Magic Quadrant for Intrusion Detection and Prevention Systems

Published: 10 January 2018 **ID:** G00324914

Analyst(s): Craig Lawson, Claudio Neiva

IDPS continues to be absorbed by firewall placements at the perimeter, yet still offers the best detection efficacy and a central prevention, detection, and response solution on a network. Security and risk management leaders should seek innovation in advanced analytics and public cloud support.

Strategic Planning Assumptions

By year-end 2020, 70% of new stand-alone intrusion detection and prevention system (IDPS) placements will be cloud-based (public or private) or deployed for internal use cases, rather than the traditional placement behind a firewall.

By year-end 2020, 60% of IDPS deployments will be augmented with the use of analytics methods, like machine learning and user and entity behavior analytics, up from less than 10% today.

Market Definition/Description

The network IDPS market is composed of stand-alone physical and/or virtual appliances that inspect network traffic, either on-premises or in virtualized/public cloud environments. 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 (i.e., intrusion detection system [IDS]) is still often used, a large number of appliances are still deployed in line to allow for blocking capabilities. They provide detection via several methods — for example, signatures, protocol anomaly detection, various methods of analytics, 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. For detection mode, clients have justifiable concerns over how this technology is just another "event canon" generating alerts that, even if events of interest are there, are drowned out by noise. 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").

So, while the stand-alone IDPS market is forecast to start shrinking from 2017 (see "Forecast: Information Security, Worldwide, 2015-2021, 3Q17 Update"), 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.

In addition, some vendors such as Alert Logic and McAfee 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 reasons:

- When separation of duties means that some networking functions (firewalls) are managed by a different team managing security (i.e., IDPS)
- Behind the firewall as an additional layer of defense to inspect north-south traffic
- Behind an application delivery controller (load balancer) to inspect traffic allowed
- When best-of-breed detection efficacy is required
- As an IDPS on the internal network in line to provide protection/detection for internal assets
- As an IDS monitoring the internal network for lateral movement of threats and other compliance mandates
- When high IDPS throughput and low-latency performance are required
- To provide network security separation (segmentation) 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
- For network-based intrusion and threat detection using additional methods like advanced analytics (such as user and entity behavior analytics [UEBA]) to detect threats that have bypassed other controls

Magic Quadrant

Figure 1. Magic Quadrant for Intrusion Detection and Prevention Systems

Source: Gartner (January 2018)

Vendor Strengths and Cautions

Alert Logic

Alert Logic is a privately held security-as-a-service provider based in Houston, Texas. Services it offers include managed IDS, web application firewall (WAF), log management and vulnerability management. Alert Logic's IDS is built on a Snort foundation with additional anomaly-based signatures, heuristics and supervised machine learning intelligence. It is offered in two packages: Alert Logic Threat Manager is an IDS-only offering and includes vulnerability management capabilities; and Alert Logic Cloud Defender includes out-of-band WAF and log management, along with detection based off of 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 applying 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 with managed components, 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 high-throughput detection needs by scaling horizontally, not in the appliance.

Strengths

- Alert Logic is especially strong in public cloud and virtualized environments where the solution can be deployed quickly and enabled by prebuilt integrations via Chef/Puppet/Ansible.
- Customers value Alert Logic's ease of use.
- Alert Logic's capability to deploy, and to rapidly shift an existing deployment, is ideally suited for agile and DevSecOps environments.
- Alert Logic is one of the first vendors to use analytics and machine learning to postprocess IDS event streams. This improves its ability to detect threats and incidents that take multiple days/weeks to evolve faster and with more efficacy.

Cautions

- The solution is "IDS only" and blocking requires additional solutions, using Alert Logic's WAF or via the capability to send blocking requests to firewalls.
- There is no "user" context in the product today, which reflects its main use case for internet-facing and cloud deployments.
- Alert Logic doesn't have advanced threat or sandbox integrations in the product today, limiting its ability to detect threats in network objects/files that traverse a network.

Cisco

Cisco, headquartered in San Jose, California, has a broad security product portfolio and has had IDPS offerings for many years. The Sourcefire acquisition has continued to be a positive and strong influence on Cisco's network security portfolio, giving the company traction in the firewall market that it would not have garnered otherwise. The Firepower IDPS line also shares a management console with the Cisco firewall offerings, called the Firepower Management Center.

Cisco has 22 models of IDPS available in the 4100, 7000, 8000 and 9300 Series Appliances, and virtual appliances for VMware deployments. They range from 50 Mbps through to 60 Gbps of inspected IDPS throughput, giving Cisco a very versatile appliance range — from remote branch up to demanding data center use cases. 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 enterprise firewall, 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, making its IDPS technology ubiquitous throughout its network security portfolio. It is also the most widely deployed IDPS on the market today. The continued evolution of OpenAppID and the addition of DNS security for features like inspection and sinkholing are also seen as net improvements for detection and prevention use cases.

New capabilities introduced include URL-based security intelligence and AMP Threat Grid integration. Cisco will benefit from IBM's exit of the IDPS market as IBM is now co-selling Cisco IDPS and directing renewals.

Strengths

- Gartner's clients that are described as advanced security with larger budgets enjoy Firepower's usefulness as an IDS analysis/investigation 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 return merchandise authorization (RMA) response 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 supplies coordinated malware detection at the network, sandbox and endpoint layers. This coordination differentiates it from many competing solutions.
- Talos, Cisco's security research organization, has a large team researching malware and vulnerabilities and developing security content for all Cisco security products, including writing signatures and determining default blocking policies. During the evaluation period, Talos discovered 171 vulnerabilities. It is a key differentiator for this technology as it demonstrates Cisco's continued ability to understand specific threats and the threat landscape in general as it relates to IDPS.

- Support for its own Cisco's Application Centric Infrastructure (ACI) architecture with its IDPS is well-implemented for heavily virtualized environments that use it, although ACI is not widely deployed yet.

