps in range. TrusGuard IPX currently does not come in the form of a virtual appliance. Secure Sockets Layer (SSL) decryption is available for traffic visibility, and TI can be used for command and control (C&C) threat detection. Malicious URL detection/blocking is also supported.

AhnLab has the majority of its presence in South Korea today, followed by a number of other East Asian countries (such as Indonesia, Thailand and Vietnam), mostly within midmarket organizations. It is trying to expand into Latin America as well.

AhnLab is assessed as a Niche Player because it sells its IDPS primarily in one region and lacks visibility with Gartner clients in non-Asia regions.

**Strengths**

* AhnLab is an established endpoint and network security player in South Korea, with significant local sales and support presence. Hence, it is a good shortlist candidate for clients based in South Korea looking for a local vendor with regional support and services.
* AhnLab is one of a few East Asian vendors with a local certification (Korean Common Criteria), which is significant in South Korea.
* AhnLab's network security portfolio allows the use of different components to cover different network security use cases (firewall, endpoint security, ATD and DDoS) under the same contract support.

**Cautions**

* AhnLab is currently regionally constrained primarily to the South Korean security market.
* The vendor does not support integration with vulnerability management tools to automate the deployment of protection on known vulnerabilities.
* AhnLab's user-based policies are either configured by mapping a username to a static IP address or via a captive portal, making it less useful for some environments and other non-web-based network protocols.
* AhnLab also does not have a virtual version of its technology at this time, limiting its ability to be deployed in virtualized or public cloud environments.
* The vendor does not have current independent testing results with organizations like NSS Labs.

**Alert Logic**

Houston, Texas-based Alert Logic is a privately held security-as-a-service provider. Services they offer include managed IDS, web application firewall (WAF), log management and vulnerability management. Alert Logic's IDS, which is built on a Snort foundation with additional anomaly-based signatures, heuristics and machine learning intelligence, is offered in two packages: Threat Manager is an IDS-only offering and includes vulnerability management capabilities; and Cloud Defender includes WAF and log management, along with detection based off logs. Alert Logic's IDS is offered as a physical on-premises appliance, with new deployments more often in the form of virtual machines deployed in hosting or cloud environments. The vendor has also invested in some interesting methods to apply machine learning to the IDS event stream to help reduce the amount of "net events" that need to be reviewed by human analysts.

Since Alert Logic's IDS is deployed out-of-band in detection mode and as a managed service, it does not offer a wide range of high-performance appliances. Alert Logic adds and subtracts sensors where it makes sense for the customer's changing network in order to meet detection needs.

Alert Logic is designated as a Niche Player because of its relevance to hosting and public cloud environments, and because its low-priced, high-touch IDS services appeal to a broad swath of midmarket customers.

**Strengths**

* Alert Logic offers a wide range of straightforward compliance templates. Its IDS is a good shortlist candidate for resource-constrained security shops that need IDS to fulfill compliance use cases. Gartner clients with compliance use cases sometimes consider Alert Logic's IDS solution — Threat Manager — to meet regulatory needs.
* Surveyed customers value Alert Logic's ability to deploy across physical, IaaS, container-based and VMware environments. In this use case, customers often use Cloud Defender.
* Alert Logic's fully managed ability to spin up and spin down virtual instances makes it a good candidate for agile DevOps environments.
* Alert Logic's aggressive pricing and 24/7 monitoring appeals to midmarket environments and organizations with a small security staff.

**Cautions**

* Organizations that desire the ability to quickly build custom signatures or enable existing signature sets find that it takes extra time having to curate requests through Alert Logic's security operations center team.
* Alert Logic's out-of-band model means that there is no application DoS mitigation or general blocking offered with its solutions, which is often an IPS requirement. The Alert Logic WAF is used for DDoS and in-line blocking use cases.
* Alert Logic doesn't target the federal market and isn't pursuing FIPS, and independent testing from NSS Labs does not have a specific IDS-only test.

**Cisco**

Cisco, which is headquartered in San Jose, California, has a broad security product portfolio and has had IDPS offerings for many years. In 2013, Cisco acquired Sourcefire and incorporated the acquired Firepower technology as its sole IDPS engine, replacing its legacy IDPS capabilities. The Firepower line currently shares a management console with the Cisco firewall offerings.

Cisco has 22 models of IDPS available in the 4000, 7000, 8000 and 9000 Series Appliances, and a virtual appliance (NGIDPSv) for VMware. The top 9300 configuration runs up to 90 Gbps of inspected throughput. The same IDPS is available in the Cisco Adaptive Security Appliance (ASA), labeled as "with Firepower Services." Additionally, the software-based IDPS is available as an option within the Cisco Internetwork Operating System (IOS)-based routers and Integrated Services Routers (ISR) IDPSs. The Meraki MX platform also runs the Snort engine plus Advanced Malware Protection (AMP) for Networks.

During the evaluation period, Cisco introduced the first three models of its 4100 line, and the 9300, which comes in three configurations ranging in throughput from 20 Gbps to 90 Gbps. New capabilities introduced include URL-based and DNS-based security intelligence, DNS inspection and sink holing, and AMP Threat Grid integration.

Cisco is evaluated as a Leader because of its ability to lead the market with new features based on the former Sourcefire products, and because it has the largest market share and highest visibility in Gartner client shortlists for IDPSs.

**Strengths**

* Gartner's advanced security clients enjoy Firepower's usefulness as an IDS analysis tool, in addition to its utility as an in-line, blocking IDPS. Those that deploy the product in IDS mode particularly like Cisco's Snort open rules capabilities.
* Cisco has wide international support, an extremely strong channel and the broadest geographic coverage. Certain Smart Net-supported customers can get two-hour RMA when a unit fails. In addition, thousands of partner engineers are certified on Cisco Firepower.
* The AMP products that work closely with and provide intelligence to the IDPS provide coordinated malware detection at the network, sandbox and endpoint layers. This coordination differentiates it from many competing solutions.
* Cisco's Talos, its security research organization, has a large team researching vulnerabilities, and developing security content for all Cisco security products, including writing signatures. During the evaluation period, Talos publicly disclosed more than 150 zero-day vulnerabilities.

