Magic Quadrant for Enterprise Network Firewalls

Published: 10 July 2017 **ID:** G00310171

Analyst(s): Adam Hils, Jeremy D'Hoinne, Rajpreet Kaur

Summary

"Next generation" capabilities have been achieved by all products in the enterprise network firewall market, and vendors differentiate on feature strengths. Security and risk management leaders must consider the trade-offs between best-of-breed enterprise network firewall functions and cost.

Strategic Planning Assumptions

Virtualized versions of enterprise network firewalls will reach 10% of market revenue by year-end 2020, up from less than 5% today.

By year-end 2020, 25% of new firewalls sold will include integration with a cloud-based cloud access security broker (CASB), primarily connected through APIs.

By 2020, 50% of new enterprise firewalls deployed will be used for outbound TLS inspection, up from less than 10% today.

Market Definition/Description

This document was revised on 12 July 2017. The document you are viewing is the corrected version. For more information, see the Corrections page on gartner.com.

The enterprise network firewall market represented by this Magic Quadrant is still composed primarily of purpose-built appliances for securing enterprise corporate networks. Products must be able to support single-enterprise firewall deployments and large and/or complex deployments, including branch offices, multitiered demilitarized zones (DMZs), traditional "big firewall" data center placements and, increasingly, the option to include virtual versions for the data center. Customers should also have the option to deploy versions within Amazon Web Services (AWS) and Microsoft Azure public cloud environments, and they should see the ability to support Google Cloud on the vendor roadmap within the next 12 months. These products are accompanied by highly scalable (and granular) management and reporting consoles, and there is a range of offerings to support the network edge, the data center, branch offices, and deployments within virtualized servers and the public cloud. All vendors in this market should support fine-grained application and user control. In effect, all vendors in the enterprise firewall market have what Gartner has called "next-generation firewalls (NGFWs)"; in essence, there is no longer a "next generation" in the firewall market.

The vendors that serve this market are identifiably focused on enterprises, as demonstrated by the proportion of their sales in the enterprise; and as delivered with their support, sales teams and channels. These vendors provide features dedicated to solve enterprise requirements and serve enterprise use cases.

What Has Changed

All enterprise firewall vendors offer NGFW features to better enforce policy (application and user control) or detect new threats (intrusion prevention systems [IPSs], sandboxing and threat intelligence feeds). Enterprise firewall is now synonymous with NGFW. Enterprise firewalls continue to gradually replace stand-alone network IPS appliances at the enterprise edge. Although this is happening now, some enterprises will continue to choose to have best-of-breed next-generation IPSs (NGIPSs). Many enterprises are looking to firewall vendors to provide cloud-based malware-detection instances to aid them in their advanced threat detection efforts, as a cost-effective alternative to stand-alone sandboxing solutions (see "Network Sandboxing for Malware Detection").

However, enterprise firewalls will not subsume all network security functions. All-in-one or unified threat management (UTM) approaches are suitable for small or midsize businesses (SMBs), but not for the remainder of the enterprise market (see "Next-Generation Firewalls and Unified Threat Management Are Distinct Products and Markets").

The needs for enterprise branch-office firewalls have become specialized, and they have diverged from UTM products. As part of increasing the effectiveness and efficiency of firewalls, branch-office firewalls need to truly integrate a more granular blocking capability as part of the base product, go beyond port/protocol identification and move toward an integrated service view of traffic, rather than merely performing "sheet metal integration" of point products. In short, they need to offer the same levels of security efficacy as the primary gateway does. Having a subpar configuration and protection capability for branches is not acceptable today.

In addition, firewalls are becoming important vehicles for TLS termination. The primary use case is to inspect outbound traffic for threats, such as downloading of malicious binaries and botnet command and control. TLS capabilities also allow them to act as a lightweight data loss prevention (DLP) tool as they decrypt and inspect outbound traffic to ensure that sensitive data is not wrongly sent out. However, customers that enable this capability are still frustrated by the substantial performance burden that in-firewall TLS decryption imposes.

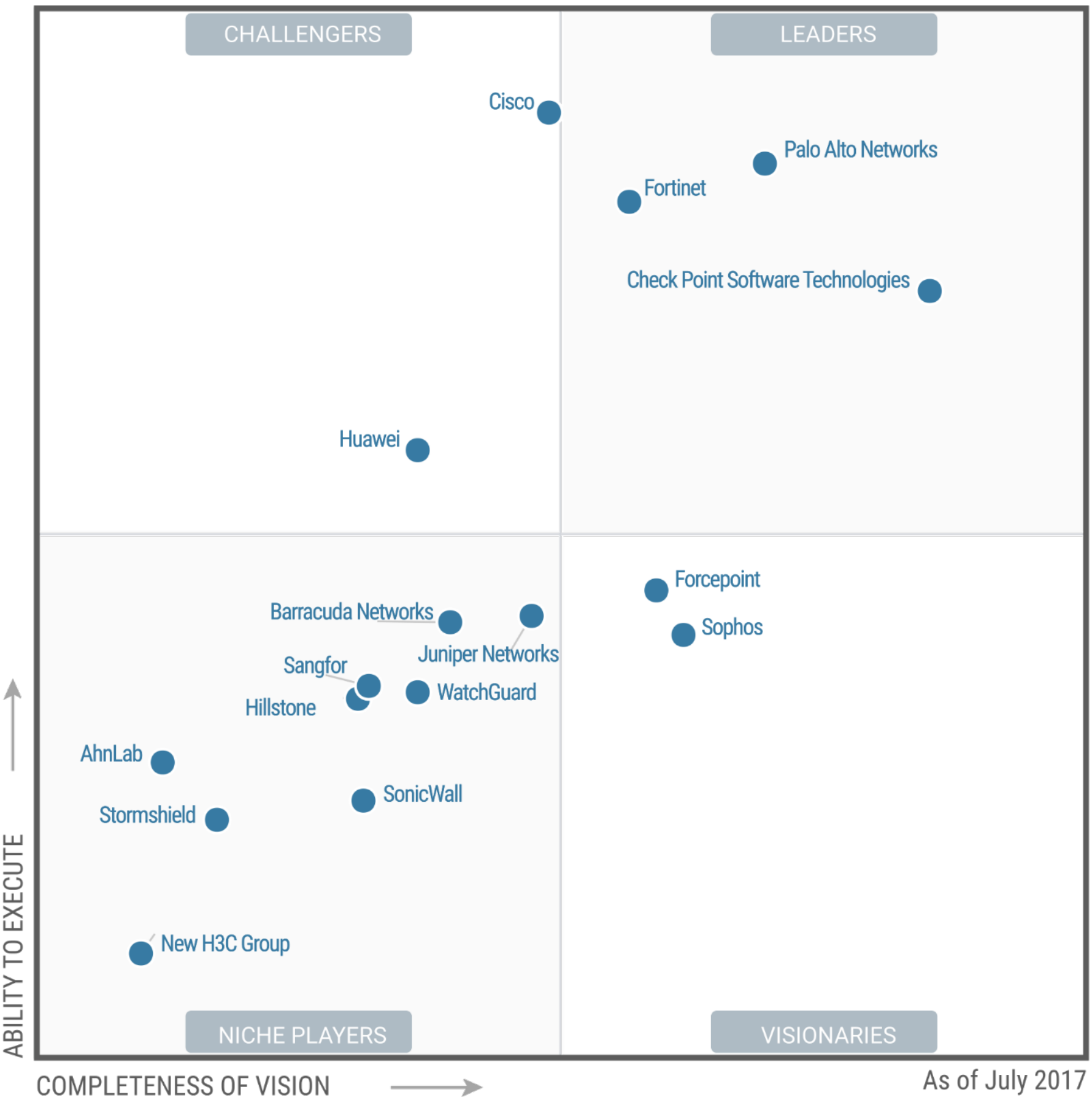
Leading-edge customers are planning, and sometimes implementing, principles of software-defined networking (SDN) and east-west microsegmentation. These customers seek vendors with some SDN support and forward-looking SDN roadmaps. Key to these roadmaps will be more automated firewall policy orchestration that will enable organizations to realize the agility and business benefits that SDN promises.

As more organizations are moving strategic workloads to the public cloud, an increasing number of them wish to protect those workloads with their incumbent enterprise firewall vendor. Today, vendor offerings to AWS and Microsoft Azure are uneven. Some don't offer the

same level of inspection that on-premises firewalls do, and they all lack sufficient policy automation. Enterprise firewall vendors must improve in these areas to remain relevant in the hybrid cloud era.

Magic Quadrant

Figure 1. Magic Quadrant for Enterprise Network Firewalls



Source: Gartner (July 2017)

Vendor Strengths and Cautions

AhnLab

Headquartered in South Korea, AhnLab enjoys sizable in-country market share, especially in the government and financial verticals, but has only a limited presence in other East Asian nations. It has sold firewalls since 2007 under the TrusGuard product line. It offers 12 UTM and firewall models for SMBs and enterprises, four of which were introduced in 2016. The firewall is Common Criteria-certified EAL4 and TTA IPv6-verified, which is a South Korean certification, but does not have other third-party evaluations (such as ICSA Labs, NSS Labs or FIPS PUB 140-2).

The AhnLab product portfolio includes firewalls, advanced threat defense, distributed denial of service (DDoS) attack mitigation, threat intelligence and endpoint security solutions. It also offers managed security services and forensic and incident response services.

AhnLab is not at parity with global or most regional competitors in advanced features. Its firewalls lack some important features (SDN support, multiple virtual firewall model support and public cloud deployment support) that are provided in most other vendors' firewalls and are significant for enterprise customers. Outside of South Korea, AhnLab has a limited regional presence.

AhnLab is a good shortlist candidate for South Korean enterprises, especially those using or considering its endpoint solutions.

STRENGTHS

Sales Execution: AhnLab is an established endpoint and network security player in South Korea, with a significant local sales and support presence. AhnLab is one of a few East Asian vendors with a local certification, which is significant in South Korea.

Capabilities: AhnLab includes URL filtering and file reputation checks for free with its TrusGuard firewalls. This is powered by the vendor's proprietary cloud-maintained malicious URL database and reputation files, which number well over a billion.

Product Offering: AhnLab's network security solutions provide existing endpoint security customers with a single vendor option to maintain the existing vendor relationship and to reduce multivendor management challenges.

CAUTIONS

Product Offering: AhnLab still does not offer a virtual firewall, and therefore has no offering for SDN frameworks or for infrastructure as a service (IaaS) platforms such as AWS, Microsoft Azure or local public clouds. Virtual firewalls and public cloud/SDN support are offered by almost all competitors, including most regional ones.

Geographic Strategy: TrusGuard firewalls are not present on Gartner client shortlists outside South Korea. AhnLab was not listed by any vendor we surveyed as a significant enterprise competitive threat.

Product Strategy: The Malware Defense System (MDS) is offered only as an appliance. The lack of a cloud version makes deploying and supporting MDS more difficult and expensive for customers than it is with leading competitors.

Barracuda Networks

Barracuda Networks is headquartered in Campbell, California. It has a broad product portfolio including security, data archiving, backup and load balancing controls. It has a legacy of selling products to the SMB market with an easy-to-use interface and affordable pricing. In 2016, it released the CudaLaunch App for macOS, Windows, iOS and Android, providing HTTPS-based access to the network and zero configuration rollout of transparent VPN to end users. During the evaluation period for this Magic Quadrant, the vendor also released Zero Touch Deployment service for the F-Series firewalls to eliminate deployment complexity. In addition, the vendor released separate hardware appliance models SC1/F15/F82/F18 3/F800 Revision C Series/F900 Revision B Series and multiple virtual appliance models.

Gartner sees Barracuda Networks mostly in public clouds and distributed office use cases. The vendor has a limited global presence concentrated in Western and Central Europe and North America. It lacks a strong global channel presence and innovation for large enterprises outside the distributed enterprise use case.

Barracuda should be considered by enterprises that have a cloud infrastructure and want to secure it. It is also a good candidate for distributed enterprises that want site-to-site VPN connectivity through multiple tunnels. Enterprises should check local value-added reseller (VAR) availability and direct services in the region before adopting it.

STRENGTHS

Technical Support: Barracuda technical support is always rated high and mentioned as a key strength by end users and VARs. Surveyed end users cite the ease of contacting Barracuda technical support to get their issues resolved in a friendly and thorough manner.

Offering: Barracuda has a strong presence in the public cloud, with support for all the major public cloud platforms such as Microsoft Azure, AWS and VMware vCloud Air. In 2016, it extended this support to Google Cloud Platform.