Cautions

- Some Type A clients have expressed concern that IDPS innovation has slowed as Cisco works on integration with acquired capabilities and focuses on its enterprise firewall product line. Customers with these concerns should insist upon roadmap clarity that makes planned IDPS enhancements explicit. For example, the ability to take the rich telemetry and then do advanced analytics is still not in the product, despite smaller startups having this capability.
- There are a plethora of support options available, sometimes complicating choices; and the support maintenance percentage (often based off recommended retail price [RRP] versus sale price) is on the higher end of solutions in the market today.
- Cisco initially lagged behind other competition in introducing support for Amazon Web Services (AWS), and has yet to offer support for Microsoft Azure. It also doesn't yet have support for a "virtual overlay" to enable coverage of agile workloads like some of its competitors.
- Cisco does not support the full range of vulnerability assessment and management tools to allow for policy to be derived from, and priorities based on, the vulnerabilities that exist in an environment; but it does have an API that would allow for other tools to do so. Firepower Management Center, however, remains an effective way to model the types of systems on a network within the Cisco IDPS solution itself.

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, security analytics, threat intelligence 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, threat intelligence, network forensics and security orchestration, as well as via adding IPS to its most well-known solution, the FireEye Network Security (NX Series) solution, which is available as a physical or virtual appliance. The virtual appliances support a range of hypervisors, including Amazon AWS, but not Microsoft Azure.

In the past year, FireEye has improved its architecture by decoupling the IDPS (the NX Series) from the Multi-Vector Virtual Execution (MVX; for ATD/sandboxing) presenting the concept of a "smart node" (the IDPS appliance) and the "smart grid" (MVX/sandbox) with version 7.9 of the solution. Additionally, the "smart grid" MVX now supports bursting from the local instance(s) to the cloud, allowing for better scalability without the need for additional on-premises appliances. These evolutions let the solution scale horizontally for performance, and allow for better support to detect lateral movement of threat use cases (versus just north-south) and also for distributed environments.

FireEye is now competing more directly with independent IDPS technology on more use cases this year, but, primarily, its focus is on advanced threats and network elements of malware on the inside of the network.

Strengths

- FireEye NX is designed for detecting and preventing known and unknown exploits to servers and endpoints, and its focus on exploitation and malware is well-regarded.
- The ability to automatically correlate alerts from the IDPS and MVX is a differentiator for day-to-day security operations as it can significantly reduce the alerts that security staff need in order to operate the solution.
- FireEye has consistently proved its ability to detect advanced threats, including zero days, via its large research and threat intelligence team. All of its products benefit from this capability, including the IDPS.
- Threat intelligence integration from existing teams, as well as subscriptions from iSIGHT Threat Intelligence (from the iSIGHT Partners acquisition in 2016), make it a very capable threat detection/prevention solution.

Cautions

- The ability to deep dive in the IDPS policy by severity, Common Vulnerabilities and Exposures (CVE), name, etc. is limited in the console compared to other IDPS solutions.
- It does not have capabilities in application/user-based policies, and delivering these is provided by FireEye's endpoint security (HX Series) solution.
- FireEye NX does not have the ability to tune the IDPS policy by using vulnerability scan data.
- The IDPS engine is still based on Snort; it would be improved significantly by using the improved Suricata engine to support higher throughput.
- Throughput has now improved with the "smart node" architecture, but is still limited to 10 Gbps — less than a majority of its competitors.

Hillstone Networks

Headquartered in Beijing and Santa Clara, California, 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 23 IDPS models; however, only five are available to the global market — the S-series models of appliances. These appliances range in performance from 1 Gbps to 50 Gbps, an increase in number and, in particular, in throughput over past year. Hillstone does not offer a virtual IDPS model, but it does support on-box virtual instances, including the ability to apply

performance constraints on each virtual instance. IDPS signatures are developed internally and obtained from other partners.

During the evaluation period, Hillstone introduced several new models. New enhancements introduced in that period include improved antivirus efficacy, HTTPS flood request protection and better IDPS reporting. Additionally it has three new features, Abnormal Behavior Detection (ABD) engine, Advanced Threat Detection (ATD) and a cloud sandbox. ABD is Hillstone's analytics approach that does network baselining looking for abnormal behavior. The sandbox is also interesting for the IDPS market because it allows for "fuzzy" malware behavior signatures to be used to help convict new iterations of existing families of malware.

Strengths

- Hillstone continues to be a good option for clients that are already consuming other Hillstone solutions, midmarket buyers and those located in Southeast Asia.
- The introduction of its cloud-based "read only" console for basic monitoring and checking alerts will be well-received by midmarket clients.
- Hillstone continues to be very competitive on price/performance metrics for IDPS across a wide scope of throughput ranges.
- Hillstone supports a wide range of detection and prevention options with signatures, behavioral analytics, anti-malware and cloud-based sandboxing available as options.

Cautions

- There is no Active Directory integration for user-based controls and only on-box user accounts are supported.
- General analyst work for alert processing is functional, but basic; for example, users can't create search templates that can be reused to speed up investigations and aid in better reporting.
- Reporting is basic and only supports PDF exporting.
- Hillstone is active, but not visible in other non-Asia markets. Clients should ensure there is relevant and contestable support for their deployments in these markets.

McAfee

McAfee, based in Santa Clara, California, has now completed its move out of Intel, creating a stand-alone company. The new McAfee company has a significant product portfolio across network, server, cloud, web, security information and event management (SIEM), network analytics, data loss prevention (DLP), and endpoint security. In November 2017, it was also announced McAfee would acquire SkyHigh Networks, a leading cloud access security broker (CASB) provider. Intel will retain a 49% equity interest in McAfee. This move to being an independent entity has been a net positive for the company. It has led to better roadmap execution and will allow McAfee to better focus and compete in the security market. Its IDPS, called the Network Security Platform (NSP), is a main

element of its network security product offerings, McAfee has focused heavily on roadmap execution and integration of this range into its other portfolio of products.