**Cautions**

* Some Type A clients have expressed concern that IDPS innovation will slow as Cisco works on integration with acquired capabilities. Customers with these concerns should insist upon roadmap clarity that makes planned IDPS enhancements explicit.
* Some clients have referred to performance impacts when enabling AMP for Networks services on existing sensors. This is due to there being a significant amount of signature-based content in the core IDPS product. Clients are advised to refer to sizing guidelines for their initial acquisitions to ensure their production performance needs are met.
* Cisco lagged behind the competition in introducing support for Amazon Web Services (AWS), and has yet to offer support for Microsoft Azure.
* Cisco publicly disclosed a number of vulnerabilities within its IDPS products during the evaluation period. Because of its market presence and large deployment footprint, clients need to take this into account as part of their vulnerability management program.

**Hillstone Networks**

Headquartered in Beijing, Hillstone Networks is a network security provider that offers NGFWs along with IDPSs. Hillstone has been shipping IDPS devices since 4Q13. At present, its IDPS customer base is predominantly located in China.

The vendor offers a total of 12 IDPS models, of which five are available to the global market. These appliances range in performance from 350 Mbps to 4 Gbps. Hillstone does not offer a virtual IDPS model. IDPS signatures are developed internally and obtained from Trend Micro.

During the evaluation period, Hillstone introduced several new models. New enhancements introduced in that period include improved AV efficacy, http flood request protection and better IDPS reporting.

Hillstone is designated a Niche Player because of its lack of innovation features and its lack of presence outside of the Asia/Pacific region.

**Strengths**

* Hillstone's price/performance ratio makes it a good candidate for midmarket organizations considering dedicated IDPS. Hillstone's IDPS also has low-latency metrics.
* Hillstone's surveyed customers report that ease of deployment and management are among the top reasons the vendor gets selected.
* Hillstone continues to be regarded as a credible pure-play network security vendor that is anchored in Asia.

**Cautions**

* Hillstone's top performance level — 4 Gbps with IMIX traffic — makes it unsuitable for some enterprise placements.
* The Hillstone IDPS is missing some important features such as TI integration and advanced threat detection.
* All system patches and upgrades require IDPS restart, which can present problems in security and network operations.
* Hillstone's IDPS product lacks third-party certifications and testing.

**Huawei**

Headquartered in Shenzhen, China, Huawei, with a core strength in networking, offers a range of network security controls, including IDPS, firewall and DDoS mitigation appliances. Huawei introduced its IDPS product line, called Network Intelligent Protection (NIP) System, in 2004. NIP includes eight physical appliances, ranging from 800 Mbps to 15 Gbps. The vendor's IDPS currently does not come in the form of a virtual appliance, although this is expected to change. SSL decryption for visibility and TI (reputation)-based blocking is supported.

Huawei is evaluated as a Niche Player because it operates mainly in one country or within the existing Huawei client base, addressing a specific segment of the IDPS market.

**Strengths**

* Customers like the NIP Manager interface, especially the ease of installation and policy templates.
* Huawei has a very strong presence among midsize Chinese organizations looking for cost-effective IDPS solutions.
* Users report good pricing as well as performance in the production environments, which is in line with the vendor's marketing material.

**Cautions**

* Despite a large channel in EMEA, Huawei does not often appear in shortlists outside of China. Potential customers from other regions should first check local channel experience with the NIP product line.
* Huawei's IDPS offers a lower number of IDPS signatures and categories compared with leading vendors. While generic approaches are a good reason for the low number of signatures, this could translate into less flexibility and a coverage gap for clients.
* The vendor has undertaken significant steps in the past to address concerns about relying on technology developed in China; however, for many prospective customers in the U.S., those concerns remain.
* Huawei does not have embedded or cloud-based advanced threat detection, and sandbox options are not available.

**IBM**

IBM, headquartered in Armonk, New York, has the IBM Security Network Protection (XGS; four appliances) and Network Intrusion Prevention System (GX; nine appliances) products positioned within a recently unified security product and services division. IBM offers the XGS 3100, 4100, 5100 and 7100, which incorporate next-generation IDPS capabilities at up to 25 Gbps of inspected throughput. The virtual network security platform is available as a VMware virtual appliance based on the XGS product line. IBM focuses on IDPSs as being part of the QRadar portfolio, but management consoles (Security SiteProtector System) are still separate from the QRadar management console.

In other areas of its dedicated security business unit portfolio, IBM continues to grow both with new acquisitions (like Resilient Systems) and its services (such as incident response services).

IBM is rated as a Challenger because it has solid next-generation IDPS features, and executes well in making integrated security sales in the IBM customer base, rather than replacing other vendors.

**Strengths**

* IBM's Protocol Analysis Module (PAM) IDPS engine is still leading the market in its ability to provide low false positives and protection for entire classes of vulnerabilities, with the smallest number of signatures in the market.
* Customers often buy IBM IDPS in conjunction with QRadar security information and event management (SIEM) to achieve deeper levels of security intelligence integration.
* IBM has a wide sales and distribution network, and customers with a strong IBM relationship are generally pleased with the IDPS support they receive.
* IBM offers a flexible license model that allows customers to upgrade inspected throughput on an XGS via software only, without the need to upgrade hardware.

**Cautions**

* IBM IDPSs do not regularly appear in shortlists of Gartner customers. Many Gartner clients do not perceive IBM as a strategic supplier of network security products.
* IBM's highest-throughput IDPS appliance has 25 Gbps throughput (without third-party load balancers), which makes it one of the lowest-throughput high-end boxes. This disqualifies IBM for some specific high-throughput use cases.
* IBM's network security portfolio is incomplete. The vendor lacks native ATD and support for open TI standards. The current ATD integration relies on an OEM. As a result, Gartner clients often do not view IBM as a strategic network security vendor.
* The centralized management solution (Security SiteProtector System) has not had an update for some time. In addition, there have not been any significant integrations with other IBM technologies — for example, using IBM Security QRadar Vulnerability Manager and BigFix to help inform IDPS policy creation, and Resilient Systems for integration with incident response.

