Magic Quadrant for Enterprise Network Firewalls

25 May 2016 | ID:G00277994

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

Summary

"Next generation" capability has been achieved by the products in the network firewall market, and vendors differentiate on feature strengths. Buyers must consider the trade-offs between best-of-breed function and costs.

Strategic Planning Assumptions

Virtualized versions of enterprise network safeguards will reach 10% of market revenue by year-end 2019, up from less than 5% today.

Less than 50% of enterprise internet connections today are secured using next-generation firewalls (NGFWs). By year-end 2019, this will rise to at least 90% of the installed base.

By 2018, 85% of new deals for network sandboxing functionality will be packaged with network firewall and content security platforms.

Market Definition/Description

This document was revised on 10 June 2016. 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.

The enterprise network firewall market represented by this Magic Quadrant is 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) 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. 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.

The companies that serve this market are identifiably focused on enterprises — as demonstrated by the proportion of their sales in the enterprise; 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

NGFWs have added new features to better enforce policy (application and user control) or detect new threats (intrusion prevention systems [IPSs], sandboxing and threat intelligence feeds). The NGFW continues 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). More recently, enterprises have begun 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 "Market Guide for Network Sandboxing").

However, next-generation 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").

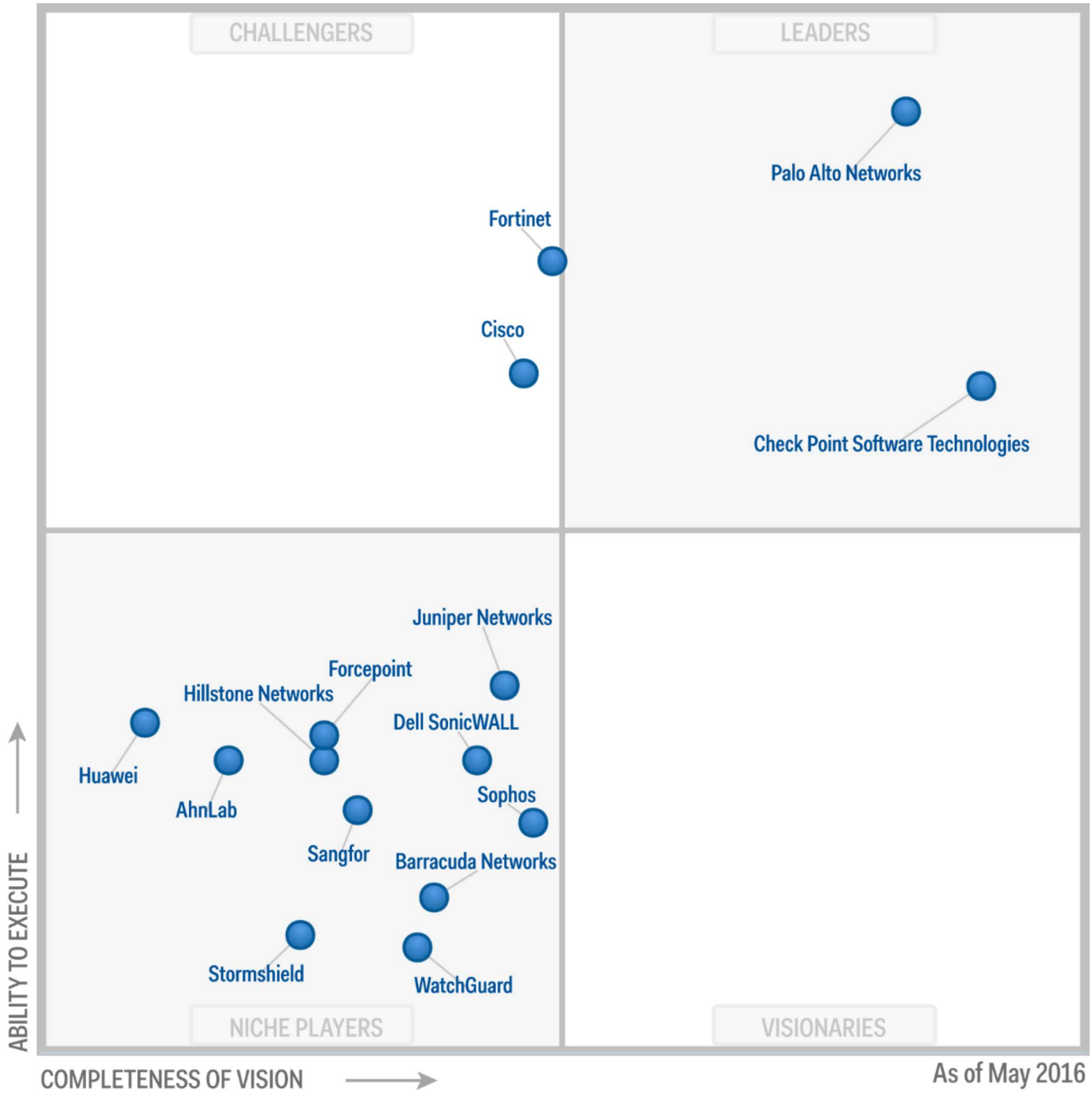
The needs for enterprise branch-office firewalls are becoming specialized, and they are diverging from, rather than converging with, UTM products. As part of increasing the effectiveness and efficiency of firewalls, branch office firewalls will need to truly integrate a more granular blocking capability 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 Secure Sockets Layer (SSL) termination, acting as a lightweight DLP tool as they decrypt and inspect outbound traffic to ensure that sensitive data is not wrongly sent out. However, customers who enable this capability are frustrated by the substantial performance burden that in-firewall SSL 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.