The 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. In addition, McAfee has significantly enhanced the ability to operate natively in public cloud with integrations that support both detection and in-line prevention modes of operation, in the same scalable way that clients operate their cloud environments with a complementary host agent to forward traffic. Gartner sees clients deploying NSP mostly in blocking mode (for IPS), but observes a number of detection mode use cases as well. McAfee's Advanced Threat Defense (ATD sandbox) is a natively integrated component and it supports deployments both on-premises and from the cloud. The Network Threat Behavior Analysis (NTBA) product, like ATD, can be natively integrated into an IDPS deployment, offering improved network visibility, including being able to detect threats and provide enhanced metadata to security teams. This is a leading architectural approach today.

Strengths

- Clients appreciate NSP's sophisticated policy options, 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 ATD, endpoint context, NTBA 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.
- Today, McAfee's support for public cloud deployments is leading the market for this capability, as it provides the ability to support the dynamic nature of infrastructure as a service (IaaS), which makes heavy use of immutable infrastructure.

Cautions

- McAfee is an IDPS provider that lacks a firewall line. The IDPS range is vulnerable to combined firewall plus IDPS replacements from vendors such as Cisco, Palo Alto Networks and Check Point.
- Some clients find the user interface complicated, and it needs to evolve to adopt modern UX standards and to provide better workflow that allows people to understand the implications of policy configuration changes.
- McAfee does not have the ability to natively tune its IDPS based on the vulnerability landscape of the client environment.
- Some clients have reported issues when troubleshooting the product when in IPS mode to determine specifically which configuration element(s) is blocking the specific session.

NSFOCUS

NSFOCUS is headquartered in Beijing and California. It is a large regional security vendor for Asia and is expanding to other geographies. NSFOCUS offers distributed denial of service (DDoS; via its Anti-DDoS System [ADS] offering), web application scanning (via Web Vulnerability Scanning System [WVSS]), and WAF and vulnerability management (via Remote Security Assessment System [RSAS]). The vendor also offers managed security services (MSSs) on a number of its products.

The NSFOCUS IDPS has a large range of appliances, models ranging from 300 Mbps to 120 Gbps of throughput and four virtual appliances. This is an improvement over when it was reviewed for the previous Magic Quadrant, with higher-throughput chassis now available. The virtual appliances are certified on VMware, Kernel-Based Virtual Machine (KVM) and OpenStack, but not Xen. Its IDPS includes sandboxing capabilities called Threat Analysis Center (TAC), as well as application control and anti-malware, and it can also utilize reputation-based controls. Additionally, most models support a flexible licensing scheme, allowing clients to buy a chassis from a "range," but then simply increase the inspected throughput with a licensing update — increasing throughput without having to replace the device.

Strengths

- NSFOCUS has a large client base in China with good support for region-specific applications (like instant messaging).
- NSFOCUS has a functional threat intelligence portal for clients that includes the ability to search and visualize all the data in its threat intelligence database (for the purpose of investigations) and general information that is not found in the base logs.
- NSFOCUS has its own ATD technology allowing it to detect malware that can be defined by policy of location and file type. If the cloud option is used, this feeds its entire intelligence network that is used by all of its clients.
- NSFOCUS has a functional threat intelligence portal that can also be helpful for using IDPS as it has data on IP addresses, vulnerabilities and malware with the ability to configure notifications on them.

Cautions

- The core IDPS engine is signature-based and might be prone to evasion by heavily obfuscated threats.
- There is limited ability to enforce policies based on users, but rudimentary correlation to match traffic to an internal user is possible.
- Today, there is no support for public clouds like AWS or Azure for the product, although NSFOCUS does support a range of other hypervisors like VMware.
- NSFOCUS only supports its own vulnerability scanner to tune the policy based on the vulnerability landscape of the client environment.

Trend Micro

Headquartered in Japan, Trend Micro is a large, global IT security vendor. It completed its acquisition of TippingPoint from Hewlett Packard Enterprise (HPE) in March 2016. The acquisition of TippingPoint has been a net positive for Trend Micro's IDPS product, sales and marketing operations. 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 120 Gbps of inspected throughput. The new TX Series range can run up to 40 Gbps of inspected throughput in a 1U chassis, which is one of the leading traffic/chassis combination in this market. While using Intel CPU technology, field-programmable gate array (FPGA) and a switch fabric are used in the larger models to support higher throughput, lower latency and availability — all key features for use in sensitive and more demanding data center applications. IDPS content updates are provided through Digital Vaccine Labs (DVLabs). The DVLabs team also operates the Zero Day Initiative (ZDI) program, which continues to be an excellent source of vulnerability information for Trend Micro, while also supporting independent security researchers.

The IDPS is also benefiting from synergies between TippingPoint's and Trend Micro's research teams on malware, which is enhancing the ability of the IDPS to specifically address the network-based elements of malware threats. Additionally, the Trend Micro advanced threat (sandbox) technology for its IDPS, called Deep Discovery, 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. The Security Management System (SMS) has moved from a SQL back end to Vertica for most data storage tasks now, which significantly improves performance and enables new use cases. For example, the IDPS can natively export NetFlow to the SMS manager and to itself (rather than a separate NTA/NBA tool), and is then used for real-time and historical investigations of network traffic passing through deployed IDPSs.

Trend Micro's 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.