**Intel Security (McAfee)**

Intel, based in Santa Clara, California, announced on 7 September 2016 that it will spin out Intel Security, creating a stand-alone company. The new McAfee company will have a significant product portfolio across network, server, content, SIEM, data loss prevention (DLP) and endpoint security. Under the proposed arrangement, Intel will retain a 49% equity interest in McAfee. Additionally, in 1Q16, Intel Security sold its NGFW product lines to Forcepoint, eliminating a second IDPS code base within its overall portfolio.

The Intel Security Network Security Platform (NSP) is the stand-alone IDPS model line, with 18 physical appliance models that range from 100 Mbps to 40 Gbps of throughput, and three virtual models (including one specially tailored for VMware NSX deployments). Gartner sees clients deploying NSP mostly in IDPS (blocking mode), but observes a number of IDS (detection mode) use cases as well.

During the evaluation period, Intel Security introduced four entry-level NS-Series sensors: NS-5200, NS-5100, NS-3200 and NS-3100. Features introduced in that time frame include improved on-box gateway anti-malware inspection, significant manager UI improvements and improved custom signature creation capabilities.

Intel Security is evaluated as a Leader because of its continued presence on Gartner client shortlists and its feature leadership in areas such as TI context and heuristic techniques that lessen reliance on signatures.

**Strengths**

* Clients give high marks for NSP's ease of management, ease of deployment and performance under load, and the IDPS console continues to score well in competitive selections and independent tests.
* Customers cite McAfee's thorough integration with other McAfee products, including Advanced Threat Defense and Threat Intelligence Exchange, as strong positives.
* In organizations concerned with false-positive rates coming from heavy use of signatures, McAfee's multiple signatureless inspection techniques give it an advantage over more signature-based IDPS technologies.
* McAfee is the sole certified VMware NSX-certified IDPS partner, making it a good candidate for securing NSX software-defined networking (SDN) data center projects.

**Cautions**

* As Intel spins out McAfee, customers and prospects must evaluate roadmap and progress against it, as well as account team continuity and support quality. Customers and prospects should especially examine the ongoing efficacy of joint development projects between Intel Security and the spun-out McAfee. Gartner believes there will be a short- to medium-term disruption because of this move, and has also noted in the previous two years a number of staff resignations from both the field and product development areas.
* In January 2016, Intel Security finalized the divestiture of multiple network firewall products to Forcepoint. This has made the IDPS range vulnerable to combined firewall plus IDPS replacements from vendors such as Cisco, and dilutes Intel Security's overall network security brand.
* Intel Security has lagged behind its competition in addressing AWS and Microsoft Azure public cloud IaaS use cases.

**NSFOCUS**

NSFOCUS is headquartered in Beijing and Santa Clara, California. It is a large regional security vendor for Asia and is expanding to other geographies. NSFOCUS offers DDoS (Anti-DDoS System [ADS]), secure web gateway (Web Vulnerability Scanning System [WVSS]), and WAF and vulnerability management (Remote Security Assessment System [RSAS]). The vendor also offers managed security service (MSS) on a number of its products. The NSFOCUS IDPS has a large range of appliances, with 10 models ranging from 300 Mbps to 20 Gbps of throughput, and four virtual appliances. Its IDPS, Next Generation Intrusion Prevention System (NGIPS), includes sandboxing capabilities called TAC, as well as application control and anti-malware, and can also utilize reputation-based controls.

NSFOCUS is assessed as a Niche Player because it sells NGIPS almost exclusively in one region.

**Strengths**

* NSFOCUS has a faithful base of large Chinese organizations and often appears in final shortlists in the Asia/Pacific region.
* NSFOCUS is delivering on next-generation IDPS capabilities around application control, anti-malware and TI, and is generating good revenue and market traction in the main geographic area in which it competes.
* NSFOCUS customers like the vendor's support timeliness and ability to provide extensive answers.

**Cautions**

* NSFOCUS is rarely visible in the Asia/Pacific region outside of China, and has yet to build a large channel for its IDPS in the U.S. and other regions.
* Gartner customers report poor visibility in application and user contexts.

**Trend Micro (TippingPoint)**

Headquartered in Japan, Trend Micro is a large, global, IT security vendor that has now completed its acquisition of TippingPoint from Hewlett Packard Enterprise (HPE). TippingPoint is well-placed within Trend Micro in the same division as the Deep Discovery products. The top IDPS model now supports stacking with no other external hardware and can run up to 100 Gbps of inspected throughput. The TippingPoint IDPS is also delivered using an Intel-based platform, which is a move away from the traditional network processing unit (NPU) architecture used for a decade. IDPS content updates are provided through TippingPoint's Digital Vaccine Labs (DVLabs). The DVLabs team also works with the Zero Day Initiative (ZDI) program, which continues to be an excellent source of vulnerability information for TippingPoint products, while also supporting independent security researchers. There are also synergies between TippingPoint's and Trend Micro's research teams on malware, which is enhancing the IDPS's ability to specifically address malware threats. Additionally, the Trend Micro advanced threat (sandbox) technology for its IDPS, called Advanced Threat Protection, now has integrations to its IDPS to be able to receive telemetry in real time that can be used for prevention and detection use cases.

We have seen the TippingPoint move to Trend Micro to be an overall net positive for TippingPoint customers at this point in time. The IDPS platforms have gained native integrated advanced threat capabilities, a significantly larger channel with more expertise in selling security, and access to Trend Micro's significant research resources.

Trend Micro (TippingPoint) is assessed as a Leader due to its large installed base, good support, significantly improved channel and ability to meet a wide range of use cases.

**Strengths**

* Customers describe easy, confident deployment of this IDPS in blocking mode, including the ability to have malware-centric content.
* Customer support earns high marks with customers. Support fees are based on a percentage of the sales price, not list price, providing potential support savings for customers.
* The ability to integrate third-party vulnerability scanning data to speed up IDPS policy workflow, and the ThreatLinQ user portal for policy assistance, are well-regarded.
* The SMS management console now has the ability to take and explore flow data from managed IDPSs, giving users better visibility into the network. This can also be used to detect threats, particularly in relation to lateral movement.
* The divestiture of TippingPoint has been a net positive, with improvements noted in its roadmap and field organization.