Magic Quadrant

Figure 1. Magic Quadrant for Enterprise Network Firewalls



Source: Gartner (May 2016)

Vendor Strengths and Cautions

AhnLab

AhnLab (http://global.ahnlab.com/site/main.do) , headquartered in South Korea, is a network and endpoint security vendor. It is a long-established endpoint security vendor, and has sold firewalls since 2007 under the TrusGuard product line name. It offers 11 UTM and firewall models for SMBs and enterprises. The AhnLab product portfolio includes firewalls, advanced threat defense, distributed denial of service (DDoS) attack mitigation and endpoint security solutions. It also offers managed security services and forensic and incident response services.

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).

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

AhnLab is assessed as a Niche Player because of limited regional presence in Asia, which is, again, not very strong other than in South Korea. Most of its firewall wins are associated as a part of endpoint security deals. AhnLab firewalls lack in some important features (SDN support, multiple virtual firewall support, public cloud deployment support) that are provided in most other vendors' firewalls and are significant for enterprise customers.

STRENGTHS

AhnLab is an established endpoint and network security player in South Korea, with significant local sales and support presence. Hence, it is a good shortlist candidate for clients based in South Korea looking for a local vendor with regional support and services.

AhnLab is one of a few East Asian vendors with a local certification, which is significant in South Korea.

AhnLab 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

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.

The TrusGuard firewalls do not provide support for SDNs. They also do not support public cloud deployments. These two features are provided by most of the other firewall vendors, including the major local Asian vendors.

AhnLab does not offer virtual firewall models.

Barracuda Networks

Campbell, California-based Barracuda Networks (https://www.barracuda.com/) is a long-established security and storage vendor that is particularly suitable for midsize businesses and small-enterprise markets. Its product portfolio includes storage and application delivery solutions, along with a broad range of security solutions, which include email security, secure web gateway (SWG), web application firewall (WAF), firewalls and SSL VPN.

The Barracuda enterprise firewall offering is the NextGen Firewall (NGF) F-series with 11 models, whereas the NextGen Firewall X targets SMBs. Barracuda also sells firewalls to connect remote operational devices, such as ATMs and kiosks, with the NGF S-series. Barracuda is frequently seen as a firewall deployed within Microsoft Azure public cloud environments.

Barracuda partners with Lastline to provide its customers the option for cloud-based sandbox advanced threat detection. The NGF virtual firewalls provide support for AWS, Microsoft Azure and VMware vCloud Air. The Barracuda NextGen Firewalls are certified by ICSA Labs and Virtual Private Network Consortium (VPNC), and are evaluated by NSS Labs, but do not have other third-party certifications such as Common Criteria Labs or FIPS PUB 140-2.

Barracuda is assessed as a Niche Player because it has majority of its presence in Western and Central Europe and North America, with proportionally less presence in other regions. In addition, the company does not have a strong enterprise channel.

STRENGTHS

The Barracuda NextGen Firewall is a good option for customers that already have other Barracuda products, to avoid the complexities of multivendor relationships.

The Barracuda management console scores well in selections where ease of use is weighted heavily. The NGF's graphical VPN also scores well for the ease of setting up VPN connections and monitoring them.