Features: Barracuda offers strong VPN connectivity with enhanced monitoring and deployment features. As a result, Gartner has observed that its main presence is in distributed enterprise use cases with multiple site-to-site VPN tunnels. With the release of the CudaLaunch app in 2016, it has extended its managed VPN feature to iOS and Android mobile devices. Barracuda also offers a VPN client for Windows, which provides centrally managed network access along with a host-based firewall.

Technology Partner Ecosystem: Barracuda has multiple OEM partnerships, such as IBM ISS for its URL filtering database and Trend Micro for IPS signatures. In 2016, it also acquired the Sookasa CASB solution. Barracuda also has partnerships with major public cloud platforms including Microsoft Azure, AWS, VMware vCloud Air and Google Cloud Platform, and virtualization platform providers including Microsoft Hyper-V, VMware NSX, KVM, Citrix XenServer and Open Xen. These partnerships have enabled Barracuda to offer better features and services to its clients.

Product Execution: Barracuda offers quality of service (QoS) policy selection at the rule level. It also offers the capability to dynamically change QoS for live open sessions, such as to prioritize Office 365 and Salesforce. This provides easy allocation of QoS features to its traffic dynamically.

CAUTIONS

Sales Execution: Gartner has observed Barracuda's NextGen Firewalls typically being adopted for public cloud and distributed branch-office enterprise use cases. It is less visible in large data centers and large enterprise use cases.

Marketing Execution: Surveyed customers have cited that the vendor does not communicate its roadmap and future enhancements clearly to end users; hence, they are not aware of the vendor's product vision.

Channel Execution: Surveyed VARs have reported that Barracuda does not provide sufficient notice before announcing a product's end of life (EOL). This creates problems with the VARs that have sold those EOL products to end users.

Technical Architecture: Despite Barracuda selling multiple products such as Web Application Firewall, Web Security Gateway and Email Security Gateway, along with firewalls, it still lacks a centralized management platform to monitor and operate all the products from a single console. This does not give an ease of management advantage to those Barracuda clients that use multiple Barracuda product lines, other than to maintain a single vendor relationship.

Certification: Barracuda firewalls lack Common Criteria EAL4 certification, while the majority of firewall vendors have attained such certification. Gartner has observed many enterprises in Asia mentioning EAL4 certification as a selection criterion.

Check Point Software Technologies

Check Point Software Technologies is a leading network firewall vendor. Co-headquartered in Tel Aviv, Israel and San Carlos, California, Check Point is a large pure-play security vendor, with more than 1,300 employees in R&D. The vendor is providing a variety of solutions, including next-generation security gateway appliances and endpoint, cloud and mobile security solutions. Enterprise firewalls include the 5000, 15000, 23000, 44000 and 64000 series of appliances. Cloud security is provided through vSEC for private and public cloud, as well SandBlast Cloud for SaaS applications. Endpoint security products include SandBlast Agent and mobile security products include Check Point Capsule and SandBlast Mobile. Also released was SandBlast Cloud to scan Microsoft Office 365 email traffic. In 2016, Check Point made available a number of models, including 15400 and 15600 for large enterprises, and 23500 and 23800 for data centers.

Recent news include the introduction of new 44000 and 64000 high-end platforms, the release of vSEC for the Google Cloud platform, and the availability of R80.10 with improvements to the management console, performance and SandBlast Anti-Ransomware, providing protection against ransomware. Check Point recently introduced Check Point Infinity security architecture, a consolidated security across networks, cloud and mobile.

The vendor has also recently expanded its cloud security offering with a cloud-based malware detection service that can be integrated in front of SaaS email offerings. Check Point offers numerous subscriptions (e.g., Software Blade) to augment its firewall gateway, including advanced malware protection (Threat Emulation and Threat Extraction) and multiple threat

intelligence feeds (ThreatCloud IntelliStore and Anti-Bot). Check Point offers its firewall over AWS and Microsoft Azure for public cloud support, and integrates with VMware NSX and Cisco Application Centric Infrastructure (ACI) for SDN use cases.

Check Point continues as a Leader in the enterprise firewall space. Its firewall product meets all the enterprise deployment use cases with the breadth of models and features. It continues to lead in multiple features such as simplified centralized management and granular role-based administration.

Check Point is one of the largest security vendors, and continues to lead in market share for firewall equipment. In 2016, along with the R80 release, the SandBlast Agent was made available, both for endpoint and browser protection.

Check Point's firewalls should be shortlisted by enterprises for which price sensitivity is not as important as granular security features such as high-quality central management for complex networks. It is a good candidate for enterprises running hybrid networks with a mix of on-premises, virtual data centers and cloud.

STRENGTHS

Offerings: Check Point offers a large breadth of security products covering network, mobile and endpoint. It also offers a mobile security solution, which consists of a software container called Capsule (Workspace, Docs and Cloud) for both iOS and Android, Mobile Threat Prevention, and Capsule Connect/VPN. This makes the vendor a shortlist candidate for enterprises looking for an integrated and consolidated approach to their perimeter, endpoint and mobile security based on the maturity on their enterprise security.

Product Execution: Check Point offers a large number of firewall models to meet the requirements of all enterprise network types. Enterprise firewalls include the 12000, 13000, 15000, 21000, 23000, 41000 and 61000 series of appliances. In 2016, the vendor extended the integration capabilities for its vSEC virtual appliance line for VMware, Cisco ACI, KVM, Hyper-V, OpenStack, AWS, Google Cloud and Azure to support public cloud and highly virtualized infrastructure. This makes it a strong enterprise firewall vendor capable of meeting different enterprise deployment use cases.

Partners: Check Point has built a strong ecosystem of technology partners including software, server, and networking and managed services. Gartner strongly believes that security vendors should be able to identify and build product support and integration capabilities with the right technology providers to enhance their product offerings. Check Point also has a strong and well-established channel globally, through its partner program.

Features: Check Point's enterprise firewalls offer strong web filtering capabilities with a combination of application control, URL filtering and DLP. It offers mature URL filtering capabilities with multiple end-user block and information pages. It allows end users to explain their reason to bypass policy. It also offers a user check feature to alert users in real time about their application access limitations, while educating them on internet risk and corporate usage policies. Both application control and URL filtering operations can be performed within the same rule. This makes these firewalls a desirable candidate for enterprises that are considering consolidating their web proxy and require granular web

filtering capabilities in their firewall. Clients frequently comment that the Check Point roadmap aligns very well to their enterprise needs of tomorrow, imbuing strong client retention, especially in high-compliance environments.

Central Management: Check Point continues to lead the market with its strong, robust centralized management offering, which makes it a desirable vendor for complex firewall policy environments, such as deployments by very large enterprises and organizations that need formal approval workflow, have complex topologies, are subject to compliance that requires reliable reporting or have large operations teams. Even the surveyed VARs and customers have rated this to be the vendor's strongest feature, and competitors acknowledge Check Point's leadership in this domain.

CAUTIONS

Delivery: Existing Check Point clients have often reported that their major firmware releases require jumbo hot fixes and take considerable time to become stable. Surveyed Check Point clients have also highlighted this and stated that the vendor needs to improve its delivery capabilities on new releases for a smoother customer experience.

Features: Although Check Point has partnered with multiple CASB solution providers, including FireLayers, Avanan and Microsoft (Adallom), it still lacks a built-in CASB feature for granular control and monitoring of growing SaaS applications. Gartner has gradually observed more enterprises considering CASB as a firewall-attached cloud service.

Marketing Execution: Check Point lacks proper marketing execution, which leads to confusion in its messaging in the market, or a notable absence especially when releasing interesting new features. Gartner clients often consider Check Point as a "traditional" firewall vendor, despite innovating in the threat detection and mobile security spaces. Surveyed VARs have also scored the vendor lower on marketing and stated that it requires better product marketing to compete with its competitors.

Technical Support: Gartner still receives anecdotal feedback from existing Check Point clients that it lacks prompt support, especially if the issue is escalated to a higher level of support and is not communicated well to clients. Even the surveyed VARs have reported that the vendor lacks prompt technical support for higher-level support issues. Check Point is working toward opening more technical assistance centers (TACs) across the globe for direct availability in different regions.

Sales Execution/Pricing: Check Point's firewalls are perceived as high-priced solutions, and some customers have expressed surprise at perceived higher-than-expected renewal costs; however, as a feature leader, clients that need best-in-class security get what they pay for.

Cisco

Cisco, based in San Jose, California, is the largest networking infrastructure vendor with a broad security portfolio. Its main product line that includes all new releases is Cisco Firepower NGFW, which exists alongside the older Adaptive Security Appliance (ASA) product line and the Meraki range for smaller organizations. In addition, Cisco has two virtual firewalls — the ASAv and NGFWv. For Cisco deployments with a mix of newer and older firewalls, Firepower

Management Center (FMC) and Cisco Security Manager (CSM) are available. Some in-service ASA appliances do not support FMC for complete management, so some clients should expect to have to maintain CSM as part of one firewall replacement life cycle. In addition, Cisco Defense Orchestrator (CDO) enables cloud-based, low-touch management visibility and orchestration across distributed environments. Cisco offers a range of services on its firewall line, including NGIPS, URL filtering, cloud-based sandboxing and the Advanced Malware Protection (AMP) network. In addition, Cisco has a broad portfolio of additional products that includes advanced endpoint security, network traffic analysis (Stealthwatch), secure web gateway, email security, network access control and CASB.

Cisco's recent enterprise firewall news includes the release of its 2100 series, which claims to process traffic more efficiently, and the release of Firepower Device Manager (FDM), a web-based, on-box device manager for Cisco Firepower NGFWs and replacement for Adaptive Security Device Manager (ASDM) in managing ASA 5500-X series devices. Cisco also completed the acquisition of Cloudlock, its CASB product.

Cisco is executing well in sales and meeting its roadmap execution goals, but Gartner does not often see Cisco enterprise firewalls selected on the basis of features or vision.

Cisco is a good shortlist candidate for most enterprise use cases, particularly when enterprises want to deploy a broad set of security services that interact with the firewall.

STRENGTHS

Sales Execution: Gartner sees Cisco firewalls on an increasing number of shortlists, and sees continued momentum for the Cisco Security Enterprise License Agreement (ELA), which is good for organizations that want a single vendor multiproduct solution that provides for staged deployment and product flexibility. Under the terms of the Cisco Security ELA, customers can move resources around and even add security services as their needs change and grow.

Advanced Threat Protection: Surveyed customers and partners value the integration between AMP for Networks and AMP for Endpoints, a level of integration that some competitors lack. Gartner sees AMP for Endpoints included in more new deals than it sees endpoint advanced threat detection attached for competitors.

Customer Experience: Gartner clients consistently rate the Cisco support network as excellent, and it is an oft-cited reason for loyalty to Cisco security products. The vendor has strong channels, broad geographic support and wide availability of other security products.

Capabilities: Cisco stakeholders like Cisco Defense Orchestrator, which is a simplified approach to policy management across NGFW, ASA and Umbrella. Distributed enterprises use it to gain policy visibility and control across enterprise and mobile/cloud edge security safeguards.

Portfolio: Gartner clients and surveyed Cisco partners value the integration of the Firepower NGFW enterprise firewall with existing and emerging elements of Cisco's enterprise security portfolio.

CAUTIONS

Management: Gartner clients and surveyed customers dislike having to continue to use CSM to manage some models and FMC to manage others, citing increased complexity of central management.

Product Execution: Cisco customers and partners complain about configuration and management difficulties caused by the Java ASDM on-device management graphical user interface (GUI) that persists on in-support ASA models.

Product Strategy: For the evaluation period, Cisco firewalls did not yet integrate with VMware NSX, so Cisco could not participate in NSX-led SDN projects. This was a competitive disadvantage, and caused some Cisco firewall customers to switch to other vendors. A signed agreement between Cisco and VMware is now in place.

Customer Experience: Surveyed customers and partners cite complex and confusing licensing as a significant negative when they attempt to deploy, alter or renew their Cisco firewall and associated portfolio licenses.

Sales Execution: In the survey sent to enterprise firewall vendors, Cisco's product was the most frequently listed as the one that vendors claimed to replace the most. Cisco's current messaging around its network security platform confuses Gartner clients that see instead a list of many products.