**Cautions**

* Trend Micro has a different IDPS engine on the network and host. End users should be aware that there is a difference in the breadth and depth of IDPS features with its network- and host-based IDPS engines.
* TippingPoint does not have a full user and application-based capability to define and enforce policies using these two attributes.
* The Trend Micro acquisition will be a big shift for TippingPoint, especially in field sales and presales staff, and may cause issues with retention.
* Today, the IDPS does not offload objects to the ATD for inspection natively like other leading products, and has to be separately deployed and managed via different interfaces.
* Trend Micro will have to invest considerable effort in enabling its existing direct sales and channel partners to bring this new product set to market.

**Venustech**

Venustech is a security vendor headquartered in Beijing China. It was founded in 1996, and has been shipping IDS since 2003 and dedicated IPS since 2007. In addition to its IDPS, Venustech has a range of security product offerings covering SIEM, firewall, UTM, WAF, database compliance and audit (DCAP), vulnerability assessment, application delivery controller, and an endpoint security solution. Venustech has a virtual IPS edition available that supports VMware and OpenStack. It also has support for the Alibaba, Tencent and Huawei clouds as deployment options.

Venustech is rated as a Niche Player for this research due to its lack of visibility among Gartner clients and its regionally constrained client base and market recognition.

**Strengths**

* The policy configuration interface is laid out in an easy-to-understand and navigate manner.
* Venustech also has an anti-malware capability in the appliance which enables the blocking of malicious-content-based attacks, as well as other more advanced methods to detect threats, like SQL injection
* Support for the Chinese cloud providers gives Venustech a strong advantage for cloud deployments in that geography.

**Cautions**

* Venustech is seen as a follower in the IDPS market and does not have features causing disruption to its competitors in the market.
* Venustech is almost exclusively active in the China region today, constraining its growth.
* Venustech's IDS and IPS products today are separate product lines, with separate management interfaces and subtly different security content and features between the two. Until the two lines merge, clients should understand which appliance is usable for which IDS or IPS use case.

**Wins**

Wins is headquartered in Seongnam, Gyeonggi-do Province, South Korea, and it was established in 1996. Its IDPS was released on or before 2005. Wins has previously achieved Common Criteria certifications for its IDPS technology. It is shipping six appliances between 400 Mbps to 40 Gbps in range. The Sniper One series also supports SSL decryption. Gartner was unable to contact Wins for this research. Wins did not respond to requests for supplemental information and/or to review the draft contents of this document. The Gartner analysis is therefore based on other credible sources, including public information and limited discussions with users of this product.

Wins is assessed as a Niche Player because it sells its IDPS in one region and lacks visibility with Gartner clients.

**Strengths**

* Wins is successful in South Korea and Japan, where its Sniper IDPS is marketed.
* It offers one of the few IDPSs that has support for some carrier mobile protocols around inspecting 3G/LTE encapsulated traffic.
* The vendor supports the Snort standard, which allows clients to create custom signature content and to reuse publicly available security content.

**Cautions**

* Today, Wins is regionally constrained to specific areas in Asia.
* The vendor does not appear to discover original vulnerabilities, making it more of a "fast follower" in terms of security content creation.
* The chassis in its lineup does not support a high physical port density.

**Vendors Added and Dropped**

We review and adjust our inclusion criteria for Magic Quadrants as markets change. As a result of these adjustments, the mix of vendors in any Magic Quadrant may change over time. A vendor's appearance in a Magic Quadrant one year and not the next does not necessarily indicate that we have changed our opinion of that vendor. It may be a reflection of a change in the market and, therefore, changed evaluation criteria, or of a change of focus by that vendor.

**Added**

* AhnLab
* Alert Logic
* Hillstone Networks
* Venustech

**Dropped**

There were no vendors dropped from this iteration of the Magic Quadrant.

**Inclusion and Exclusion Criteria**

Only products that meet the majority of the following criteria will be included:

* Meet Gartner's definition of a network IDPS and IDS:
  + Operate as a network appliance that supports both in-line network intrusion prevention and/or network intrusion detection use cases.
  + Operate as a virtual appliance in private or public cloud environments.
  + Perform packet normalization, assembly and inspection to support these detection and prevention use cases.
  + Apply policy based on several detection methodologies to network traffic, including methods like protocol anomaly analysis, signature analysis, behavior analysis and TI.
  + Be able to identify and respond to malicious and/or unwanted sessions with multiple methods, such as allow/multiple alert types/drop packet/end/reset sessions, etc.
  + Achieve network IDPS product sales in the calendar year 2015 of over $4 million globally within a customer segment that is visible to Gartner.
  + Sell the product as primarily meeting stand-alone network intrusion prevention and detection use cases.

Products and vendors were excluded if:

* While there are many products and implementations using the popular open-source IDPS projects (like Snort and Suricata), this Magic Quadrant does not evaluate this open-source technology. If a vendor is using this, it must clearly demonstrate that it is providing over and above the functionality delivered by these projects by improved packaging (hardware or software), and especially additional research and security content that would take this beyond "just running Snort/Suricata."
* They are in other product classes or markets (such as network behavior analytics [NBA] products or network access control [NAC] products), are not IDPSs, and are covered in other Magic Quadrant research.
* They are host IDPSs — software on servers and workstations, rather than a device on the network.
* They are sold only as components of a NGFW or UTM platform.

**Vendors to Watch**

There are three vendors that provide capabilities that are relevant to the IPS market, but have not fully met IPS market inclusion criteria. Organizations that need to implement IPS functions for the supported use cases should also evaluate these vendors.

**Bricata**

Bricata, which is headquartered in Columbia, Maryland, is a startup that leverages open-source IPS and other detection frameworks, adding software and hardware expertise to maximize performance and scalability. Its ProAccel IDPS solution is based on open source that combines the Bro and Suricata engines with commercial technologies, delivering signature-based and anomaly detection with network and behavior analysis. The combination of Suricata and Bro achieves better detection via Suricata's packet inspection, while Bro's anomaly-based engine, provides context around alerts and provides correlation across multiple sessions identifying interrelated events. The Central Management Console (CMC) also supports a "manager of managers" deployment architecture. Bricata's appliances also ship with a large (in comparison to other solutions) amount of on-chassis storage, allowing for the collection of large amounts of network traffic for future analysis that supports use cases like incident response. Bricata did not meet inclusion revenue thresholds for this research.