Strengths

- Trend Micro continues to be one of the easiest to deploy and manage IDPSs on the market, including at very high throughput.
- Structured Threat Information Expression (STIX)/Trusted Automated Exchange of Indicator Information (TAXII) support is now included in the SMS Manager, making it easier to operationalize machine-readable threat intelligence (MRTI).
- While also available for end users, the DVToolkit can be used by TippingPoint support to create custom filters for end users, providing "time to coverage" value.
- TippingPoint has always excelled at very-high-throughput and low-latency hardware, and the new 8200TX supports 40 Gbps of inspected throughput in 1U, a market-leading rate from a throughput-per-rack-unit point of view. This supports the most demanding use cases for data center and high-performance network perimeters.

- During the evaluation period, the ZDI vulnerability disclosure program discovered roughly 700 vulnerabilities, which directly benefits all of Trend Micro's clients with early coverage of threats.
- SSL decryption in hardware is supported natively inside the new TX range.

Cautions

- Coverage of public/private cloud is via a separate solution with the complementary Deep Security product range, which is a host-based intrusion prevention system (HIPS)-based solution. End users should be aware that there is a difference between the two in terms of the IDPS technology used.
- End-user context is available in SMS, but customers cannot create policy for enforcement by user at this point in time.
- Today, the IDPS can only offload some objects (like URLs) to the ATD (Deep Discovery) for inspection. Deep Discovery has to be deployed separately, and it can stream threat telemetry directly into the IDPS via its SMS management server.

Vectra Networks

Vectra Networks is based in San Jose, California. It has been shipping its Cognito product since 2014 and is a leading example of using advanced analytics (like UEBA) for network IDS use cases. It focuses on detection of threats that have bypassed traditional controls and on detecting lateral movement of threats on the inside of an organization's network.

The solution is available in a physical or virtual appliance form factor. The hardware sensors, called the S-series and X-series, are distributed on the network, and the management server provides the collection, deduplication, and analytics functions. Due to its behavioral nature, content updates are infrequent (often monthly) and primarily in the form of new algorithms or enhancements to existing mathematical models used to detect threats.

Vectra's approach is innovative as it directly addresses some key issues in security operations today. First, the issue of alert fatigue, where a traditional IDS generates alerts that describe malicious activity, it also generates a large volume of alerts. Determining what is an alert and what is an incident — as the two are not the same — consumes too much time. This solution excels at the ability to roll up numerous numbers of alerts to create a single incident to investigate that describes a chain of related activities, rather than isolated alerts that an analyst then has to piece together. Second, adversary dwell time today is far too long for organizations, and having different means to detect malicious or unwanted activity is a key value proposition for Vectra. This is especially true for detecting the lateral movement of threats on a network that have already evaded other security controls.

While an IDS in terms of deployment, Vectra does have a number of other integrations with existing tools for further response actions. Example categories are firewalls, network access control (NAC), endpoint, ticketing systems and SIEM.

Strengths

- The evolution of IDS to using advanced analytics like machine learning is well-suited to the types of telemetry these technologies generate, and proves to add a different way of detecting malicious or unwanted behavior within an environment.
- Use of virtual test access point (TAP) architecture from Gigamon/Ixia, as well as other integrations with hypervisors like VMware, allows the product to be deployed into heavily virtualized environments like public, private and hybrid cloud.
- Management overhead of this product is minimal in comparison to many other solutions on the market.
- Clients appreciate the lack of onerous policy work and continuous policy updates. Vectra's algorithms require infrequent updates and little to no tuning by end users in day-to-day operations because they are based on advanced analytics.

Cautions

- This solution is "detection-centric" and has no typical prevention capabilities. It relies on integrations with other solutions like endpoint detection and response (EDR) and security orchestration, automation and response (SOAR) tools.
- Because the product is focused on threat detection only, it cannot be used for "virtual patching" of known vulnerabilities, which is a use case that is popular with Gartner clients.
- Vectra Networks is a startup and has yet to establish a global channel that has global reach. Clients outside of North America and parts of the EMEA geographies may receive different levels of support and not have access to same level of support from channel partners.

Venustech

Venustech is a security vendor headquartered in Beijing. It was founded in 1996, and has been shipping IDPSs since 2003 and dedicated IPSs 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 a good option for its existing clients consuming its other products, and large and midmarket organizations in South East Asia that need to augment existing controls with an IDPS that covers a range of threats.

Strengths

- The policy configuration interface is laid out in an easy-to-understand and -navigate manner.

- Venustech also has a traditional anti-malware plus advanced threat detection 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 is not yet making use of advanced analytics to help postprocess the events that are generated by the solution.
- Venustech is not able to use vulnerability scanning output to help derive a more effective IDPS policy.

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

- Vectra Networks

Dropped

- IBM exited the IDPS market in 2017, and thus was not included in this research.
- Huawei failed to meet revenue requirements.
- AhnLab failed to meet revenue requirements.

Inclusion and Exclusion Criteria

Only products that meet the following criteria will be included:

- Operate as a network appliance (physical or virtual) that supports both in-line intrusion prevention and/or intrusion detection of threats and network usage.

- Apply policy based on several detection methodologies to network traffic, including methods like protocol and content analysis, signatures, security analytics, behavior analysis, historical metadata analysis and threat intelligence.
- Perform packet normalization, assembly and inspection to support these detection and prevention use cases.
- Provide the ability to identify and respond to malicious and/or unwanted sessions with multiple methods, such as, allow/multiple alert types/drop packet/end session, etc.
- Adapt the policy based on correlation with vulnerability assessment tools to dynamically apply protections to protect internal and external assets found to be vulnerable.
- Have achieved network IDPS product sales and maintenance revenue globally in the year between June 2016 and June 2017 of over $10 million in U.S. dollars.
- Sell the product as primarily meeting stand-alone network intrusion detection and prevention use cases or materially compete with intrusion detection and prevention technology.
- Be visible to Gartner clients and have an active presence or an office or official partner in at least two of the major regional markets — that is, North America, South America, Asia/Pacific and EMEA — and compete in those markets.
- Have active customers buying the IDPS product(s) in the past 12 months in at least two of the major regions (that is, North America, South America, Asia/Pacific and EMEA).