Forcepoint

Based in Austin, Texas, Forcepoint (formerly Raytheon|Websense) is a pure-play security vendor. It offers a firewall (Forcepoint NGFW), launched in 2001, web and email security gateways (Forcepoint Web Security and Forcepoint Email Security), a data loss prevention offering (Forcepoint DLP), an insider threat solution (Forcepoint Insider Threat) and a cloud access security broker offering (Forcepoint CASB, recently acquired from Imperva). The vendor has more than 2,000 employees. The Forcepoint NGFW product line was acquired from Intel Security in January 2016, along with the McAfee Firewall Enterprise (Sidewinder was part of the Secure Computing acquisition by McAfee in 2008).

Forcepoint recent news includes the availability of the NGFW offering on AWS, the addition of the Sidewinder proxies on the Forcepoint NGFW and the possibility of tunneling web traffic to the Forcepoint cloud-based secure web gateway (Forcepoint Web Security Cloud).

Forcepoint has demonstrated consistently good feature quality and an expanded capacity to execute on its roadmap. The vendor is a valid shortlist candidate on enterprise firewall shortlists for distributed organizations.

STRENGTHS

Product Vision: Forcepoint offers multiple solutions that have the ability to augment firewall capabilities. The vendor has started with the integration of the ThreatSeeker threat intelligence feed, and the ability to tunnel web traffic to the Forcepoint Web Security Cloud solution.

Customer Experience: Customers give excellent scores to the centralized management console (Forcepoint Management Center [SMC]) and high availability. Forcepoint scores comparatively high for the quality of its hardware.

Capabilities: Independent tests grant Forcepoint NGFW better results for attack detection than some of the Leaders evaluated in this research. The vendor has an historical focus on building detection engines resistant to evasion techniques.

Ease of Use: A zero-touch deployment is available for Forcepoint NGFW. The filtering policy commit process integrates an optional approval workflow. SMC includes easy-to-use filters and visualizations to ease the analysis of incidents.

Geographic Strategy: Forcepoint is visible on distributed organizations' shortlists in Europe, especially for local government agencies. Two of its three R&D centers for firewall development are located there.

CAUTIONS

Geographic Strategy: Forcepoint NGFW continues to have much lower visibility among enterprise firewall buyers in North America and the Asia/Pacific region than in Europe. Its channel is relatively small compared to many of its competitors.

Market Responsiveness: Forcepoint has just released cloud-based sandboxing, six years after the first vendor evaluated in this market. It has only recently added Geo-IP and IP reputation in the filtering policy. Integration of Sidewinder proxies into the NGFW is also very recent.

Market Segmentation: Forcepoint offers a smaller number of firewall appliances than its leading competitor. It lacks the entry-level devices that suit the needs of the smallest branches. Embedded web management for one device is not feature-complete, forcing clients with a single location to learn the more comprehensive SMC.

Capabilities: Forcepoint's firewall offering does not yet fully integrate with the recently acquired Forcepoint CASB.

Product: Forcepoint NGFW's high availability is less appealing for SDN and IaaS use cases, where part of the resiliency requirements are handled by the infrastructure. Forcepoint NGFW is not yet available on Microsoft Azure. Forcepoint lags behind the competition on integration with AWS services and SDN vendors.

Fortinet

Fortinet is a large network and security vendor, with more than 4,600 employees, based in Sunnyvale, California. Its main product line is the FortiGate firewall, which represented roughly 75% of its total revenue in 2016. The vendor offers other products, such as a wireless LAN (FortiAP) and web application firewall (FortiWeb). Its more recent marketing message highlights the Security Fabric concept, focused on cross-device integration to improve overall visibility and provide additional control options.

Fortinet recent news includes more models of its E Series, which benefits from the latest generation of Fortinet Security Processors (SPU). Fortinet also acquired AccelOps and rebranded it FortiSIEM. Latest releases include several features related to the Security Fabric, with traffic forwarding between Fortinet appliances, unified visibility and tighter integration with FortiClient endpoints. Fortinet also recently announced availability of FortiCASB, its firewall-attached offering for SaaS security.

Fortinet has introduced important new product functionalities and has made product and marketing strategy improvements. The vendor is a good shortlist candidate for all enterprise firewall appliance use cases, especially when price/performance is rated high in the evaluation.

STRENGTHS

Marketing Execution: Fortinet has improved its visibility in final two vendor shortlists for enterprise firewalls, being frequently the finalist against one of the other two leaders. Surveyed channel partners acclaim Fortinet's assistance during RFP and implementation.

Sales Strategy: Fortinet excels in providing the best price/performance offers, relying on the combined use of an extensive appliance portfolio, good total cost of ownership for bundles and a flexible discount strategy. The vendor grows much faster than the market average.

Customer Experience: Fortinet's clients gives excellent scores to its firewall performance and hardware quality.

Capabilities: Customers not using centralized management tools liked the improved visibility they get from the FortiView reports. Fortinet customers also mentioned ease of deployment as a strong point.

Market Segmentation: Fortinet's latest chassis models (7000 Series) reinforce its ability to serve the performance required in large data centers.

CAUTIONS

Product Strategy: Fortinet focuses most of its development resources on integrating its existing solutions together (Security Fabric), at the expense of other areas. The vendor's investment lags behind the competition in IaaS/SaaS and advanced threat endpoint security. Its attach rate for cloud-based sandboxing is low, and the feature has received few improvements since its first release.

Marketing Execution: Fortinet fails to move its brand out of the "good enough vendor" zone. Several of its resellers also offer products from one of the other Leaders in this Magic Quadrant and select Fortinet for its primary "fast firewall" use case. Despite a good security score in independent testing, some prospective customers with high-risk exposure still express doubts regarding Fortinet's ability to meet their security requirements.

Capabilities: Except for performance, Fortinet often comes in second in technical evaluations to one of its direct competitors when core features (IPS, VPN, management, application control, sandboxing) are heavily weighted.

Customer Experience: Fortinet does not offer the direct vendor support and premium subscriptions that large enterprise clients might require. Client feedback on support is directly impacted by the quality of the channel partner: It gets an average score. Customers also report that firmware upgrades and new features might be unequal in quality.

Management: Centralized and cloud-based management have made insufficient progress to positively influence Fortinet's score during technical evaluation.

Hillstone

Hillstone is headquartered in Beijing, China, with regional headquarters in Sunnyvale, California. The vendor is an established network security player offering perimeter, cloud and server security solutions. In 2016, it introduced a few major features such as cloud sandboxing, URL filtering for HTTPS traffic, and TLS/SSL offloading and enhancement of its existing features.

Hillstone is one of the few Chinese network security vendors that is gradually expanding in other regions outside China, such as South East Asia, the Middle East and Africa, and Latin America. It continues to focus on expanding in different regions along with the Chinese market.

Hillstone firewalls are a good candidate for enterprises with hybrid networks, such as on-premises, cloud and virtualized environments in the abovementioned regions.

STRENGTHS

Product Strategy: Hillstone product offerings and feature enhancements meet all the enterprise use cases more focused toward carrier and cloud infrastructure networks with virtualized environments. The vendor introduced SSL offloading and cloud-based network sandboxing features in 2016 to support typical enterprise network perimeter use cases. Feature enhancements such as link load balancing and granular QoS are more useful for carrier use cases, and offerings such as CloudHive and CloudEdge (with support for multivendor public clouds) are best for cloud infrastructure and hybrid enterprise network use cases. This makes Hillstone a desirable shortlist candidate for enterprises with hybrid networks, as they can have a single vendor relationship.

Features: Hillstone has enhanced its link load balancing feature to make it more intelligent and granular. It can perform functions like link aggregation, ECMP, ISP routing, DNS domain redirection, intelligent DNS, etc., for dynamic link selection. Surveyed VARs have reported this as one of the strongest product features. The vendor offers a granular, schedule-based QoS feature with controls that can be applied to IP, users, protocols, zones, interfaces and VLAN. This offers enterprises the ability to implement tight QoS controls over their traffic. Surveyed partners have rated Hillstone's abnormal behavior detection network traffic analysis feature as one of the product's strengths.

Public Clouds: Hillstone's virtual CloudEdge firewalls support all the major regional local cloud platforms in China, including carrier cloud (China Unicom, China Telecom and China Mobile), Jindong Cloud, Huawei Cloud, AliCloud and other global public clouds like AWS and Azure. This makes it a good shortlist candidate for organizations with hybrid networks.

Segmentation: Hillstone CloudHive offers a microsegmentation solution for virtual VMware networks along with CloudEdge virtual firewalls for the networks over the cloud. This offering makes Hillstone a strong vendor for cloud security use cases.

CAUTIONS

Marketing Execution: Surveyed partners have indicated that Hillstone lacks marketing and brand recognition outside China. Gartner believes the vendor needs to focus more on strong marketing to build a strong brand in the regions it wants to expand in, where there are multiple strong firewall vendors with strong marketing.

Features: Hillstone lacks any integration with CASBs and does not offer advanced SaaS monitoring and control functionality. It does not offer any specific reports for SaaS applications, whereas with the increase in adoption of SaaS applications, enterprises are gradually more often looking for a vendor that offers such a feature.

Product Strategy: Hillstone does not offer anti-spam for emails and SD-WAN capabilities, which is offered by most international vendors against which Hillstone competes in the international market.

Product Execution: Hillstone only offers cloud-based network sandboxing and does not offer it as a separate appliance. Gartner has observed many enterprises with large data centers that want to build a private cloud for scanning their traffic against advanced malware seek an on-premises network sandboxing appliance, as opposed to a cloud service, This will lead such enterprises to select a different vendor, as Hillstone does not offer this.

Huawei

Shenzhen, China-based Huawei has been shipping firewall products for more than a decade, and offers a variety of other network security appliances, including anti-DDoS and IPS. The range of firewall appliances and models is extensive, especially for higher-throughput options, and for customers that already have Huawei products and wish to expand their business to firewalls. Unified Security Gateway (USG) is the primary enterprise line, and Eudemon is the model line for carriers and service providers. eSight and Agile Controller are the central management platforms that support the USG line. Huawei USG firewalls have been certified by ICSA, at the Evaluation Assurance Level (EAL) 4+ under Common Criteria and by NSS Labs. Firewall and related security services can be used via the USG6000V virtual gateway to implement virtual multitenant separation.

Huawei released four new models during the Magic Quadrant evaluation period. Recent features include Cloud Application Security Awareness (CASA) and TLS/SSL decryption enhancements.

Huawei has executed a fast ramp-up in market presence, particularly in EMEA; however, we still do not see it frequently displacing Leaders or other Challengers based on vision or features.

Huawei is a relevant shortlist candidate for value-conscious enterprises located in the Asia/Pacific region or EMEA, especially enterprises with high-performance needs.

STRENGTHS

Marketing and Sales Execution: Huawei's firewall sales greatly outgrew the overall enterprise firewall market during the evaluation period, demonstrating new perceived value.

Geographic Strategy: Huawei has developed a strong channel in EMEA, and has worked hard to meet regulatory and customer requirements there. Thus, the vendor has seen significant growth in the region, which accounts for a significant portion of its firewall revenue.

Product Execution: Huawei released several important new features during the evaluation period, including cloud-based advanced threat detection, support for AWS and Xen public clouds, and SDN capabilities. While these features did not lead the market, they helped Huawei gain feature parity or near parity with some competitors.

Portfolio Strategy: Customers with networks based primarily on Huawei infrastructure products can include Huawei firewalls on their shortlists. Huawei customers like that firewalls are well-integrated with their infrastructure components.

CAUTIONS

Product Strategy: Although Huawei has broadened its support in public and private cloud, it does not release new capabilities as fast as its leading competitors. Gartner clients that want first-to-market security capabilities do not often consider Huawei USG as a shortlist candidate.

Product Execution: Huawei still does not offer a virtual firewall compatible with Microsoft Azure, which is a requirement for a growing number of customers in EMEA, one of Huawei's targeted growth regions. Huawei users comment that they would like enhanced reporting and a better GUI.

Marketing Execution: Huawei has limited competitive visibility outside the Asia/Pacific region and EMEA. The vendor has taken considerable steps to address concerns about relying on technology developed in China; however, this concern continues to be a security sales challenge in some markets, especially North America.

Juniper Networks

Based in Sunnyvale, California, Juniper is a sizable networking infrastructure vendor with a long history of providing network security capabilities. Its physical enterprise firewall line, the SRX Series, comprises 11 models. Juniper has two virtual firewalls — vSRX and cSRX. The cSRX is a firewall that can protect containerized environments. Its Junos Space Security Director is the central management platform. Juniper offers AppSecure for application control and visibility, integrated IPS, integrated threat intelligence feeds, and a new cloud-based anti-malware service (Sky Advanced Threat Protection [ATP]). In addition, Juniper has an initiative called Software-Defined Secure Networks (SDSN), which aims to integrate security into all elements of the network infrastructure, whether it is Juniper or another vendor, in order to minimize the impact of any compromised device.