**Fidelis Cybersecurity**

Fidelis Cybersecurity, headquartered in Washington, DC, has been in the network security market since the mid-2000s, originally with a network DLP solution with a content and session focus. As the threat landscape over the last decade has increasingly moved to content-based threats, Fidelis has further aligned its network security offerings to also protect against an increasing range of threats, including certain types of threats that can be difficult to detect using traditional packet-based technologies. Its product also now has native advanced threat integration, as well as a very credible incident response endpoint technology that was acquired from Resolution1 in 2015. Fidelis also has the ability to have its appliances generate a rich flavor of metadata that is stored to allow for analysis that enables effective near-real-time as well as historical incident investigation capabilities. This integrated metadata storage and analysis capability is seen as innovative in the IPS industry. We expect Fidelis to orient to the IPS market more explicitly over the next 12 to 18 months.

**FireEye**

FireEye is a U.S. based cybersecurity company headquartered in Milpitas, California. It is a well-known security vendor specializing in advanced threat protection and incident response. In recent years, it has expanded its product and service portfolio extensively with a mix of organic growth and acquisitions. These additions are with managed services, cloud security analytics, TI, network forensics and security orchestration, and via adding IPS to its most well-known solution, Network Security (NX Series) solution, which is available as a physical or virtual appliance. As a recent entrant to this long-established market, FireEye has taken a different approach by making its IPS a part of the subscription for the NX Series, meaning there is no upfront cost to have FireEye's IPS if you have NX technology. FireEye's IPS is, therefore, an add-on to the NX range, augmenting its threat prevention and detection capabilities with network blocking capabilities by leveraging the Snort engine. FireEye is competing with independent IPS technology on a limited set of use cases, primarily for advanced threats and network elements of malware. FireEye did not meet inclusion revenue thresholds for this research.

**Evaluation Criteria**

**Ability to Execute**

**Product or Service (and customer satisfaction in deployments):** Performance in competitive assessments and having best-in-class detection and signature quality are highly rated. A vendor should compete effectively to succeed in a variety of customer placements.

**Overall Viability:** This includes overall financial health and prospects for continuing operations.

**Sales Execution/Pricing:** This includes dollars per Gbps, revenue, average deal size, market share change, installed base, presence in cloud deployments and use by managed security service providers (MSSPs). Winning in competitive shortlists versus other IDPS vendors is also highly weighted.

**Market Responsiveness/Record:** This includes delivering as promised on planned new customer-valued features.

**Marketing Execution:** This includes delivering on features and performance, customer satisfaction with those features, and those features beating competitors in selections. Delivering products that are low latency and multi-Gbps, have solid internal security, behave well under attack, have high availability, and have available ports that meet connectivity demands is rated highly. Speed of vulnerability-based signature production, signature quality and dedicating internal resources to vulnerability discovery also are highly rated.

**Customer Experience:** This includes management experience and track record, as well as 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 IDPS is actively managed, is another key criterion.

**Operations:** The ability of the organization to meet its goals and commitments. Factors include the quality of the organizational structure, including skills, 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 or Service | High |
| Overall Viability | High |
| Sales Execution/Pricing | Medium |
| Market Responsiveness/Record | Medium |
| Marketing Execution | Medium |
| Customer Experience | High |
| Operations | Medium |

Source: Gartner (January 2017)

**Completeness of Vision**

**Market Understanding:** These include providing the correct blend of detection and blocking technologies that at least meet (and ideally exceed) the requirements for next-generation IDPSs. Innovation, forecasting customer requirements, having a vulnerability rather than an individual exploit product focus, and being ahead of competitors on new features and integration with other security solutions (such as ATD) are highly rated. Also included is an understanding of and commitment to the security market — and, more specifically, to the network security market. Vendors that rely on third-party sources for signatures, have weak or "shortcut" detection technologies, and have limited ATD approaches score lower.

**Marketing Strategy:** This includes a clear and differentiated set of messages consistently communicated throughout the organization and externalized through the web presence, advertising, customer programs and positioning statements.

**Sales Strategy:** This includes prepurchase and postpurchase support, value for pricing, and providing clear explanations and recommendations for addressing detection events.

**Offering (Product) Strategy:** This includes an emphasis on product roadmap, signature quality, performance, and a clear differentiated advanced threat detection strategy. Successfully completing third-party testing — such as the NSS Labs IDPS tests and Common Criteria evaluations — are important. Vendors do not score well if they commonly reissue signatures, are over reliant on behavioral detection and are slow to issue quality signatures.

**Business Model:** This includes the process and success rate of developing new features and innovation. It also includes R&D spending.

**Innovation:** This includes R&D and quality differentiators, such as performance, management interface and clarity of reporting. Features that are aligned with the realities of network operators, such as those that reduce "gray lists" (for example, reputation and correlation), are rated as important. The roadmap should include moving IDPS into new placement points and better-performing devices, as well as incorporating advanced malware detection. Rich next-generation IDPS features (beyond only reputation feed) are highly weighted, as are robust network sandboxing capabilities and the ability to provide placements in the cloud.

**Geographic Strategy:** This includes the technology provider'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.

| **Table 2.**   Completeness of Vision Evaluation Criteria | |
| --- | --- |
| **Evaluation Criteria** | **Weighting** |
| Market Understanding | High |
| Marketing Strategy | Low |
| Sales Strategy | Medium |
| Offering (Product) Strategy | High |
| Business Model | Medium |
| Vertical/Industry Strategy | Not Rated |
| Innovation | High |
| Geographic Strategy | Low |

Source: Gartner (January 2017)

**Quadrant Descriptions**

**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 IDPS deployments, and in winning competitive assessments. Leaders produce products that embody next-generation IDPS capabilities, provide high signature quality and low latency, innovate with or ahead of customer challenges (such as providing associated ATD technologies to make enriched IDPS intelligence) and have a wide range of models, including high throughput 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; however, they do not often fare well in competitive selections, and they generally lag in new feature introductions.

**Visionaries**

Visionaries invest in leading-edge/"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, especially new next-generation IDPSs or novel anti-threat capabilities, 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, such as those in a particular geography or vertical market. 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 segment, or a vertical market), and they often do so more efficiently than Leaders. Niche Players frequently are smaller vendors, and do not yet have the resources to meet all enterprise requirements.