The Barracuda NGF is a strong competitor in situations where price is highly weighted in the selection. Barracuda customers indicate that high availability and clustering capabilities were also key reasons they selected the NGF.

Barracuda has established good early presence in public cloud deployments, particularly in Microsoft Azure environments.

CAUTIONS

Barracuda customers are primarily SMBs, and the vendor does not yet have well-established enterprise network security channels or support outside of Western and Central Europe.

Barracuda NGFs do not provide support for SDN implementations.

No vendor we surveyed listed Barracuda as a significant enterprise competitive threat. Although we see Barracuda Firewall in SMB deals, Barracuda has low visibility on the firewall shortlists of Gartner enterprise customers, except in some regions, notably Germany and Austria. Most interest has come from incumbent customers that have other Barracuda products.

Check Point Software Technologies

Co-headquartered in Tel Aviv, Israel, and San Carlos, California, Check Point Software Technologies (http://www.checkpoint.com/) is a large security vendor providing a variety of solutions, including next-generation firewalls, endpoint and mobile security solutions. 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 Blades) 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.

In early 2015, Check Point announced its R80 major release and conducted a year-long beta program through the end of the first quarter of 2016, at which time it was released.

Check Point is assessed as a Leader for enterprises because of its steady presence in enterprise shortlists visible to Gartner, its high renewal rate from its existing client base and the strong execution on its enterprise-focused roadmap. The vendor also continues to innovate on its already strong management and reporting capabilities, and, as a result, is often the firewall of choice for complex firewall policy environments. It also innovates security, with new features such as Threat Extraction.

STRENGTHS

Check Point continues to drive a very high number of Gartner client inquiries, both from existing clients willing to expand their use of the technology with new features, and for prospective customers with complex deployments or looking for high security.

The vendor often gets stronger scores than other vendors during competitive evaluation for its management capabilities, especially when supporting complex deployments, deployments by very large enterprises, and organizations that need formal approval workflow or have large operation teams. It very rarely gets displaced based on features when it is the incumbent provider. Trust in Check Point's brand also attracts large conservative customers in search of a mature solution.

Check Point's large R&D allows it to bring new, unique capabilities, such as Threat Extraction, and to sustain continuous improvement on its existing strengths, such as the recent firewall policy management overhaul included in R80. Check Point is not always first to market, but when a new feature is released, it often goes deeper than its competitors' first releases.

Its comprehensive portfolio includes in-depth coverage for use cases that are considered too niche for many of its competitors, including a ruggedized firewall for industrial control system (ICS) requirements, with support for many supervisory control and data acquisition (SCADA) protocols, a dedicated software option providing detail reports for many compliance standards, and support for multiple software-defined networking SDN platform standards. Check Point has a very well-developed third-party ecosystem for security information and event management (SIEM), threat intelligence and firewall policy management.

CAUTIONS

Check Point's policy to include for free a few one-year subscriptions for Software Blades when purchasing a new appliance has generated the most vocal complaints from customers at renewal time, despite what was, in theory, a good way for the vendor to let its clients test new subscriptions. It often results in unexpectedly high renewal costs, taking customers by surprise, due to a lack of clear, consistent communication on the first-year software discount from the reselling partner.

Gartner analysts frequently observe that, despite the availability of an online sizing tool, hardware platforms submitted in reseller proposals tend to be more tightly sized, and see this as a tactic to control total costs. In some reported client situations, undersizing was a clear reason for performance issues, and caused unnecessary back-and-forth discussion to get the adequate model.

Gartner receives anecdotal reports from clients about support issues, mostly focused on the time it might take to get appropriate escalation. Gartner analysts recognize that this is inevitable for a vendor of this scale, but note that the frequency of issues is, of late, slightly higher than its direct competitors. Check Point has recently extended the support quality metrics it monitors to address this issue and monitor its progress.

Check Point has been offering firewall integration with its mobile security suite (Check Point Capsule), and, in February 2016, threat prevention endpoint (SandBlast agent), but Gartner does not observe a strong interest from its firewall customers to purchase either solution. Similarly, the adoption of Check Point cloud-based sandboxing option is slower than cloud sandboxing is for its direct competitors.

Gartner believes Check Point underperforms in marketing and brand recognition. Although incumbent Check Point clients are well-informed, new clients rarely know Check Point product names or are aware that Check Point has certain features when speaking with Gartner, yet these same clients are familiar with competitors' features and product names.