Juniper's recent enterprise firewall news includes an expansion of its SDSN partner infrastructure to build out SDSN with CASB, access and endpoint security solutions. Juniper also recently introduced the SRX 4100 and 4200, two midrange enterprise firewalls. And finally, Juniper just announced that its SDSN Policy Enforcer can now detect threats and enforce policy to non-Juniper switches. Juniper serves incumbent Juniper infrastructure customers well with a product with good security features, but it has had difficulty executing in sales, and Gartner sees it being displaced more often than it is selected in competitive situations.

Juniper is a good shortlist candidate for enterprises that desire high throughput at a low price and the ability for the firewall to support advanced routing scenarios. It is also suitable for enterprises buying security and networking in the same buying center.

STRENGTHS

Product Execution: Surveyed customers and partners often note satisfaction with the SRX's ease of configuration and rich interface, often citing these as primary reasons for selection and continued usage. Juniper has a strong range of branch-office firewalls complementing its enterprise products. These branch-office firewalls include WAN and cellular backup technologies.

Product Strategy: Juniper has a strong SDN security story around vSRX, cSRX and the Juniper Contrail SDN framework, supporting it with its developing SDSN schema. The vendor is unique among its competitors in offering a container-focused firewall.

Product Performance: Good options exist for high-throughput, purpose-built appliances, especially in the higher-end SRX models, because Gartner sees Juniper often deployed in large data centers. The vSRX offering is highly rated for performance relative to other virtual firewalls, and is cited for strong clustering and advanced routing capabilities.

Marketing Execution: During this Magic Quadrant evaluation period, Gartner began to see awareness of Sky ATP and other advanced security functions and roadmap items among the Juniper ecosystem. Continued emphasis on these items will encourage more existing customers to stick with Juniper and, if this marketing execution is consistent and sustained, could inspire potential prospects to evaluate the SRX line.

CAUTIONS

Innovation: Gartner clients and surveyed customers and partners perceive that Juniper lags behind its major competitors in releasing new security features; however, the new roadmap direction for Juniper security solutions is very encouraging to Gartner.

Product Execution: Juniper has been late to market compared to competitors in areas such as public cloud support and VMware NSX integration, although Azure and VMware NSX integration were announced during the evaluation period. As a result, Gartner clients lack confidence in Juniper's security strategy.

Product Strategy: Gartner believes that most enterprises want an operating system in their security products that differs from the one in network infrastructure components.

Sales Execution: Juniper has continued losing security market share in the past year, and has experienced declining year-over-year revenue in a growing market. The vendor must more effectively address fundamental sales challenges, and demonstrate that it can win back customers and market share with its newer capabilities.

New H3C Group

New H3C Group was established in November 2003 and is headquartered in Hangzhou, China. Until 2016, it operated as a subsidiary of Hewlett Packard Enterprise (HPE) and now is a part of UniGroup. It is a strong infrastructure vendor in China with a large portfolio, including security products that also cover firewalls, cloud computing products, switches, routers, WLAN products and management products.

While New H3C Group is focusing more on introducing new product offerings for different growing markets, it lacks the market understanding and strong product strategy for meeting all enterprise firewall use cases and lacks multiple built-in security features, such as network sandboxing, SD-WAN capabilities and SaaS application monitoring, which the majority of competitors in the region offer. The vendor is a regional Chinese player, with a presence only in China.

The vendor's firewalls should be considered by clients based in China that are already using its products and looking for a high-performance, strong firewall with basic security features.

STRENGTHS

Portfolio: New H3C Group has a large portfolio of products and offerings. It offers a range of solutions for data centers, cloud infrastructure and big data. Product offerings include servers, storage products, security products, networking and software. This gives an advantage to end users that want to maintain a single vendor relationship for their broad range of infrastructure products.

Security Architecture: The vendor offers H3C SecCenter Management Center for centrally managing the security devices on a network. It includes the function modules IPS Manager, UTM Manager, Firewall Manager and intelligent Traffic Analysis System (iTAS). This gives an advantage to existing customers, providing centralized management of a variety of devices.

Offering: New H3C Group also offers H3C SecBlade FW modules, which can be used on H3C switches (S5800, S7500E, S9500E or S12500) and routers (SR6600 and SR8800). These FW modules help customers extend network security capabilities within their existing H3C switches and routers.

Customer Experience: Surveyed clients have highly rated the Intelligent Flow Forwarding (IFF) and Security One Platform (SOP) features of the M9000 Series Multi Service Security Gateways. As per the vendor, the IFF feature is designed to implement distributed traffic flow and the SOP feature offers a virtual firewall function using container-based virtualization technology. Clients have reported these features to be effective in a highly virtualized live environment, along with support for SDN.

Capabilities: Since New H3C Group is a large infrastructure vendor, it has invested a large amount to develop a high-end testing center and lab with enhanced testing capabilities. This shows commitment from the vendor to deliver reliable products and services to the market.

CAUTIONS

Marketing Execution: The vendor's firewalls lacks recognition and brand value in its local market. Surveyed VARs have also reported that the vendor lacks brand recognition and needs better product marketing compared to other local Chinese vendors.

Product Strategy: New H3C Group's firewall offerings and feature enhancements are more focused on carrier and large data center use cases that operate in highly virtualized environments. This has led to a lack of focus on meeting all enterprise firewall use cases, especially perimeter security for enterprises.

Features: The vendor's firewalls lack an advanced malware network sandboxing feature, which is offered by a majority of firewall vendors, including those in China. This leaves customers to go with a separate vendor for advanced malware capabilities, as opposed to being an add-on feature of their existing firewalls. New H3C Group does not offer any CASB integration and lacks SaaS monitoring and management features, which increasingly are sought by enterprises with growing adoption of SaaS applications.

Palo Alto Networks

Palo Alto Networks is a large pure-play security vendor, based in Santa Clara, California, with more than 4,000 employees. The vendor has been shipping enterprise firewalls since 2007, and its 2016 revenue exceeded $1.4 billion. Its offerings include enterprise firewall physical and virtual appliances, endpoint software (Traps and GlobalProtect), threat Intelligence (AutoFocus), and SaaS security (Aperture). The vendor has recently started to highlight integrations between its solutions as a security platform.

Palo Alto Networks has recently released version 8 of its operating system (PAN-OS), with improvements for WildFire and Panorama, and new SaaS security and user credential protection features. It has also released a new entry-level hardware model (PA-220), two new intermediate appliances (PA-800 Series) and has refreshed its 5000 Series, available since 2011, with the 5220, 5250 and 5260 models.

Palo Alto Networks enjoys continued success in enterprise firewall selections, and has high customer satisfaction for its application visibility capabilities.

Palo Alto Networks is a solid contender for all enterprises, especially when evaluations give more weight to feature and management quality than to price.

STRENGTHS

Marketing Execution: Palo Alto Networks is the pure-play security vendor with the highest visibility on enterprise firewall shortlists. The vendor is visible on shortlists across all industries. Presales support is efficient, and the vendor very frequently comes out from shortlists with the highest overall evaluation score.

Sales Execution: Palo Alto Networks maintains a very high growth rate. With a list price of $1,000, the new PA-220 allows the vendor to target smaller branches. WildFire, the vendor's sandboxing option, has the highest attach rate and the largest customer base of all vendors evaluated in this research.

Capabilities: The Application Command Center (ACC) includes visibility of sanctioned and unsanctioned SaaS applications. Combined with its automated event aggregation and filtering and drill-down options, it makes it easy to understand application flows and related risks.

Customer Experience: Palo Alto Networks has a faithful customer base and scores very highly for overall customer satisfaction. Many clients report that they will renew without performing a competitive assessment and that they recommend the product to their peers. Several clients give good scores to vendor support in North America, and to the vendor's ability to meet expected performance in production environments.

Improvements: The vendor has initiated a refresh of its firewall appliances (PA-800 Series, PA-5200 Series and PA-220), with upgraded performance and a higher number of decrypted concurrent TLS connections. WildFire regional cloud options are available in Europe and Asia.

CAUTIONS

Marketing Strategy: Gartner observes that Palo Alto Networks' security platform strategy may impact the vendor's development capabilities across a growing set of products that also require development for better integrating together.

Innovations: Gartner has noticed in recent years that the ability of the vendor to lead the market with in-house innovations ahead of what other vendors offer has shifted to continuous improvements combined with acquisitions of small companies filling a gap in the vendor's portfolio.

Market Responsiveness: Some clients have expressed concern about the pace of firmware releases. They would like to see smaller batches of features instead of the very large updates that require more time to stabilize, forcing more conservative organizations to stick with an older version for a long time.

Sales Execution: Price is frequently cited by Gartner clients, especially distributed organizations, as a reason not to select Palo Alto Networks. The vendor has a smaller market share than its direct competitors in some of the European countries and Asia. Organizations from these regions should evaluate local resellers more stringently and request local references, especially in regions where the vendor does not provide direct vendor support. Despite recent improvements, resellers continue to hope for better tools when migrating from another firewall brand.

Customer Experience: Some clients cite that the vendor's centralized solution, Panorama, can become slow when managing a large number of appliances. The release notes of the recently published PAN-OS 8.0 include mentions of performance improvement for Panorama.

Sangfor

Sangfor was founded in 2000 and is headquartered in Shenzhen, China, with its EMEA regional headquarters in Dubai. Sangfor provides network security and cloud computing solutions such as Next Generation Application Firewall (NGAF), Internet Access Management (IAM), WAN Optimization (WANO), SSL VPN and Hyper-Converged Infrastructure (HCI). Sangfor started shipping its enterprise firewall product line (NGAF) in 2011. NGAF integrates web application firewall (WAF) functionality in the NGAF platform, a unique feature among the vendors evaluated. It now features 17 models for China and 10 models for international customers, for a firewall throughput of up to 80 Gbps. In addition, the vendor has four virtual firewall models and a central management system, Sangfor SC, along with a reporting platform, Sangfor DC. Sangfor offers support for AWS public cloud, and it has some SDN capabilities.

Recent feature releases include geoawareness and stability improvements. 2016 also saw the first release of virtual firewalls.

Sangfor serves a narrow segment of the market, with sales and operations mostly in China. The vendor is a good shortlist contender for Chinese customers that want WAF merged with a firewall, and those that want access to advanced security features faster than some other regional vendors have provided them.

STRENGTHS

Product Execution: Sangfor clients enjoy NGAF's ease of deployment and use, and its good price/performance ratio. Customers and partners indicate satisfaction with other advanced features, such as behavioral botnet detection and risk reporting, which enables customers to locate threats.

Product Strategy: Surveyed customers cite the presence of WAF as a primary motivation for selecting NGAF.

Customer Experience: Sangfor stakeholders give the vendor's presales and postsales customer support high marks.

CAUTIONS

Customer Experience: Some customers perceive and don't like that only Sangfor support can perform debugging and software and firmware upgrades. End users believe that they can't do advanced configurations without involving the vendor.

Geographic Strategy: Gartner does not see Sangfor firewalls often being shortlisted outside of China. Internationalization and an expanded geographic presence of the Sangfor firewall product line are ongoing efforts.

Product Execution: Potential customers outside of China should first verify the availability of vendor support and product documentation for their use case, and request references for organizations in the same region. Sangfor does decryption acting as a proxy. It has no on-box TLS decryption, which is a growing feature request among Gartner clients.

Partnerships: The vendor does not have any integration with network security policy management tools, making it more difficult for enterprises to manage policy in a multivendor situation.

SonicWall

Now based in Santa Clara, California, SonicWall was spun out of Dell in 4Q16, going private and becoming a stand-alone company. SonicWall's enterprise firewall portfolio comprises a total of five physical appliances across the NSA Series, aimed at midsize enterprises; and the SuperMassive Series for larger enterprises and data center deployments. SonicWall has no virtual firewall products. All SonicWall firewalls now have integration with Dell Networking X-Series switches, SonicPoints and WAN Acceleration Appliances (WXA).

The Global Management System (GMS) is a central management platform. SonicWall recently launched its Cloud GMS management solution. In addition to the main GMS consoles, SonicWall also offers GMS Analyzer and GMS Flow Server for additional reporting views.