**Context**

* Current users of network IDPSs highly prioritize next-generation network IDPS capabilities at refresh time.
* Current users of NGFWs look at a next-generation network IDPS as an additional defense layer, and expect best-of-breed signature quality.
* Enterprises with traditional network IDPS and firewall offerings should build and plan to execute migration strategies to products that can identify and mitigate advanced threats.

**Market Overview**

According to Gartner market research, the worldwide IDPS market in 2016 for stand-alone appliances was $1.76 billion. We forecast that the IDPS market will likely start to decline in stand-alone revenue from 2017 onward, from $1.69 billion in 2015 to $1.59 billion by 2018 (see "Forecast: Information Security, Worldwide, 2014-2020, 3Q16 Update" ). Data collected from vendors in this Magic Quadrant validates this range. Factors driving those estimates include:

* The threat landscape is currently aggressive, but major IDPS vendors were initially slow to address botnet and advanced targeted threats. Some spending that could have gone to IDPS products instead has gone to advanced threat detection and network forensics products (see "Five Styles of Advanced Threat Defense" ). With leading products now containing this feature, IDPS is no longer losing out to this feature being missing.
* NGFWs are taking a significant portion of the stand-alone perimeter IDPS market as next-generation IDPSs are absorbed into firewall refreshes and are enabled in existing IDS-/IPS- capable firewalls.
* IDPS continues to be a significant network security market, but needs to start addressing the internal use case better that covers protection of internal assets, and helps detect and prevent lateral movement. The "flat internal network" problem is one that Gartner sees still existing in many of our clients' networks. If IDPS vendors can address this significant issue in organizations with better messaging and use case support, it may cause this market to instead flatten out, rather than decline through 2020.
* Organizations are adopting public cloud IaaS for their compute. Traditional firewall vendors are not showing signs of traction due to SDN and IaaS providers delivering basic routing and network address translation (NAT) as part of their offerings for free or little cost. IDPS still has an opportunity here, as there is no sign of these providers delivering more advanced DPI security capabilities and, concurrently, many IDPS vendors can be deployed in these more agile compute architectures.
* As market penetration for these integrated and cloud-resident IDPS form factors has advanced, the IDPS appliance market is predicted to start declining in 2017, but from a large base.
* TI integration is now almost pervasive in the IDPS market. This has added significant context and visibility to both traditional and advanced threats. It has also added to the ability for third-party integrations to occur, extending the life of next-generation IDPSs by allowing them to perform the "block and tackle" role of outbound data exfiltration detection and prevention.
* IDS is still a valid use case, and Gartner is considering the further inclusion of newer delivery methods — for example, fully managed and cloud — that are not currently under consideration for this Magic Quadrant.

As adjacent platforms continue to integrate IDPS technology of various levels of efficacy, growth in the stand-alone IDPS market will continue to slow.

**Next-Generation IDPSs Are Available From Leading Vendors**

Next-generation IDPSs have had two primary performance drivers: the handling of network traffic at near-wire speeds, and the deep inspection of that traffic based on more than just signatures, rules and policies. The first generation of IDPSs were effectively a binary operation of "threat or no threat," based on signatures of known vulnerabilities. Rate shaping and quality of service were some of the first aspects that brought context to otherwise single-event views. As inspection depth has increased, digging deeper into the same silo of the traffic yields fewer benefits. This next generation of IDPSs applies fuller stack inspection, but also applies new sources of intelligence to existing techniques:

* Signatures — These are often developed and deployed rapidly in response to new threats, and are often exploit-specific, rather than vulnerability-generic.
* Protocol analysis — This enables the IDPS engine to inspect traffic for threats, regardless of the port that the traffic is traversing.
* Application and user awareness — It should identify applications and users specifically.
* Context awareness — It should be able to bring multiple sources together to provide more context around decisions to block sessions. Examples include user directory integration that ties IDPS rule hits overlaid by the user, and application and geolocation information where you can permit (or deny) access to services, based on its origin on the internet.
* TI reputation services — These include action-oriented intelligence on spam, phishing, botnets, malicious websites, web exploit toolkits and malware activity.
* Content awareness — It should be able to inspect and classify inbound executables and other similar file types, such as PDF and Microsoft Office files (that have already passed through antivirus screening), as well as outbound communications.
* User extensibility — The solution should support user-generated IDPS signature content.
* Advanced threat detection — The solution should be able to use various methods to identify and send suspicious payloads to another device or cloud service to execute and positively identify potential malicious files.
* Historical analysis — The solution should assist or support the short to medium traffic storage either in full or via other means, like metadata extraction and NetFlow. This can identify applications, files, users, communications, URLs, domain names, etc. It is then used for analytics and incident investigation use cases.
* Optionally support entry-level routing and network address translation — The solution will optionally be able to process traffic and act as a Layer 3 control and enforcement point. This means basic routing and network address translation can occur. This supports use cases in which security and performance features are paramount, and only course-grain firewall rules are required, using a limited-in-size rule base.

These advances are discussed in detail in "Defining Intrusion Detection and Prevention Systems." Best-of-breed next-generation IDPSs are still found in stand-alone appliances, but have recently been incorporated into some NGFW platforms.

**Advanced Threat Detection Is Now Available From Next-Generation IDPSs**

Along with SSL decryption, Gartner IDPS Magic Quadrant customer references regularly mention advanced threat detection as a feature in future IDPS selections. To compete effectively, next-generation IDPS vendors must more deeply integrate ATD capabilities to step up their ability to handle targeted attack detection — for malware detection, anomaly detection, and also for outgoing communication with command-and-control servers from infected endpoints.

Gartner notes that some specialized advanced threat detection vendors have evolved their products' capabilities to deliver basic network IDPS capabilities to complement their advanced threat solutions. If other advanced threat vendors bring "good enough" IDPS capabilities from adjacent network security areas to market, clients will have more options and new IDPS approaches to choose from. This could, in some way, cause this market to instead flatten out in revenue versus the predicted decline.