Product and vendors will be excluded if:

- They are sold only as features of an NGFW or UTM platform.
- They are in other product classes or markets we already identify as different, such as network behavior assessment (NBA) products or NAC products, are not IDPS and are covered in other Gartner Research.
- They are only host IPS, such as software on servers and workstations rather than a device on the network.

This Magic Quadrant is not evaluating pure open-source technology like Snort, Suricata, Bro IDS, etc. If a vendor is using this, they must demonstrate that they are providing over and above the functionality delivered by these projects by improved packaging (hardware or software), analytics and especially additional research and security content that would take this beyond "just running Snort/Suricata/Bro IDS."

Vendors to Watch

There are eight vendors in particular that provide capabilities that are relevant to the IDPS market, but that have not fully met IDPS Magic Quadrant inclusion criteria. Organizations that need to implement IDPS functions for supported use cases should also consider and evaluate these vendors.

AhnLab

AhnLab, founded in 1995 and headquartered in South Korea, is a network and endpoint security vendor. TrusGuard IPX was released in 2012. The AhnLab product portfolio includes firewalls, ATD, DDoS attack mitigation and endpoint security solutions. It is shipping three IPX appliances between 5 Gbps and 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.

BluVector

BluVector is a recent startup, based out of Fairfax, Virginia, and has been shipping product since January 2017. It is one of a small number of new entrants that is also making use of advanced analytics techniques (like supervised machine learning) to deliver innovation to the intrusion detection market space. The solution also supports sandboxing and other methods of object inspection for detection of various fileless and other malware threats. It has invested its efforts in the core value proposition of "detecting threats" by using robust open-source solutions like Suricata/Bro IDS for general detection capabilities, malware detection and third-party threat intelligence support. The solution is running on industry-standard x86 architecture and coupled with its own custom-developed analytics capabilities — some of which are patented and have been under development for many years under Northrop Grumman before being commercialized. The solution can run on a physical appliance or in a virtual form factor as well, allowing for use in virtualized environments including public cloud. BluVector did not meet the revenue requirements for this research.

Bricata

Bricata, headquartered in Columbia, Maryland, is a startup that leverages open-source IDPS and other detection frameworks, adding software and hardware expertise to maximize performance and scalability. Its IDPS solution is based on open source that combines the Bro IDS and Suricata engines with commercial technologies, delivering signature-based and anomaly detection with network and behavior analysis. The combination 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) supports a "manager of managers" deployment architecture. Bricata's appliances ship with a large (in comparison to other solutions) amount of on-chassis storage, allowing for the collection of large amounts of network metadata and packet capture for future analysis that supports use cases like threat hunting, incident response and forensics. Bricata did not meet inclusion revenue thresholds for this research.

Corelight

Corelight is a relatively new startup based on Bro IDS, or, as it's often simply called, Bro. Many of the company's founders both founded the Bro IDS project and also have been heavily involved in its ongoing maintenance to this day. The Bro IDS open-source project, along with Snort/Suricata, powers a number of vendors' engines in network security today. Additionally, Bro IDS is in use by an extensive number of security practitioners and companies around the world. Corelight provides a way to get value out of this powerful and very popular solution with its dedicated appliances. It still needs to work on its ability to provide a centralized management platform, its event storage and analytics capabilities, and enterprise policy management capabilities. Corelight did not meet the revenue inclusion criteria for this research.

Darktrace

Darktrace is a late-stage startup security vendor with headquarters in both San Francisco and Cambridge, U.K. It is focusing on using advanced analytics, like unsupervised machine learning, to detect threats on an organization's network. Darktrace does not orientate its technology as a replacement for all IDS use cases today. Darktrace deploys like all existing IDS technology, but then uses a number of existing and its own custom-developed algorithms and analytics to build a mathematical model of users and entities on a network, looking for outliers that are turned into alerts for analysts to then investigate. The solution is primarily subscription-based.

This approach is innovative because it helps deal with a number of pressing issues in the network security market as the technology addresses alert fatigue by generating significantly less alerts for analysts to triage. The technology can also detect active threats on the inside of a network. Alternatively, because there is no "known threat" capability, it does not rapidly detect existing known threats.

Darktrace does not deploy in line, allowing for primarily intrusion detection use cases only, but it does support response options found in IDS such as TCP resets. This feature is called Antigena and is an optional extra. It is in use by a smaller, but growing, portion of its client base. Darktrace also supports integrations with other technologies, like firewalls and EDR for further response options. Antigena can operate in three modes: recommendation, active or human confirmation. The analytics does take a period of time to begin to surface information, often measured in days and weeks, based on the mathematical model built from activity on an organization's network. Some clients do report difficulty in getting more details on threats from the user interface, and day-to-day usage by security analysts has given feedback for improvements in this area.

Fidelis Cybersecurity

Fidelis Cybersecurity, headquartered in Washington, D.C., 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 past 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 those 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. It also includes strong synergies between IDPS and EDR technologies in general and clients value having credible options for these capabilities from one provider.

Fidelis also has the ability to have its appliances generate detailed metadata of network sessions that is stored to allow for analysis. This then enables effective near-real-time, as well as historical, incident investigation capabilities. Metadata storage is advantageous for historical threat hunting as well as for opportunities for correlation and detailed investigations of incidents. This is a leading capability in this market currently. This integrated metadata storage and analysis capability is seen as innovative in the IPS industry.

Fidelis does not have an extensive channel serving global markets outside of North America and Europe, so finding both resellers and contestable professional services can be difficult.