Recent company news includes announced training and marketing enhancements to its channel programs.

SonicWall is not typically visible on a large number of enterprise shortlists, and it does not address some enterprise data center use cases. The vendor is a good shortlist candidate for value-conscious enterprises that desire more throughput at a reasonable price and a solid firewall appliance that is easy to manage.

STRENGTHS

Product Execution: Surveyed customers frequently mention the ability of the SonicWall product to meet budget and performance requirements. They also give good scores for ease of management.

Product Performance: SonicWall customers and partners note that the vendor does a very good job handling SSL/TLS decryption on-box without massive performance degradation.

Product Strategy: The cloud-based Capture Advanced Threat Protection service takes a multiengine approach to advanced threat detection. This approach shows promise and early feedback is positive.

Marketing Strategy: SonicWall has worked hard to rebuild its channels in order to reach more customers, and its continued investment in channel programs may raise visibility among Gartner clients.

CAUTIONS

Product Strategy: SonicWall's continued lack of a virtual firewall makes it increasingly less relevant to modern data center use cases as enterprises adopt public cloud IaaS and conduct private cloud projects.

Product Execution: SonicWall cloud security is less mature than its leading competitors, especially in its ability to inspect JavaScript to provide visibility on SaaS usage.

Market Responsiveness: The vendor has been slow in providing differentiating new features and enhancing its existing capabilities.

Marketing Execution: Gartner less frequently sees SonicWall being shortlisted by enterprise clients. The vendor has recently experienced a decline in revenue. Gartner attributes some of this to the succession of ownership changes and subsequent disruptions to the company.

Sophos

Sophos is a network and endpoint security vendor headquartered in Abington, U.K., with more than 3,000 employees. Historically an endpoint security vendor (Sophos Endpoint Protection, Intercept X), Sophos' portfolio now includes firewalls (XG Series and the older SG Series), wireless access point (Sophos AP), and enterprise mobility management (Sophos Mobile). Sophos Firewall Manager is the name of the centralized management software, and Sophos Central is the cloud-based centralized management portal for all Sophos security products.

Sophos' releases in recent months comprise evolutions of its firewall and endpoint integration, including automated host quarantine and the release of a cloud-based sandbox (Sophos Sandstorm). The vendor also made two acquisitions of security vendors leveraging machine learning techniques (Invincea and Barricade).

Sophos has demonstrated continued market focus and feature improvements, The vendor has demonstrated its commitment to align the roadmap of all its product lines to its product vision of a fully integrated solution.

Sophos is worth including on enterprise firewall shortlists, especially for the upper- and lower-midsize enterprise organizations, and for existing Sophos endpoint customers.

STRENGTHS

Marketing Execution: The vendor's revenue growth and customer retention rate are higher than the market average. Sophos regularly adds to its intellectual property with tactical acquisitions of technology-driven companies. Sophos' clients cite good price for value as a key factor in selecting the vendor, especially when purchasing a firewall cluster.

Geographic Strategy: Sophos firewalls are visible on European client shortlists for enterprise firewalls. Its visibility on U.S. shortlists is growing, helped by its existing presence in the endpoint protection market. Sophos management console is available in many European and Asian languages.

Capabilities: The Sophos XG product line includes a comprehensive set of appliances, including a dedicated offering, Remote Ethernet Device (RED), for the smallest branches. Embedded and centralized reports are comprehensive and easy to navigate, with easy-to-use filtering.

Customer Experience: Clients like the short learning curve to understand the new XG management interface. The vendor scores relatively higher than its competition for the value of the integration between endpoint and firewall (synchronized security).

Platform: Under the name Synchronized Security. Sophos executes on a very ambitious roadmap to integrate the XG firewall with Sophos' endpoint and cloud-based management.

CAUTIONS

Market Segmentation: Sophos' strategy focuses on enterprises with 5,000 employees or less, and heavily distributed organizations. Its product strategy is not a good fit for very large enterprise and data center use cases.

Customer Experience: Several clients and surveyed channel partners would like to see substantial improvements in vendor support, especially in providing enterprise-class responsiveness for first direct contact with the vendor.

Capabilities: The XG firewall is not yet available on AWS, and lacks dedicated SaaS discovery, visibility and control features. Some clients in regulated environments or with compliance requirements cite the limited reports and logs. Sophos XG lacks the ability to create virtual instances within a single physical appliance.

Platform: Surveyed clients would like to see Sophos providing integration with leading endpoint protection platforms, in addition to the vendor's own solutions. It does not offer, nor does it integrate with, CASB solutions for increased SaaS security.

Stormshield

Stormshield resulted from the merger of two French security providers (Arkoon and Netasq) in 2014. It provides enterprise firewalls and multifunction firewalls for SMBs to EMEA organizations with its Stormshield Network Security appliances. For enterprises, Stormshield offers 15 physical appliances and six virtual models. Its portfolio also includes host IPS (Stormshield Endpoint Security) and data-at-rest encryption software (Stormshield Data Security). The vendor provides virtual firewall appliances for AWS and Microsoft Azure IaaS platforms. For management and reporting, Stormshield has introduced Stormshield Management Center and Stormshield Visibility Center.

In addition to the new management appliances, Stormshield introduced a new ruggedized firewall for industrial environments during the Magic Quadrant evaluation period. Company news includes an agreement with Ingram Micro to distribute Stormshield products throughout EMEA.

Stormshield remains primarily a solution serving clients in Western Europe, and it is often selected in that region because it's from a trusted European vendor. The vendor is a suitable shortlist contender for European organizations that value a dependable enterprise firewall that can integrate with same-vendor endpoint protection.

STRENGTHS

Compliance: Stormshield owns several regional and nationwide European certifications, which makes it a good choice for European government agencies and private organizations working with the public sector. For example, Stormshield had early support for the European General Data Protection Regulation (GDPR) by introducing integration between its encryption solution and the firewall.

Product Execution: Surveyed customers and partners tout a strong behavioral IPS that impacts firewall performance minimally (compared to competitive offerings) as a reason to buy.

Support: Stormshield's customers cite the value of having in-country customer support. Certified support centers are available in nine European nations, as well as in the United Arab Emirates (UAE) and Singapore.

Product Strategy: Stormshield provides vulnerability management that leverages an integrated passive scanner. It allows security analysts to dynamically apply dedicated rules to vulnerable hosts by adding them to a group of vulnerable hosts.

Threat Research: Stormshield's internal threat research team collaborates with parent company Airbus Defence and Space CyberSecurity's Security Research Team to gain access to an expanded set of findings.

CAUTIONS

Product Execution: Stormshield continues to lag behind market leaders in some functional areas — how it integrates application control in the security policy and support of only a limited number of virtual domains within a single hardware appliance. It lacks threat intelligence feeds, and has yet to build an offering for SDN use cases. Stormshield does not support active/active use cases, making it unsuitable to address certain high-availability use cases.

Sales Execution: The vendor has fewer customers using its firewalls in IaaS environments than most of its competitors.

Geographic Strategy: Although Stormshield gets support from the large Airbus Defence and Space CyberSecurity group, the majority of its penetration, visibility and channel remain focused on EMEA, especially France.

WatchGuard

WatchGuard, headquartered in Seattle, Washington, is a recognized brand name for SMBs and distributed enterprises. In 2016, it released two new M models for firewalls, Firebox M4600 and M5600 for SMBs. WatchGuard also made a few significant feature enhancements around mobile security and VPN.

With recent enhancements around threat detection capabilities and multiple technology partnerships, WatchGuard offers a good product with better price versus performance relative to other vendors in the space. However, its product strategy is more focused toward midsize and distributed enterprise use cases than toward a majority of enterprise use cases.

WatchGuard should be considered by distributed enterprises that want good price/performance value.

STRENGTHS

Product Execution: WatchGuard has enhanced its threat detection capabilities as two separate threat intelligence subscriptions. Reputation Enabled Defense, under the Basic Security suite, includes feeds from OEM partners like Kaspersky, Deutsche Telekom and

other threat intelligence sources. Also offered is Threat Detection and Response (TDR) as a part of the Total Security suite. TDR offers better correlation with network and endpoint security events, along with third-party threat intelligence feeds that the vendor has partnered with. Host Ransomware Prevention is also a component in TDR. This will equip WatchGuard customers with better correlation and threat detection capabilities. WatchGuard offers good analytics and reporting capabilities with its cloud-based reporting solution, Dimension. Surveyed stakeholders have cited it as one of the key strengths of the portfolio.

Technology Partner Ecosystem: Watchguard has partnered with multiple technology providers to provide better features and integration capabilities. It uses Forcepoint as a URL filtering provider, AVG as its antivirus engine and Trend Micro as a provider of an IPS signatures database. WatchGuard also offers integration with ManagedMethods, a dedicated CASB provider. It also has OEM partnerships with multiple threat intelligence feeds.

Features: WatchGuard offers a policy mapping feature for identifying the firewall rule usage. Policy Map provides a visual flow map showing which policies are hit by traffic moving through the firewall. This helps in identifying overlapping rules.

Sales Execution: The vendor offers good price versus performance value, with cost-effective products and subscriptions. Surveyed end users have cited this as one of the vendor's strengths.

CAUTIONS

Technical Support: Some surveyed end users have reported that the vendor lacks quick resolution through the technical support ticket process, which is raised as an email, and it needs improvement there.

Marketing Execution: WatchGuard has its major presence in midsize and distributed enterprises, and does not effectively address several enterprise use cases. Surveyed VARs have also indicated they sell WatchGuard Firebox appliances to only midsize and distributed enterprise customers. In addition, Gartner does not see WatchGuard being frequently shortlisted by the enterprise clients as a possible firewall candidate.

Product Strategy: WatchGuard lacks support for SDN vendors in supporting SDN deployment use cases. However, WatchGuard can help distributed enterprises manage and secure a mixed WAN environment. WatchGuard has lagged behind most of its competitors in releasing virtual firewall services to support customer deployments in the public cloud.

Vendors Added and Dropped

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

New H3C Group was added to the Magic Quadrant.

Dropped

No vendors were dropped from the Magic Quadrant.

Inclusion and Exclusion Criteria

Inclusion Criteria

Network firewall vendors that meet the market definition and description were considered for this research under the following conditions:

- Gartner analysts have assessed that the vendor has the ability to effectively compete in the enterprise firewall market.
- The vendor regularly appears on shortlists for selection and purchases.
- The vendor demonstrates a competitive presence in enterprises and sales.
- Gartner analysts consider that aspects of the vendor's product execution and vision merit inclusion.
- The vendor has achieved enterprise firewall product sales (not including maintenance) in the past calendar year of more than $10 million, and within a customer segment that is visible to Gartner.

Exclusion Criteria

Network firewall vendors may have been excluded from this research for one or more of the following reasons:

- The vendor has minimal or negligible apparent market share among Gartner clients, or it is not actively shipping products.
- The vendor is not the original manufacturer of the firewall product. This includes hardware OEMs, resellers that repackage products that would qualify from their original manufacturers, as well as carriers and ISPs that provide managed services. We assess the breadth of OEM partners as part of the evaluation of the firewall, and we do not rate platform providers separately.
- The vendor's products sell as network firewalls, but do not have the capabilities, scalability and ability to directly compete with the larger firewall product/function view. Products that are suited for SMBs (such as UTM firewalls, or those for small office/home office placements) are not targeted at the market this Magic Quadrant covers (enterprises) and are excluded.
- The vendor primarily has a network IPS with a non-enterprise-class firewall.
- The vendor has personal firewalls, host-based firewalls, host-based IPSs and WAFs (see Note 1) — all of which are distinctly separate markets.

Evaluation Criteria

Ability to Execute

Product or Service: This includes service and customer satisfaction in enterprise firewall deployments. Execution considers factors related to getting products sold, installed, supported and in users' hands. Strong execution means that a company has demonstrated to Gartner analysts that products are successfully and continually deployed in enterprises, and that the company wins a large percentage in competition with other vendors. Companies that execute strongly generate pervasive awareness and loyalty among Gartner clients, and also generate a steady stream of inquiries to Gartner analysts. Execution is not primarily about company size or market share, although those factors can affect a vendor's Ability to Execute. Sales are a factor; however, winning in competitive environments through innovation and quality of product and service is more important than revenue. Key features are weighted heavily, such as foundation firewall functions, console quality, low latency, range of models, secondary product capabilities (logging, event management, compliance, rule optimization and workflow), and the ability to support complex deployments and modern DMZs. Having a low rate of vulnerabilities in the firewall is important. The logistical capabilities for managing appliance delivery, product service and port density matter. Support is rated on the quality, breadth and value of offerings through the specific lens of enterprise needs.