**IDPS Appliance Market Consolidation Continues, but Internal Deployments, Cloud and Pure Managed Security Service Offerings Gain Traction**

In 2013, McAfee acquired Stonesoft, and Cisco acquired Sourcefire. Both of these acquiring vendors had their own IDPS technologies before they made their purchases. Both vendors have streamlined their IDPS portfolios to offer one stand-alone solution. Additionally, both have continued to execute well in the IDPS market, despite other changes and acquisitions in their respective businesses. Bricata is a new IDPS vendor that has an additional focus on post breach features by supporting large amounts of on-chassis storage capacity, allowing for investigation use cases and the ability to replay old traffic, but with up-to-date signatures and intelligence to help detect breaches.

As the IDPS market growth rate potentially flattens or even may decrease, we expect the strongest next-generation IDPS providers to grow both their market share and revenue, driving weaker solutions or point approaches from the market and leaving buyers with a stable set of vendors from which to choose.

Mostly cloud-based IDS solutions, such as Alert Logic, are today outside the scope of this Magic Quadrant's selection criteria, as are pure IDPS managed sensors, such as those from Dell SecureWorks and Trustwave. Such solutions are gaining momentum, and Gartner will monitor their progress. We are considering the inclusion of such options in future Magic Quadrants.

**More IDPSs Get Absorbed by NGFWs, but the Stand-Alone IDPS Market Will Persist**

With the improvement in availability and quality of the IDPS within the NGFW, NGFW adoption reduces the need for a dedicated network IDPS in enterprises, especially smaller ones. However, the stand-alone IDPS market will persist to serve several scenarios:

* The incumbent firewall does not offer a viable next-generation IDPS option.
* Clients continue to report significant performance impact of enabling IDPS in their NGFWs. This impact, in real-world feedback from Gartner clients, is frequently in the 40% to 80% range, depending on the traffic profile. For environments that require sustained throughput of 10 Gbps to 20 Gbps and higher, a separate NGFW and next-generation IDPS is a sensible architecture to pursue.
* Separation of the firewall and IDPS is desired for organizational or operational reasons, such as where firewalls are a network team function and IDPSs and IDSs are run by the security team.
* A best-of-breed IDPS is desired, meaning a stand-alone next-generation IDPS is required.
* Niche designs exist (as in certain internal deployment scenarios) where a IDPS capabilities is desired, but don't require a firewall. This can also apply to SDN and public cloud scenario's where routing/NAT functions are covered in the base platform and only advanced network inspection is required.
* For internal segmentation projects, next-generation IDPS deploys at Layer 2 transparently, with better reliability and higher quality security content than a transparent NGFW, and therefore is considerably easier to deploy while providing the best protection available.

While the trend is toward IDPS consolidation on NGFWs, Gartner sees anecdotal examples of organizations switching back from an NGFW to a stand-alone IDPS, where improved blocking quality and performance are required.

**IDS Is Still Widely Deployed and Effective**

Gartner continues to see a credible percentage of user organizations that are still deploying IDS technology purely for monitoring and visibility use cases, and not for blocking, especially in the network core or where any kind of blocking technology often cannot meet performance needs or will not be considered for deployment by the operations team.

While going "in-line" with this technology is preferred as it at least offers the capability to block should the need arise, IDS is still a staple in a large number of environments. As the adaptive security architecture highlights (see "Designing an Adaptive Security Architecture for Protection From Advanced Attacks" ), detection is a critical capability. The number of breaches in recent history highlight clearly that organizations large and small are failing in their ability to perform detection and response once threats are active inside the network. IDS is still very effective at delivering threat detection capabilities in familiar ways to organizations security teams.

Some organizations are getting additional life out of older IDPS investments (or by making new investments in IDS) by enabling IDPS in the NGFW and moving their existing dedicated IDPS and IDS elsewhere in the environment. So rather than decommission stand-alone IDPSs, they instead deploy in "IDS mode" internally or on other parts of the network for monitoring of what is generally called east/west traffic, versus the traditional north/south traffic at the internet perimeter. Detecting vulnerability exploitation, service brute forcing, botnet command and control channel activity, application identification, and so on, are all standard features of modern IDPSs and IDSs, and still have utility.

**Endpoint Context Is Increasingly Important and Available**

An interesting development over the last few years is how vendors are increasingly bringing in various levels of details from endpoints. This compliments IDPSs on the network significantly. As a simple example, being able to dig into traffic by mapping the specific binary on the host that is generating the traffic is a very important use case, which previously would only be possible from multiple consoles or via event processing in an SIEM. This is increasingly becoming available from IDPS vendors, like Cisco and McAfee, as available built-in options. Other vendors in this Magic Quadrant, like IBM with BigFix and Resilient Systems have the opportunity to further add significant value for organizations by making the network IDPS and IDS more effective with host context and also the reverse with host agents being more effective by having a complimentary network option.

**Retrospective Analysis Is Useful as an IDS Use Case**

Adversary "dwell time" (the time a person or group are inside an environment undetected) is still a serious problem today. Organizations are still taking a long time to find out that they have been breached. One feature that is an interesting use case for IDS is the ability to take "new security content and intelligence," but use that new knowledge of threats on "old data." Today, most IDPS and IDS vendors don't do this natively; you would have to collect the old data via packet capture, then load it onto something like a dual NIC machine and "replay" that traffic through an IDPS segment (or to a SPAN port). You would then need a policy that likely only included the new content (excluding the old) so that you are only seeing alerts from the new content and not events from signatures that have likely already fired. It's possible, but takes additional resources with manual overheads, which means that most organizations don't take advantage of this capability.

There are solutions, however, that do some of this, but they are more often packet capture technologies like ProtectWise and Arbor Network's Security Analytics that can leverage an IDS engine to do this. Examples of this could be when a big threat is discovered, like Heartbleed, you could replay traffic from the previous month or two and look for activity related to that threat that you didn't detect the first time due to that content not being available.

IT security and risk management leaders are encouraged to investigate this use case as it can help close the dwell time gap that exists today. For example, if you could say every week or two weeks, go back and reanalyze the previous one or two months' worth of traffic for threats that new security content detects in old data that could provide significant value to your organization's ability to address the dwell time gap.