Huawei

Headquartered in Shenzhen, China, Huawei, with a core strength in networking, offers a range of network security controls, including IDS/IPS, firewall, log management, advanced threat detection (sandbox) and DDoS mitigation appliances. Huawei introduced its IDS/IPS product line, called Network Intelligent Protection (NIP) System, in 2004. NIP includes six physical appliances, ranging from 600 Mbps to 200 Gbps. They have the ability to offload objects to anti-malware and sandbox engines for additional threat detection capabilities. 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 did not meet revenue requirements for this research.

IronNet Cybersecurity

IronNet is a relatively new startup based out of Fulton. Maryland. It was formed by a number of industry luminaries in the area of cybersecurity with the goal of improving organizations' abilities to detect threats that have bypassed other controls. Its technology deploys by collecting network traffic from multiple locations, including OT networks, and then applies multiple techniques to surface events of interest to security operations teams.

IronNet also uses various analytics measures to reduce "alert fatigue." Examples of the types of threats detected are, but not limited to, suspicious beaconing, DNS tunneling, behavior changes of users/devices on the network, VPN misuse, data exfiltration and lateral movement of threat actors. As a point of visibility for a network, it also provides full packet capture to support proactive/reactive threat hunting and incident investigation and response use cases. IronNet did not meet the revenue requirements for this research.

Evaluation Criteria

Ability to Execute

Product or Service: Core goods and services that compete in and/or serve the defined market. This includes current product and service capabilities, quality, feature sets, skills, etc. This can be offered natively or as defined in the market definition and detailed in the subcriteria.

- Product service and customer satisfaction in deployments.
- Performance in competitive assessments and having best-in-class detection and security content quality are highly rated.
- Competing effectively to succeed in a variety of customer placements.

Overall Viability: Viability includes an assessment of the organization's overall financial health as well as the financial and practical success of the business unit. Views the likelihood of the organization to continue to offer and invest in the product as well as the product position in the current portfolio.

Sales Execution/Pricing: The organization'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.

Also included is pricing including dollars per Gbps, revenue, average deal size, installed base and use by managed security service providers (MSSPs), managed detection and response (MDR) and service providers.

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 to changing market demands.

Marketing Execution: The clarity, quality, creativity and efficacy of programs designed to deliver the organization's message in order to influence the market, promote the brand, increase awareness of products and establish a positive identification in the minds of customers. This "mind share" can be driven by a combination of publicity, promotional, thought leadership, social media, referrals and sales activities.

Customer Experience: Products and services and/or programs that enable customers to achieve anticipated results with the products evaluated. Specifically, this includes quality supplier/buyer interactions technical support, or account support. This may also include ancillary tools, customer support programs, availability of user groups, service-level agreements, etc.

Winning in highly competitive shortlists versus other competitors is highly weighted.

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

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 2018)

Completeness of Vision

Market Understanding: This includes providing the correct blend of detection and blocking technologies that meet or are ahead of the requirements for network intrusion detection and prevention. Innovation, forecasting customer requirements, having a vulnerability-based (rather than exploit-based) product focus, being ahead of competitors on new features, and integration with other security solutions are highly rated. Additionally, handling placement on the inside of clients' networks, deployments in public cloud, and support for using advanced threat detection and advanced analytics are considered.

Also included is an understanding of and commitment to the security market, addressing the prevailing threat landscape and, more specifically, the network security market. Vendors that rely on third-party sources for signatures or have weak or "shortcut" detection technologies score lower.

This criterion also refers to the ability to understand customer needs and translate them into products and services; that is, vendors that show a clear vision of their market — listen, understand customer demands, and can shape or enhance market changes with their added vision.

Marketing Strategy: Clear, differentiated messaging consistently communicated internally, externalized through social media, advertising, customer programs and positioning statements.

Sales Strategy: This criterion refers to a sound strategy for selling that uses the appropriate networks including: direct and indirect sales, marketing, service, and communication. It also includes partners that extend the scope and depth of market reach, expertise, technologies, services and their customer base.

Sales strategy includes pre- and postproduct sales support, value for pricing, and providing clear explanations and commendations for detection events. Also included is the ability to handle newer licensing methods that are purely subscription-based, and how this works for direct and indirect sales and channel partners.

Offering (Product) Strategy: This refers to an approach to product development and delivery that emphasizes market differentiation, functionality, methodology, and features as they map to current and future requirements. Emphasis is on product roadmap and threat detection efficacy. Successfully completing third-party testing, such as the NSS Group IPS tests and Common Criteria evaluations, is important. Vendors that reissue signatures are overreliant on potentially evadable detection methods and are slow to issue quality signatures do not score well.

Business Model: This includes the design, logic and execution of the organization's business proposition to achieve continued success. Additionally, the process and success rate for developing new features and innovation through investments in research and development are considered.

Innovation: This criterion includes:

- Direct, related, complementary, and synergistic layouts of resources, expertise or capital for investment, consolidation, defensive or pre-emptive purposes.
- Innovation, including R&D, and quality differentiators, such as performance, management capabilities, and interface and clarity of reporting.
- Features that are aligned with the operational realities of security analysts, such as those that reduce event fatigue, "gray lists" (e.g., reputation and correlation). Enterprise management capabilities,
- The ability to monitor/instrument the IDPS with a supported API that allows for additional integration, workflow and automation options. Examples include integrations with SOAR or threat and vulnerability management (TVM) tools.
- Support for open standards like STIX/TAXII for threat intelligence.
- The ability to reduce the number of alerts that require security analyst interaction and security efficacy. For those that need investigation, having high levels of threat and other environment context, which allows for better decision support, enables efficiency of operational process and supports workflow.
- A roadmap that includes moving IDPS into new placement points (for example, on the internal network or public cloud) and better-performing devices that support the reality of data centers with 10 Gbps/40 Gbps connectivity.
- Ability to assist clients with mitigating the core issue of vulnerabilities being exploited and how this work is prioritized by understanding context from tools like vulnerability assessment tools.
- Use of additional methods like endpoint context, ATD/sandbox integrations, metadata capture and analysis, and advanced analytics.