Overall Viability: This includes overall financial health, prospects for continuing operations, company history, and demonstrated commitment in the firewall and security markets. Growth of the customer base and revenue derived from sales are also considered. All vendors were required to disclose comparable market data, such as firewall revenue, competitive wins versus key competitors (which are compared with Gartner data on such competitions held by our clients) and devices in deployment. The number of firewalls shipped or the market share is not the key measure of execution. Rather, we consider the use of these firewalls to protect the key business systems of enterprise clients and those being considered on competitive shortlists.

Sales Execution/Pricing: We evaluate the company's pricing, deal size, installed base, and use by enterprises, carriers and managed security service providers (MSSPs). This includes the strength of the vendor's sales and distribution operations. Presales and postsales support is evaluated. Pricing is compared in terms of a typical enterprise-class deployment, and includes the cost of all hardware, support, maintenance and installation. Low pricing will not guarantee high execution or client interest. Buyers want good results more than they want bargains, and think in terms of value over sheer low cost. Cost of ownership over a typical firewall life cycle (three to five years) is assessed, as is the pricing model for conducting a refresh while staying with the same product and replacing a competing product without intolerable costs or interruptions. The robustness of the enterprise channel and third-party ecosystem is important.

Market Responsiveness/Record: This evaluates the vendor's ability to respond to changes in the threat environment, and to present solutions that meet customer protection needs rather than packaging up fear, uncertainty and doubt. This criterion also considers the provider's

history of responsiveness to changes in demand for new features and form factors in the firewall market, and how enterprises deploy network security.

Marketing Execution: Competitive visibility is a key factor; it includes which vendors are most commonly considered to have top competitive solutions during the RFP and selection process, and which are considered top threats by the others. In addition to buyer and analyst feedback, this ranking looks at which vendors consider the others to be direct competitive threats, such as by driving the market on innovative features co-packaged within the firewall, or by offering innovative pricing or support offerings. An NGFW capability is heavily weighted, as are enterprise-class capabilities, such as multidevice management, virtualization, adaptability of configuration and support for enterprise environments. Unacceptable device failure rates, vulnerabilities, poor performance and a product's inability to survive to the end of a typical firewall life span are assessed accordingly. Significant weighting is given to delivering new platforms for scalable performance in order to maintain investment, and to the range of models to support various deployment architectures.

Customer Experience and Operations: These include management experience and track record, as well as the depth of staff experience — specifically in the security marketplace. The greatest factor in these categories is customer satisfaction throughout the sales and product life cycles. Low latency, throughput of the IPS capability and how the firewall fared under attack conditions are also important. Succeeding in complex networks with little intervention (for example, one-off patches) is highly considered.

Table 1. Ability to Execute Evaluation Criteria

Evaluation Criteria	Weighting
Product or Service	High
Overall Viability	Medium
Sales Execution/Pricing	Medium
Market Responsiveness/Record	High
Marketing Execution	Medium
Customer Experience	High
Operations	Medium

Source: Gartner (July 2017)

Completeness of Vision

Market Understanding and Marketing Strategy: This includes providing a track record of delivering on innovation that precedes customer demand, rather than an "us, too" roadmap. We also evaluate the vendor's overall understanding of and commitment to the security and network security markets. Gartner makes this assessment subjectively by several means, including interaction with vendors in briefings and feedback from Gartner customers on information they receive concerning roadmaps. Incumbent vendor market performance is reviewed year by year against specific recommendations that have been made to each vendor, and against future trends identified in Gartner research. Vendors cannot merely state aggressive future goals; they must put plans in place, show that they are following their plans and modify those plans as they forecast how market directions will change. Understanding and delivering on enterprise firewall realities and needs are important, and having a viable and progressive roadmap and continuing delivery of NGFW features are weighted very highly. The NGFW capabilities are expected to be integrated to achieve correlation improvement and functional improvement.

Sales Strategy: This includes preproduct and postproduct support, value for pricing, and clear explanations and recommendations for detecting events, including zero-day events. Building loyalty through credibility with a full-time enterprise firewall staff demonstrates the ability to assess the next generation of requirements. Vendors need to address the network security buying center correctly, and they must do so in a technically direct manner, rather than selling just fear or next-generation hype. Channel and third-party security product ecosystem strategies matter insofar as they are focused on enterprises.

Offering (Product) Strategy: This criterion focuses on a vendor's product roadmap, current features, NGFW integration and enhancement, virtualization and performance. Credible, independent third-party certifications include the Common Criteria for Information Technology Security Evaluation. Integration with other security components is also weighted, as well as product integration with other IT systems. We also evaluate how the vendor understands and serves the enterprise branch office and data center. Innovation, such as introducing practical new forms of intelligence to which the firewall can apply policy, is highly rated. An articulated, viable strategy for addressing the challenges in SDN deployments is important, as is evidence of execution within cloud and virtualized environments.

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

Vertical/Industry Strategy and Geographic Strategy: These include the ability and commitment to service geographies and vertical markets, such as complex enterprise multinational deployments, MSSPs, carriers or governments.

Innovation: This includes R&D and quality differentiators, such as:

- Performance, which includes low latency, new firewall mechanisms, and achieving high IPS throughput and low appliance latency.
- Firewall virtualization and securing virtualized environments.
- Integration with other security products.

Management interface and clarity of reporting — that is, the more a product mirrors the workflow of the enterprise operation scenario, the better the vision.

"Giving back time" to firewall administrators by innovating to make complex tasks easier, rather than adding more alerts and complexity.

Products that are not intuitive in deployment, or operations that are difficult to configure or have limited reporting, are scored accordingly. Solving customer problems is a key element of this criterion. Reducing the rule base, offering interproduct support and leading competitors on features are foremost.

Table 2. Completeness of Vision Evaluation Criteria

Evaluation Criteria	**Weighting**
Market Understanding	High
Marketing Strategy	Medium
Sales Strategy	Medium
Offering (Product) Strategy	High
Business Model	Medium
Vertical/Industry Strategy	No Rating
Innovation	High
Geographic Strategy	Medium

Source: Gartner (July 2017)

Quadrant Descriptions

Leaders

The Leaders quadrant contains vendors that build products that fulfill enterprise requirements. These requirements include a wide range of models, support for virtualization and virtual LANs, and a management and reporting capability that is designed for complex and high-volume environments, such as multitier administration and rule/policy minimization. A solid NGFW capability is an important element, as enterprises continue to move away from having dedicated IPS appliances at their perimeter and remote locations. Vendors in this quadrant lead the market in offering new features that protect customers from emerging threats, provide expert capability rather than treat the firewall as a commodity and have a good track

record of avoiding vulnerabilities in their security products. Common characteristics include handling the highest throughput with minimal performance loss, offering options for hardware acceleration and offering form factors that protect enterprises as they move to new infrastructure form factors.

Challengers

The Challengers quadrant contains vendors that have achieved a sound customer base, but they are not consistently leading with differentiated next-generation capabilities. Many Challengers have not fully matured their NGFW capability — or they have other security products that are successful in the enterprise and are counting on the relationship, rather than the product, to win deals. Challengers' products are often well-priced, and, because of their strength in execution, these vendors can offer economical security product bundles that others cannot. Many Challengers hold themselves back from becoming Leaders because they choose to place security or firewall products at a lower priority in their overall product sets. Firewall market Challengers will often have significant market share, but trail smaller market share Leaders in the release of features.

Visionaries

Visionaries have the right designs and features for the enterprise, but they lack the sales base, strategy or financial means to compete consistently with Leaders and Challengers. Most Visionaries' products have good NGFW capabilities, but lack in performance capabilities and support networks. Savings and high-touch support can be achieved for organizations that are willing to update products more frequently and to switch vendors if required. If firewalling is a competitive element for an enterprise, then Visionaries are good shortlist candidates. Vendors that do not have strong NGFW capabilities are supplementing them in a defensive move, while vendors that have strong NGFW offerings are focused on manageability and usability. Gartner expects the next wave of innovation in this market to focus on better, more automated east/west microsegmentation in public cloud and SDN environments.

Niche Players

Most vendors in the Niche Players quadrant are smaller vendors of enterprise firewalls, makers of multifunction firewalls for SMBs or branch-office-only product makers that are attempting to break into the enterprise market. Many Niche Players are making larger versions of SMB products with the mistaken hope that this will satisfy enterprises. Some enterprises that have the firewall needs of an SMB (for example, some Type C risk-averse enterprises and some distributed enterprises) may consider products from Niche Players, although other models from Leaders and Challengers may be more suitable. If local geographic support is a critical factor, then Niche Players can be shortlisted.

Context

The enterprise firewall market is the largest security product market. It is populated with mature vendors and some more recent entrants. Changes in threats, as well as increased enterprise demand for mobility, virtualization, SDN and use of the cloud, have increased demand for new firewall features and capabilities. Organizations' final product selection

decisions must be driven by their specific requirements, especially in the relative importance of management capabilities, ease and speed of the deployment, acquisition costs, IT organization support capabilities, and integration with the established security and network infrastructure and teams.

Market Overview

As the first line of defense between external threats and enterprise networks, firewalls need to continually evolve to maintain effectiveness, responding to the continuing evolution in threats as well as to changes in enterprise network speed and complexity. Firewalls have high adoption and penetration rates in all markets. This means that, to protect their installed base, incumbents must add improved capabilities and increase performance, or face either replacement by innovative market entrants or commoditization by low-cost providers. Network security policy management (NSPM) products are increasingly used to manage complexity, especially in multivendor situations (see Note 2).

Enterprise Firewalls Are Next-Generation Firewalls

One key area of firewall evolution that has been widely supported is what Gartner (in 2009) called "NGFW features" — namely, integrated deep packet inspection intrusion prevention, application identification and granular user control. The key differentiators in these areas are IPS effectiveness, as demonstrated through third-party testing under realistic threat and network load conditions, and fine-grained, user-based policy enforcement in the top business and social media applications. Identity-based policy enforcement, or the ability to enforce policy on thousands of applications, remains a defining feature.

All enterprise firewall vendors today offer NGFWs. For new firewalls, there is no distinction between an enterprise firewall and an NGFW.

Because it is saturated, the firewall market is driven by refresh cycles of four to five years. Gartner estimates that the transition to NGFW from traditional firewalls will complete within the next two years. We have seen some common patterns in the firewall market as enterprises with 3- to 5-year-old firewalls and IPSs evaluate replacement:

- Enterprises with traditional firewalls seek to have firewalls that have application and user visibility, and to require enforcement options in their next refresh.
- Enterprises not currently using any IPSs migrate to NGFWs with minimal use of advanced features.
- Enterprises with firewalls and stand-alone IPSs that are employed primarily in detection mode (that is, using minimal signature sets) migrate to NGFWs using the built-in IPS capabilities.
- Enterprises with firewalls and stand-alone IPSs that are used for active prevention, with large signature sets and some custom signatures, migrate to NGFWs for the firewall with application control and user context, but continue using stand-alone IPSs.
- High-security environments upgrade to NGFWs for the firewall, and upgrade IPSs to NGIPSs.

Organizations look to extend their on-premises firewall vendor into IaaS cloud providers.

Enterprises seek NGFW functionality as they transition from physical data center to virtualized environments and SDN.

UTM Still Can't Compete With Enterprise Firewalls

Historically, UTM vendors have and continue to target SMB clients. However, in the past few years, the large UTM vendors have tried to expand beyond their traditional use case by stretching into the large enterprise market. They now try to sell high-throughput UTM to enterprise clients that score price competitiveness higher than security. Gartner sees some limited success for Type C enterprises (see Note 3), but it is mostly restricted to two use cases: distributed Type C enterprises (mostly in the retail industry), and firewall-only for network segmentation at low cost. However, the UTM approach fails to convince Type A and Type B enterprises that require mature application and user control capabilities, and do not consolidate web antivirus on the internet-facing firewall (see "Next-Generation Firewalls and Unified Threat Management Are Distinct Products and Markets").

UTM vendors also face difficulties in building a strong sales and support channel for enterprises (similarly, enterprise firewall vendors underestimate the work of building an SMB channel). Most enterprise buyers are also wary of shortlisting a UTM vendor because of its primary focus on SMBs and limited brand awareness.