**Developments in Threat Intelligence Have Implications for IDPSs**

TI or reputation feeds have provided much-needed additional visibility, threat context and blocking opportunities for IDPS deployments. In the last few years, all IDPS vendors have added these "feeds" to their existing product lines. TI feeds have the following strengths and challenges:

**Strengths:**

* Time to coverage — for example, a piece of malware can be inspected and TI feeds updated with detection/blocking metadata like IP address, DNS host name or URL, which is considerably faster than the deep-soak signature testing cycle that IDPS vendors require to ship IDPS security content.
* Improved context and visibility on the threat landscape for fast-moving threats, particularly malware and botnets.
* Most feeds have the concept of not only the threat (botnet), but also a score (often from 0 to 100, for example), allowing users to define the threshold of when alerting versus blocking occurs.
* Allow for the use of relatively accurate geographic IP details for context and blocking opportunities.
* Allow for third-party integration via IDPS vendors' APIs of other feeds. This normally requires additional work.

**Challenges:**

* TI feeds are proprietary in nature, and users cannot use open standards such as Structured Threat Information Expression (STIX)/Trusted Automated Exchange of Indicator Information (TAXII) without additional software.
* Like all security content, TI feeds are prone to various levels of false positives, meaning clients may often have to tune policies to avoid blocking nonmalicious traffic.
* Most vendors, without third parties creating their own integrations or doing so from additional products, generally only use their own TI feeds. These are limited in scope and coverage of the threat landscape from that vendor only.
* The volume of TI that is available today is literally staggering. There are well over 100 free (open-source) feeds and dozens of commercial and industry-led initiatives that organizations can consume. The issue is in how to target the type, volume and variety of TI so that it doesn't:
  + Overload security operations with yet more events
  + Bring false positives from low- or semi-trusted sources
  + Overload the IDPS with too much TI, which can significantly affect performance

STIX/TAXII standards are now at a point that they have the momentum of security organizations, including computer emergency response teams (CERTs), global information sharing and analysis centers (ISACs), vendors, and end users. While nascent, in the coming two to three years, we expect to see an acceleration of block-and-tackle vendors — such as firewall, intrusion prevention, secure web gateway, endpoint threat detection and response (ETDR), and SIEM tools — all supporting full implementations of these open standards. These two standards in particular will accelerate the ability to consume threat information and then act on it at time scales not previously possible, and will do so in an end user's environment that has a mixed ecosystem of vendors.

Finally, while not meeting the definition of a next-generation IDPS, and therefore not included in this research, in-line TI appliances have appeared on the market. These are not fully featured IDPSs per se; they only offer blocking around source, destination IP address, DNS and sometimes URLs, meaning they are based purely on TI feeds. However, they often support much larger TI databases than are available from leading IDPS vendors. Example vendors are Centripetal Networks, LookingGlass and Ixia.

**Evidence**

Gartner used the following input to develop this Magic Quadrant:

* Results, observations and selections of IDPSs, as reported via multiple analyst inquiries with Gartner clients
* A formal survey of IDPS vendors
* Formal surveys of end-user references
* Gartner IDPS market research data

OASIS taking over the development of the STIX/TAXII standard: Oasis-open, ["OASIS Advances Automated Cyber Threat Intelligence Sharing With STIX, TAXII, CybOX."](https://www.oasis-open.org/news/pr/oasis-advances-automated-cyber-threat-intelligence-sharing-with-stix-taxii-cybox) 16 July 2015.

Details on [STIX](http://stix.mitre.org/) and [TAXII](http://taxii.mitre.org/) .

WINS Common Criteria: ["WINS Technet SNIPER IDPS V5.0 E2000 Certification Report"](http://www.commoncriteriaportal.org/files/epfiles/NISS-54-2006-EN.pdf) and [Common Criteria: Certified Products](http://www.commoncriteriaportal.org/products/) .

HP divests the TippingPoint division to Trend Micro: Trend Micro, ["Trend Micro Acquires HP TippingPoint, Establishing Game-Changing Network Defense Solution."](http://newsroom.trendmicro.com/press-release/company-milestones/trend-micro-acquires-hp-tippingpoint) 21 October 2015.

Intel Security divests its firewall products: S. Kuranda. ["Intel Security to Sell McAfee NGFW, Firewall Enterprise Businesses To Raytheon."](http://www.crn.com/news/security/300078604/intel-security-to-sell-mcafee-ngfw-firewall-enterprise-businesses-to-raytheonwebsense.htm) CRN, 27 October 2015.

**Evaluation Criteria Definitions**

**Ability to Execute**

**Product/Service:** Core goods and services offered by the vendor for 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:** Viability includes an assessment of the overall organization's financial health, the financial and practical success of the business unit, and the likelihood that the individual business unit will continue investing in the product, will continue offering the product and will advance the state of the art within the organization's portfolio of products.

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

**Market Responsiveness/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 initiatives, 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 to 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 website, advertising, customer programs and positioning statements.

**Sales Strategy:** The strategy for selling products 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 sets 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 vertical markets.

**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.

[](https://www.gartner.com/technology/contact/become-a-client.jsp?cm_sp=bac-_-reprint-_-banner)

© 2017 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. or its affiliates. This publication may not be reproduced or distributed in any form without Gartner's prior written permission. If you are authorized to access this publication, your use of it is subject to the [Usage Guidelines for Gartner Services](https://www.gartner.com/technology/about/policies/usage_guidelines.jsp) posted on gartner.com. The information contained in this publication has been obtained from sources believed to be reliable. Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information and shall have no liability for errors, omissions or inadequacies in such information. This publication consists of the opinions of Gartner's research organization and should not be construed as statements of fact. The opinions expressed herein are subject to change without notice. Gartner provides information technology research and advisory services to a wide range of technology consumers, manufacturers and sellers, and may have client relationships with, and derive revenues from, companies discussed herein. Although Gartner research may include a discussion of related legal issues, Gartner does not provide legal advice or services and its research should not be construed or used as such. Gartner is a public company, and its shareholders may include firms and funds that have financial interests in entities covered in Gartner research. Gartner's Board of Directors may include senior managers of these firms or funds. Gartner research is produced independently by its research organization without input or influence from these firms, funds or their managers. For further information on the independence and integrity of Gartner research, see "[Guiding Principles on Independence and Objectivity.](https://www.gartner.com/technology/about/ombudsman/omb_guide2.jsp)"