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.

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 2018)

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.
- Organizations with traditional network IDPS and firewall offerings should build and plan to execute migration strategies to products that can identify and mitigate advanced threats.
- Organizations with flat internal networks should consider deploying IPS for "virtual patching" to help prevent the exploitation of vulnerabilities, the leading cause of breaches today.
- Organizations should continue to improve their ability to detect and respond to threats as "prevention-centric only" approaches will fail eventually.

Market Overview

According to Gartner market research, the worldwide IDPS market in 2016 for stand-alone appliances was approximately $1.3 billion and is forecast to shrink in coming years. Data collected from vendors in this Magic Quadrant validates this range. Factors driving those estimates include:

- The threat landscape continues to be aggressive, with the advantage on the side of threat actors. Major IDPS vendors were initially slow to address advanced targeted threats and other classes of threat. Some spending that could have gone to IDPS products instead has gone to

advanced threat detection and network forensics products. With leading IDPS products now containing these capabilities, IDPS is no longer losing out due to this capability 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.
- IDS/IPS continues to be a significant network security market, but is forecast to flatten. A large percentage of organizations have moved to collapse their IDPS for north-south use cases into their firewall and UTMs, especially in the midmarket. This has concurrently increased the amount of IDPS on networks, but has led to constraints for traditional IDPS deployments.
- Organizations need to better address the internal use case that covers protection of internal assets, and helps detect and prevent lateral movement of threats. The "flat internal network" problem is one that Gartner sees still existing in a majority of our clients' networks, and it is a systemic issue. If IDPS vendors can address this significant issue in organizations with better messaging and use case support, it will provide more relevance for organizations' security operations programs.
- Further to the point above, most breaches today occur because of the exploitation of known vulnerabilities, not zero days. Organizations are clearly not using compensating technology like IDPS to address the issues. Below are some reasons why they are leveraged by threat actors:
  - Not being able to patch systems to the same schedule of threat actors exploiting vulnerabilities
  - The absence of a patch from the vendor
  - Systems that can't be patched due to regulatory issues and compliance mandates
  - Business-level SLAs and other functional requirements that require uptime and application functionality as the top priority
- The term "virtual patching" has been in use for some time. With the plethora of security incidents originating from the exploitation of vulnerabilities in the past two years as a direct result of this issue, IDPS vendors need to improve how they integrate telemetry from vulnerability assessment and management tools to help users derive a more effective security policy. This one principle alone would considerably lower the attack surface of every single client that implements it (see "It's Time to Align Your Vulnerability Management Priorities With the Biggest Threats").
- Organizations are adopting public cloud IaaS for their compute. Traditional firewall vendors are not showing signs of traction due to software-defined networking (SDN) and microsegmentation; but, primarily, IaaS providers are delivering basic routing, network address translation (NAT) and segmentation as part of their offerings for free or little cost. IDPS still has relevance here, as there is no sign of these providers delivering more advanced deep packet inspection (DPI) security capabilities. Concurrently, IDPS vendors are now able to deploy more effectively in these more agile compute architectures, either natively or with integration with packet brokers like Gigamon and Zentara.

- 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 pervasive in the IDPS market with vendors providing add-on integrations either for free or as an optional extra. This has added significant context and visibility for both traditional and advanced threats. It has also added to the ability for third-party integrations, extending the life of next-generation IDPSs by allowing them to perform the "block and tackle" role of outbound data exfiltration detection and prevention. Support for STIX/TAXII, however, is not uniform across the vendor landscape and IT security leaders are advised to demand from their vendors that they support open standards in their IDPS solution.
- IDS is still a widely deployed use case. With the adaptive security architecture and now continuous adaptive risk and trust assessment (CARTA; see "Use a CARTA Strategic Approach to Embrace Digital Business Opportunities in an Era of Advanced Threats"), Gartner has, since 2014, advocated for improving the ability to detect and response, as well as prevent.
- There are also credible ways to be running IDS and IPS that don't involve buying an appliance per se, but in renting one that is fully managed and monitored. This suits a range of organizations, especially in the midmarket.
- Leading vendors in 2017 have architectures that have adapted to being effective in public cloud environments, leaving them additional opportunities to expand coverage (and therefore revenue) into this large and rapidly growing market of security in IaaS environments.
- Startups in recent years have taken advantage of a historical problem with IDPS: event fatigue. New startups are using IDS engine technology, like Snort/Suricata/Bro IDS, and are feeding this telemetry into advanced analytics and machine learning engines, which has proven effective in reducing event fatigue. This is a disruptor in this market, and Gartner expects this trend to continue.

IDPS Has Evolved

IDPSs have had two primary performance drivers: the handling of network traffic at wire speeds (either in line or in detection mode), and the deep inspection of that traffic based on more than just signatures, rules and policies to detect, prevent, and respond to threats. 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:

- 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 applies IDPS rules by the user, and application and geolocation information where you can permit, deny or monitor access, based on its origin.
- 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.
- Advanced analytics — This feature leverages what has become to be called UEBA in the security industry. For this market, vendors are using analytics to advance the use of IDS to detect threats that have bypassed other security controls.
- Support of 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 coarse-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 mention advanced threat detection as a feature in 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.

IDS Is Still Widely Deployed and Effective

Client reference surveys for this Magic Quadrant align with conclusions from our general client inquiry, where we see 20% of IDPSs deployed as IDS only (and approximately another 30% using IPS, but run their solution mostly in detection mode). It is clear that organizations are still deploying IDS technology purely for monitoring and visibility use cases, and not necessarily for blocking only. This is especially true 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 IT operations team. This is being driven by multiple reasons, but the need to detect intrusions and respond more efficiently to incidents is still a key investment (see "Use a CARTA Strategic Approach to Embrace Digital Business Opportunities in an Era of Advanced Threats").