Decrypt This

Enterprises face a growing need for SSL decryption, principally to enforce web-filtering policy and to prevent malware infections. In "Predicts 2017: Network and Gateway Security," Gartner anticipates that, through 2019, more than 80% of enterprises' web traffic will be encrypted. Consequently, a growing number of malware attacks, including ransomware, will move to use HTTPS to covert initial infection and command and control communications.

> By 2020, more than 60% of organizations will fail to decrypt HTTPS efficiently, missing most targeted web malware.

Decrypting SSL/TLS on a firewall creates organizational issues, such as ensuring employees' right to privacy, and technical challenges, such as performance issues and product sizing difficulties for the firewall channel. End-user experience is likely to be affected too. Some application traffic cannot be decrypted, and firewall vendors do a poor job at providing an up-to-date list of exceptions, leading to traffic being blocked. In the client reference survey, despite the self-evaluation bias that generally results in inflated numbers, and the fact that references provided by vendors tend to use more features than the market average, only 29% of the respondents answered that they were decrypting HTTPS traffic.

Virtualized Firewalls: Hype Accelerates, and Demand Starts to Follow

As data center virtualization has continued, SDN projects get more numerous, and as IaaS deployments become more common, demand for virtualized environment support has grown. Performance and the ability to manage firewall policy through a single integrated management console for stand-alone appliances or virtual appliances are key differentiators. Gartner has not seen the firewall features of virtualization platforms (such as those offered with VMware or AWS) as a major competitor to mainstream firewall vendors because the need for separation of duties drives clients to doubt the infrastructure's ability to protect itself. Gartner covers virtual/cloud firewall vendors such as vArmour and Illumio, but has not seen significant adoption. VMware's NSX work with Palo Alto Networks, Check Point Software Technologies, Fortinet and other firewall vendors has created buzz for virtualizing and securing data centers, networks and east-west segmentation, and some lean-forward customers have adopted these. Adoption is growing quickly (from small numbers). As other virtualization platforms, such as Citrix Xen and Microsoft Hyper-V, gain traction, managing heterogeneous virtualized firewalls from existing physical firewall vendors, virtualization platform vendors and virtual-only firewalls will present a challenge. Performance remains a barrier to wider deployment: Almost all network firewalls today are delivered on purpose-built appliances because of the poorer performance of running firewalls on general-purpose servers. Almost all operating systems within firewall appliances are uniquely hardened, subject to stringent third-party security evaluations. Security-minded enterprises are also rightly skeptical of running firewalls within a hypervisor that is between the threat and the firewall.

Another big issue in deploying virtual firewalls in SDN or IaaS projects is the inability of enterprise virtual firewalls to spin up appropriate policy as servers are spun up. Agility is one of the key business benefits of SDN and IaaS, and the need for human interaction with firewall policy subtracts from the business benefits these agile architectures bring with them.

Gartner market data continues to show that virtual firewall revenue accounts for far less than 5% of enterprise firewall market revenue. However, client market inquiries show an increased interest in virtual firewalls, and vendors are scrambling to meet that demand by attempting to increase virtual firewall performance and by automating firewall policy orchestration in dynamic environments.

The Firewall Market Is Still Growing, but at a Slowing Pace

During the evaluation period, the firewall market grew 8.9% to $9.27 billion. For 2017, Gartner estimates that the firewall market will grow approximately 7.8%. We also forecast that this market will reach a compound annual growth rate of 7.4% from 2014 through 2021, with growth decelerating for the remainder of that period. Gartner believes that the firewall market is "at capacity": This is the largest security product market (fast approaching $10 billion), and incremental market growth is significant. Firewall refreshes remain constant at a five-year average, so even if great new products emerge, incumbent firewalls are rarely refreshed before they reach maturity. This refresh dynamic results in the market being linear, rather than having macrorefresh cycles or "bumps" of refreshes, as in other markets.

The Absence of Significant Innovation Brings Challengers Closer to Leaders

In most technology markets, Leaders will innovate and Challengers will later adopt those features for their clients who are fine with getting features later, but for a lower price. Since the emergence of the NGFW, the enterprise firewall market has been bifurcated into shortlists of "security first" Leaders and "price really matters, and we can't yet consume the newest features" Challengers. This gap widened at first; however, over the past year, the gap has closed — not through the innovation of Challengers, but with the slower pace of true innovation by Leaders and the absence of Visionaries. Gartner has seen these bifurcated shortlists start to change slightly as Challengers creep in, and Leaders are unable to demonstrate a clear delta in capability that justifies premium prices. Gartner believes extremes of marketing strategies by Leaders are behind this, with undermarketing making true innovations a well-kept secret, and overmarketing producing "hype" roadmaps and announcements that don't resonate with the buying center. Client "bake-offs" and hands-on comparative evaluations will show today's Leaders as having more capability, especially for management and reporting; however, if this trend continues, Leaders will allow the lower price offerings of Challengers to win more often when a hands-on evaluation is not extensive.

Have Some Advanced Threat Detection With That Firewall

Advanced threat detection using a network sandbox — offered by stand-alone vendors such as FireEye — has become a rapidly growing market. Advanced threat defense/detection is penetrating the mainstream market; almost all enterprise firewall vendors have introduced solutions over the past five years. These firewall-attached sandboxes are delivered mostly as cloud-based sandboxes priced as subscription-based services, rather than as a customer-based, on-premises sandbox where files are sent for inspection. The cloud advantage is a fixed-fee subscription that does not have to be scaled up nor consume rack space, and a considerably lower price. All of the firewall vendors evaluated here either deliver a network sandbox today, or have it on their short-term roadmaps. Some of these are built by the firewall vendors, while others are delivered through third-party partnerships.

Firewall-connected sandboxes have appealed mostly to budget-constrained Type B enterprises that would rather maintain single-console control over their firewall than deploy a separate platform. As the desire to defend against the advanced threat is permeating the mainstream market, customers are increasingly turning to their firewall vendors for their network sandboxing needs (see "Market Guide for Network Sandboxing"). Firewall-attached sandboxes have almost reached parity with stand-alone solutions, making them "good enough" for most enterprises.

Confusing Use of "Application" and "Firewall" in Three Distinct Products

Overlapping terminology and unclear marketing can lead to confusion among the three distinct issues of application control, WAFs and firewalls on application delivery controllers (ADCs). The firewall application control approaches used by enterprise vendors are mostly about controlling access to external applications, such as Facebook and peer-to-peer (P2P) file sharing.

WAFs are different: They are placed primarily in front of web servers in the data centers. Pure-play WAF companies (such as Imperva) or data center infrastructure vendors that provide WAF technology within their ADCs are concerned with protecting custom internal web applications.

While some ADC vendors (such as F5) are now offering network firewalling within their ADCs as well, Gartner does not see NGFW, WAF and ADC technologies converging because they are for different tasks at different placements in the network, and are often managed by entirely different teams. Most traffic to enterprise web servers remains encrypted until it reaches the ADC (or the server itself, if no ADC/WAF is present), meaning the owners of firewalls and IPSs face the decision of whether to engage SSL inspection, which involves a termination and re-encryption of these sessions (see "Security Leaders Must Address Threats From Rising SSL Traffic" and "Web Application Firewalls Are Worth the Investment for Enterprises"). This performance impact is often hard to measure clinically, and an underestimation of its impact affects everything the firewall is processing. Many still use discrete WAF (because of its better understanding of custom web applications) and ADC (better application performance to users) as the optimal way to answer that question, and Gartner recommends this practice, if budget allows.

As Gartner advises clients, most enterprises have a single brand of network firewall for all placements, including internet-facing, virtualized, data center and branch (see "One Brand of Firewall Is a Best Practice for Most Enterprises"). These data center firewalls will be challenged to gain any noteworthy enterprise market share until they can provide competitive firewalling for all enterprise use cases in a range of physical and virtual form factors. They can, however, serve a specialized niche of placements, such as in cases where the data center is a separate business with its own firewall operations staff.

?

Asia-Pacific Context

Market Differentiators

This document was revised on 17 July 2017. The document you are viewing is the corrected version. For more information, see the Corrections (http://www.gartner.com/technology/about/policies/current_corrections.jsp) page on gartner.com.

Firewall technology continues to be a fundamental element of the network security strategy for Asia/Pacific (APAC) organizations. Gartner observes two usage profiles in Asia/Pacific concerning firewall acquisition and deployed features:

- Technologically more advanced Asia/Pacific countries (such as Japan, Singapore and Australia) are considering advanced firewall capabilities, such as firewall integration with the software-defined network (SDN), support for hybrid networks (private and cloud), and more visibility and control into SaaS applications.

Emerging Asia/Pacific countries (India, Indonesia and others) are still moving through slow but consistent refreshes of their traditional firewalls with the latest firewalls and features such as cloud-based sandboxing.

- Also, with the slow but steady increase in adoption of cloud and SaaS applications in emerging countries, we have seen a shift in the selection criteria toward the "lean forward" features in a firewall, such as support for SDN and SaaS monitoring.

The Greater China region has multiple local firewall players that provide competitive vendor selection choices while delivering regional support and services to clients.

Considerations for Technology and Service Selection

Clients in Asia/Pacific show a preference for providers that have a local presence, at a minimum for sales and presales support. APAC organizations expect support for local languages in product management interfaces, documentation, technical support, and reporting. Gartner has observed that a growing number of international firewall vendors are improving their local presence in the region, which is, of course, a positive for end users and overall market growth.

In addition to the application awareness and intrusion prevention capabilities delivered by current-generation firewalls, vendors also need to support the social networking and browser applications that are specific to and heavily used by Asia/Pacific customers, even though the region-specific applications are not prevalent in the product's "home" country. Examples include Tencent (QQ, WeChat and QQ Browser), Weibo, Line, KakaoTalk, Viber and PPS Entertainment. Deep understanding of this application ecosystem and subsequent ability to filter are important product differentiators in the Asia/Pacific market.

In the emerging Asia/Pacific countries (such as India, Malaysia, Thailand and China), there is mixed adoption of local and international vendors. Security-conscious enterprises are primarily adopting international vendors that provide the best-of-breed technology, as seen globally. Price-conscious enterprises prefer a local vendor that offers competitive pricing with local support. High throughput is an important factor in the telco/ISP vertical in Asia/Pacific's heavily populated countries, due to the significant amount of 3G/4G mobile usage. These deployments tend not to use advanced functions like intrusion prevention systems (IPSs) and application control due to performance issues at that scale. Some countries are already, or are very close to, rolling out 5G, and the telco-class firewall is still a vibrant subsegment of the APAC firewall market.

Inside mature Asia/Pacific markets (such as Japan, Singapore, Australia, New Zealand, South Korea and Hong Kong), enterprise firewall features such as security efficacy, centralized management and robust support are all valued by customers, as is competitive pricing. In Japan, there is also a trend to use managed firewall services from system integrator or service providers, such as Fujitsu, Hitachi and NTT Communications. Gartner is also seeing high levels of interest in mature countries in the region for integrated advanced threat detection capabilities, leading to an increased attach rate of this "add on" feature in firewall sales.

Firewall vendors that offer this feature to advanced Asia/Pacific customers as part of their overall architecture will be more successful than point product providers of advanced threat detection.

Notable Vendors

Vendors included in this Magic Quadrant Perspective have customers that are successfully using their products and services. Selections are based on analyst opinion and references that validate IT provider claims; however, this is not an exhaustive list or analysis of vendors in this market. Use this perspective as a resource for evaluations, but explore the market further to gauge the ability of each vendor to address your unique business problems and technical concerns. Consider this research as part of your due diligence and in conjunction with discussions with Gartner analysts and other resources.

360 ESG

China-based 360 Enterprise Security Group (360 ESG) is an established regional security technology and service provider that sells exclusively in China. It offers Common Criteria (CC) EAL3+-certified firewalls. In addition to security products and services, 360 ESG also provides a search engine and a web browser in China. Its firewall product line is the NSG series, which supports centralized management of multiple firewalls through 360 ESG's centralized management SMAC platform. 360 ESG has a threat information analysis center in China, and threat intelligence is shared with all of its product lines. 360 ESG offers advanced malware protection with the 360 Skyeye sandbox and the Skylar endpoint detection and response (EDR) correlation. Its virtual next-generation firewall (NGFW) provides support for regional Chinese public clouds, Ali Cloud and Qing Cloud.

Language support: 360 ESG offers a management interface and documentation in simplified Chinese.

Technical support: It has highlighted that it has 30 technical assistance centers (TACs) in China where it offers support in Chinese.

AhnLab

South Korea-based AhnLab is a regional security vendor in East Asia. Its firewall has two regional (South Korean) certifications — it is Telecommunications Technology Association Internet Protocol version 6 (TTA IPv6)-verified and also has a Good Software (GS) Certification. The majority of AhnLab's firewall sales come from government agencies (mostly in South Korea) and small and midsize businesses (SMBs) with fewer than 1,000 employees.

Language support: In addition to English, AhnLab also offers a management console and documentation in the Korean language.

Technical support: AhnLab has regional technical support centers in South Korea, China and Japan.

Check Point Software Technologies

Check Point Software Technologies has a significant existing client base in the mature Asia/Pacific region. The vendor has strong brand recognition, market-leading features, a large

channel, and extensive country-level coverage in mature Asia/Pacific regions, such as Australia, Singapore and Japan. It is also expanding its direct presence in emerging APAC countries like India. Check Point opened a regional technical support center for Indian clients in 2016 to address the issue of slower resolution of technical support queries. Check Point has been named as one of the top three competitors in the region by participating vendors in our enterprise network firewall Magic Quadrant survey.

In APAC, its regional data centers for its Capsule cloud-based services are located in Japan, Australia, Singapore, Thailand and Hong Kong. It also has its Mobile Threat Prevention data center located in Singapore for the APAC region.

Language support: Along with English, Check Point also offers technical support in Chinese and Japanese regional languages.

Other than English it also offers management consoles and documentation in Japanese and claims to offer on-demand local language support when requested.

Technical support: Check Point has four regional technical support centers in the APAC region: in Japan, India, China and Australia.

Cisco

Cisco has a significant share of the security market in the APAC region, and has leveraged its networking heritage very successfully over a long period of time in sales of its firewall platform. It continues to be a strong vendor in this market due primarily to its large channel and the cross-selling opportunity with Asia/Pacific partners and clients. The move to the new more competitive Firepower platform and a better management platform/interface are proving to be successful in terms of better adoption relative to the previous years.

Cisco has not disclosed the location of their data centers in APAC region for their cloud-based services.

Language support: In addition to English, it also offers Firepower Management Center and related documentation in Japanese, Chinese and Korean languages.

Technical support: Cisco has APAC regional technical support centers in India and Japan, where it offers support in English and Japanese.

Fortinet

Fortinet has a strong presence in almost all of the Asia/Pacific countries, and is ahead of a number of regional players. In many Asia/Pacific markets, Fortinet is the second-largest network security vendor. Fortinet has been named as one of the top three competitors in the region by participating vendors in our enterprise network firewall Magic Quadrant survey.

In APAC, Forinet has a regional data center for its cloud-based services in Tokyo and research centers in Bangalore, Singapore and Taiwan.

Language support: Along with English, Fortinet also offers its management console in Japanese, tradition/simplified Chinese and Korean languages.

Technical support: It has six regional technical support centers in APAC in Malaysia, India, China, Australia, South Korea and Japan, among which China, South Korea and Japan offer support in their regional local language.

New H3C Group

New H3C Group (New H3C) is headquartered in China and provides a portfolio of network security products to its Chinese customers. It has Chinese regional certifications from Spirent for NGFW performance and a certification from China Telecommunication. New H3C is a member of China National Vulnerability Database of Information Security.

Language support: Documentation for New H3C offerings is available in both English and Chinese.

Technical support: New H3C has multiple technical support centers in mainland China and in Hong Kong. The number of technical support centers is not disclosed by the vendor. It offers support in the Chinese language.

Hillstone Networks

Hillstone Networks is a Chinese network security vendor that has a broad portfolio of network security products. The majority of company revenue comes from firewalls, and Hillstone Networks targets its sales to both carriers and enterprises from Asia. Hillstone's customer base is mostly in China.

Hillstone's CloudEdge virtual firewall provides support for public cloud, which includes regional public cloud AliCloud.

Language support: In addition to English, it offers its management console in simplified Chinese, traditional Chinese and Korean, and documentation in simplified Chinese.

Technical support: Hillstone has regional APAC technical support centers in China, Singapore and Malaysia, which offer support in English and Chinese.

Huawei

Huawei is one of the few Chinese network security companies that has expanded its foothold outside of its home region in a significant way. Although Huawei Security is part of its networking and security division, Huawei Security has its own security sales team and dedicated channel partners. In addition to international certifications, its firewalls are also certified with regional Chinese certifications, such as "China: IPv6 ready."

In APAC, its data centers for its security signature database are located in China and Japan, and the security intelligence cloud is deployed in China.

Language support: In addition to English, Huawei offers its management console and documentation in Chinese.

Technical support: Huawei has 14 regional technical support centers in APAC: Australia, China, Hong Kong, India, Indonesia, Japan, Korea, Kazakhstan, Malaysia, New Zealand, Philippines, Singapore, Thailand and Turkey. It offers support in Japanese, Chinese, Korean, Thai and Turkish along with English.

Juniper Networks

Juniper Networks has been operating in the APAC region for a considerable time and has a strong legacy customer base there. It has proven networking channel and technical support services in the region. Because of the delay in introducing advanced firewall features, Juniper has lost a significant share in APAC to vendors like Fortinet, Check Point, and Palo Alto Networks. Recent feature enhancements will be well-received by existing clients.

Juniper Networks does not have any regional data centers for its cloud services in the APAC region.

Language support: Along with English they offer their documentation in Japanese and Korean.

Technical support: Juniper has seven regional technical support centers in APAC: China, Australia, Japan, South Korea, Philippines and Hong Kong. It also has two global technical support centers in Bengaluru (also called Bangalore), India and Dalian, China, which offer support in Korean, Japanese and Mandarin along with English.

Palo Alto Networks

Palo Alto Networks has many wins among customers in Asia/Pacific with more mature IT adoption profiles. The company is continuing to invest in Asia/Pacific and has established a viable channel that has improved its presence, particularly in emerging Asia/Pacific countries. For its firewalls, Palo Alto Networks has been named as one of the top three vendors who are the greatest competitors in the region.

In the APAC region, the company has its Wildfire and Aperture data centers in Singapore and Japan.

Language support: Other than English, it offers its management console and documentation in simplified Chinese, traditional Chinese and Japanese.

Technical support: Palo Alto Networks has regional technical support centers in the APAC region in India, Singapore and Japan.

Sangfor

Sangfor is a Chinese firewall vendor, with a strong presence in Greater China through strong channel relationships. Sangfor is aggressively going after the Association of Southeast Asian Nations (ASEAN) market, where it has expanded its partners to hundreds.

Sangfor firewalls provide support for public cloud, including the regional public clouds Alibaba Cloud and Tencent Cloud. It has its data centers hosted in China, Hong Kong and Malaysia.

Language support: Sangfor offers its management console and documentation in Chinese and English.

Technical support: Sangfor has two technical support centers in APAC, in China and Malaysia, where it offers support in Chinese, English, Thai, Malay and Indonesian.

SonicWall

SonicWall is a long-established network security vendor. Its portfolio includes network security, mobile access control, and email security product lines. Gartner has observed a dip in its presence in the new enterprise firewall deals within the Gartner clients in APAC region. It continues to maintain a strong channel presence in the region.

In APAC, SonicWall's regional data centers for its cloud-based services are in Tokyo.

Language support: In addition to English, it also offers its management console in Japanese, simplified Chinese and traditional Chinese. It also offers product documentation in Korean.

Technical support: It has three regional technical support centers in APAC in China, Japan and India. SonicWALL offers technical support in Chinese, Japanese and Korean, along with English.

Sophos

Sophos is not traditionally a large player in the Asia/Pacific region for network security, but with its February 2014 acquisition of India-based Cyberoam, it has bolstered its presence in the region, especially South Asia. It has a strong presence of vendor sales engineers and channel partners in the region. Its network security capabilities are complemented by its other endpoint and content security offerings.

In the APAC region, it has its data centers of Sophos eXtensible List (SXL) servers (i.e., anti-spam database) hosted in Japan, Singapore and Australia. It also has its cloud web gateway data centers located in multiple countries in the APAC region.

Language support: It offers its management console in Korean, Japanese, Chinese and Hindi along with English. It also offers documentation in Japanese.

Technical support: Sophos has four regional technical support centers in APAC: in Australia, the Philippines, Japan and India, where they offer support in traditional Chinese, Mandarin and Japanese.

WatchGuard

WatchGuard provides a portfolio of network security offerings, and its regional presence in terms of the Asia/Pacific customer mix is about on par with its competitors from outside the region.

In the APAC region, WatchGuard has data centers for its WebBlocker URL database hosted in Hong Kong and Australia. And spamBlocker cloud is hosted in India and Hong Kong.

Language support: WatchGuard offers a management console and documentation in Japanese.

Technical support: WatchGuard has one regional technical support center in the APAC region, located in Japan. Along with English, it offers support in Chinese and Japanese.

Evidence

This Magic Quadrant was conducted in accordance with Gartner's well-defined methodology. The analysis in this research was based primarily on interviews and interactions during firewall inquiries with Gartner clients since the 2014 "Magic Quadrant for Enterprise Network Firewalls." We also considered surveys completed by vendors, vendor briefings conducted at the request of vendors throughout the year, interviews with references provided by vendors and supporting Gartner quantitative research on market share.

Guidelines for responding to the full survey were provided at the time of issue. Responses were, nevertheless, of variable quality. Responses that were lower quality (for example, respondents ignored the question, used poor grammar, were unable to explain key concepts, were unable to provide high-quality explanations of use cases, or were unable to go beyond technical capabilities and demonstrate an understanding of the business environment), or that did not meet the guidelines, generally tended to score lower. Vendors that declined to provide a survey response were assessed by Gartner as to what their likely reply would have been (usually, this was in relation to specific revenue breakdowns). Some vendors declined to answer certain questions due to market restrictions, and, therefore, did not fare as well under some of the scoring criteria.

We asked for a specific number of references from each vendor (n = 95), and each reference customer was supplied with a structured survey. References were scored on the basis of their quality and what they told us. For each vendor, we took into account the comments from that vendor's references, as well as what other vendors' customers said about that particular vendor. Vendors could be notably affected by the inability to have a sufficient number of reference customers providing input.

Note 1
Buyer Confusion Concerning WAFs

The advent of application control in firewalls has led to some natural confusion between the NGFW and WAF markets in the minds of buyers. Today, these markets remain very distinct. The critical difference is one of direction: Application control in NGFWs is concerned primarily with applications that are external to the enterprise (for example, P2P and Facebook), whereas WAFs are concerned with protecting custom web applications on servers that are internal to the enterprise. Although a few firewalls offer optional WAF modules, these are rarely enabled. Instead, we see WAFs deployed as a stand-alone product (such as from Imperva), an off-premises service (such as from Akamai) or within an ADC (such as from F5).

Note 2
Network Security Policy Management Tools

Third-party network security policy management (NSPM) tool vendors (such as AlgoSec, FireMon and Tufin) continue to exploit the absence of firewall consoles to optimize, visualize and reduce firewall rules and policies. Although the NSPM market is still somewhat small, it's growing fast, and the customers requiring help with complexity are the very largest. Additionally, very large enterprises may have firewall products from different vendors — sometimes by accident via acquisition rather than through choice, because a single-vendor

solution is usually the best choice. In other cases, an enterprise may be in the midst of a multistage rollout of a new platform. Enterprises that deploy some their infrastructure to the public cloud may choose to use native cloud firewalls there, in addition to maintaining the incumbent firewalls in the physical infrastructure. All NSPM vendors support multiple firewall products (including, in some cases, cloud-resident firewalls), whereas no firewall vendor will effectively manage a competing product. In addition, NSPM vendors are expanding into managing other network security devices, such as IPSs.

Note 3
Types A, B and C Enterprises

Enterprises vary in their aggression and risk-taking characteristics. Type A enterprises seek the newest security technologies and concepts, tolerate procurement failure, and are willing to invest for innovation that might deliver lead time against their competition; this is the "lean forward" or aggressive security posture. For Type A enterprises, technology is crucial to business success.

Type B enterprises are "middle of the road." They are neither the first nor the last to bring in a new technology or concept. For Type B enterprises, technology is important to the business.

Type C enterprises are risk-averse to procurement, perhaps investment-challenged and willing to cede innovation to others. They wait, let others work out the nuances and then leverage the lessons learned; this is the "lean back" security posture that is more accustomed to monitoring rather than blocking. For Type C enterprises, technology is not critical to the business and is clearly a supporting function.

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.