While going "in-line" with this technology is preferred for some use cases, 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 CARTA highlights, 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. If an IPS is in the mix, IDPSs concurrently have powerful uses in responding to a range of threats.

Some organizations are getting additional life out of older IDPS investments (or by making new investments in IDS) by enabling basic IDPS in the NGFW and moving their existing dedicated IDPS and IDS elsewhere in the environment, where they are tuned for those use cases. 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.

Web Application Vulnerabilities Are Still a Major Problem

Gartner recommends considering a WAF over an IDPS for protecting web applications to reduce the exposure to security threats (see "Magic Quadrant for Web Application Firewalls"). Making use of application security measures to significantly reduce the vulnerabilities during the development life cycle is even more effective (see "Magic Quadrant for Application Security Testing").

For a long time, IDPSs have had content that can address some of the web application security issues that organizations have continued to find, often in large numbers, in their web-based applications. Coverage for the more straightforward web applications issues, like SQL injection and cross-site scripting, exists in the majority of products evaluated for this Magic Quadrant. Without an application security program or a WAF deployed, IDPS can offer some coverage of web-application-focused threats. IDPS also has access to SSL decryption options for multiple types of deployments, including inspecting inbound web traffic. Some leading vendors, like McAfee, are

investing in improving their coverage of web application threats significantly in order to be able to deploy in public cloud. Alert Logic does this differently by using its WAF for blocking, but leveraging its IDS for detection use cases. Generally though, web application content can be "noisy" when enabled on IDPS, and can be more prone to false positives than what a leading WAFs are delivering today.

IDPS Has Potential in the Cloud

Traditional firewall vendors are not making an impact in terms of usage in public cloud environments like Amazon AWS, Microsoft Azure and Google Cloud. This is primarily because the built-in firewall controls are providing native integration, agility, less expensive pricing and, in general, "good enough" capabilities for the types of workloads that run in public clouds. Generally speaking, you don't need advanced enterprise firewall features to protect server workloads in the cloud, and the ruleset is often very basic. WAF and IDPS are more relevant security add-ons for workloads running in these environments. Cloud-delivered WAF is now prevalent and still far exceeds WAF functionality delivered by cloud service providers (CSPs). No CSP today is investing in the type of advanced DPI solutions delivered by cloud-ready IDPS solutions.

Gartner expects this deployment form factor for IDPS to become a leading use case for the technology in the coming years. As the shift continues to move workloads to IaaS, so too will the relevance of advanced detection, prevention and response capabilities to security teams with workloads running in private, hybrid and public clouds. The client reference survey this year reported that approximately 30% of respondents have IDPS deployed either in public and/or hybrid cloud environments.

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 NGFWs, NGFW adoption reduces the need for a dedicated network IDPS in enterprises (especially smaller ones) at the network perimeter. The perimeter placement traditionally is the most popular deployment location for IDPS. However, the stand-alone IDPS market will persist to serve several scenarios:

- The incumbent firewall does not offer a viable next-generation IDPS option for reasons of security efficacy.
- 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 IDPS policy in place) regardless of 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 for security efficacy and cost reasons.
- 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 IDPS capabilities are desired, but don't require a firewall. This can also apply to SDN and public cloud scenarios

where routing/NAT functions are covered in the base platform and only advanced network inspection is required.

- For internal network segmentation projects, IDPS deployments are advantageous as they happen at Layer 2 (transparently with no significant routing/switching requirements), with better reliability/resiliency, lower latency, and general equal or higher-quality security content than a transparent NGFW, and therefore are 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.

Endpoint Context Is Increasingly Important and Available in Leading IDPS

An interesting development over the past few years is how IDPS vendors are increasingly bringing in various levels of details from endpoints. This complements IDPSs on the network significantly. As a simple example, being able to dig into traffic by mapping the specific application 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 built-in options. Other vendors in this Magic Quadrant, like Trend Micro and Fidelis, 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 complementary network option.

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 past 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 hostname 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 include not only the threat (for example, "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 STIX/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 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 semitrusted sources
  - Overload the IDPS with too much TI, which can significantly affect performance

STIX/TAXII standards are now at a point that they have gained adoption momentum of a sizable number of groups generating/consuming threat intelligence, 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. While niche, they serve an important purpose for some clients by aggregating larger numbers of indicators of compromise (IOCs) that are not able to be run on other network appliances like IDPS and firewalls. 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 (see "Emerging Technology Analysis: Threat Intelligence Gateways").

Gartner Recommended Reading

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

"It's Time to Align Your Vulnerability Management Priorities With the Biggest Threats"

"Defining Intrusion Detection and Prevention Systems"

"Next-Generation IPS Technology Disrupts the IPS Market"

"Use a CARTA Strategic Approach to Embrace Digital Business Opportunities in an Era of Advanced Threats"

"Forecast: Information Security, Worldwide, 2015-2021, 3Q17 Update"

"How Markets and Vendors Are Evaluated in Gartner Magic Quadrants"

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 Advances Automated Cyber Threat Intelligence Sharing With STIX, TAXII, CybOX," OASIS.

Details on STIX and TAXII.

"Trend Micro Acquires HP TippingPoint, Establishing Game-Changing Network Defense Solution," Trend Micro.

"Intel Security to Sell McAfee NGFW, Firewall Enterprise Businesses to Raytheon/Websense," CRN.

"IBM and Cisco Collaboration in the Next-Gen Intrusion Prevention Market," IBM Security.

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.

GARTNER HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
USA
+1 203 964 0096

Regional Headquarters
AUSTRALIA
BRAZIL
JAPAN
UNITED KINGDOM

For a complete list of worldwide locations,
visit http://www.gartner.com/technology/about.jsp