Cisco

San Jose, California-based Cisco (http://www.cisco.com/) has a broad network security product portfolio across firewall/IPS, web security, email security, endpoint security and other security tiers. The enterprise firewall offering is delivered primarily via the Adaptive Security Appliance (ASA) brand. ASA with FirePOWER services is the ASA with the Sourcefire IPS, Advanced Malware Protection (AMP) and application visibility and control added in. Cisco's virtual firewalling lines include the Adaptive Security Virtual Appliance (ASAv) and the Virtual Security Gateway (VSG).

FireSIGHT is the new management platform intended to replace Cisco Security Manager (CSM). Some in-service ASA appliances do not support FireSIGHT for complete management, so some clients should expect to have to maintain CSM as part of one firewall replacement life cycle.

Gartner sees Cisco winning firewall procurements mostly through sales/channel execution, usually where there is already a strong Cisco networking relationship, or on shortlists for verticals where total cost of ownership (TCO) is weighted heavily or where there are many distributed offices. Cisco Advanced Malware Protection (AMP) for networking has been mentioned frequently by Gartner clients.

Cisco is assessed as a Challenger for enterprises. Gartner did not see it often displacing Leaders based on vision or features, and in Gartner's opinion, Leaders have not been forced to react to firewall innovations from Cisco.

STRENGTHS

The enterprise license agreement (ELA) for security software and hardware adds value for Cisco security customers that are undertaking multiyear deployments and wish to maintain a timetable and product flexibility.

Gartner clients consistently rate the Cisco support network as excellent, and it is the most often-cited reason for loyalty to Cisco security products. The vendor has strong channels, broad geographic support and wide availability of other security products. Surveyed Cisco firewall clients consistently ranked the availability and presence of other products from Cisco within their networks as the most important factors in their selection of the vendor.

The inclusion of Sourcefire IPS within ASA along with a single management console for both firewall and IPS is positive, especially for incumbent clients.

Unlike some of its competitors, Cisco, with its ASAv, supports very heterogeneous cloud environments, including VMware, Kernel-Based Virtual Machine (KVM), Microsoft Hyper-V and Amazon Web Services.

CAUTIONS

Gartner clients select Cisco firewall products more often when firewall offerings are added to a Cisco security infrastructure, rather than when there is a shortlist with competing firewall appliances.

Gartner clients like the direction with FireSight security functionality, but comment frequently that the firewall management still needs improvement.

Some ASA appliances still oblige customers to use Cisco Security Manager to manage them, adding to complexity with a second management platform.

In the survey sent to enterprise firewall vendors, Cisco's product was the second most frequently listed as the one vendors claimed to replace the most; however, it was also listed this year as No. 2 in the vendor list of perceived competitive threats.

Dell SonicWALL

Based in Round Rock, Texas, Dell has a broad portfolio of computers, network devices and service offerings. Since its acquisition of SonicWALL in 2012, Dell sells enterprise firewalls under the Dell SonicWALL (http://www.sonicwall.com/) name. Dell SonicWALL firewall portfolio comprises the TZ Series for small offices and branches; the NSA Series, aimed at midmarket clients; and the SuperMassive Series for larger enterprises and data center deployments. Dell SonicWALL firewalls also provide integration with the brand's wireless access points, WAN optimization products and Dell X-Series switches.

Dell SonicWALL is assessed as a Niche Player for enterprises, because it does not typically win in competitive evaluations by the enterprise and large data center segments, and has limited visibility in enterprise shortlists, especially outside of the U.S.

STRENGTHS

Surveyed customers frequently mention the ability for Dell SonicWALL product to meet budget and performance requirements. They also give good scores to vendor support quality.

Gartner clients observe manageability improvement with the GMS version 8 release.

Dell SonicWALL recently released a beta version of its cloud-based sandboxing subscription that leverages multiple engines in parallel and offers support for Mac OS.

Dell SonicWALL recently entirely refreshed its TZ Series with increased performance. It no longer requires a subscription to get SSL decryption features.

CAUTIONS

Since Dell announced it will acquire EMC and make Dell SecureWorks public, Gartner believes that Dell may lose focus on SonicWALL. While SonicWALL as an organization was an autonomous entity not so long ago, Gartner cautions that, in general, deep organizational changes can slow down a vendor's development efforts, and can distract channel and sales forces.

Dell SonicWALL cloud security is less mature than its leading competitors, especially in its ability to inspect JavaScript to provide visibility on SaaS usage.

Dell SonicWALL lacks SDN integration and provides limited interoperability with infrastructure as a service (IaaS) platforms. Consequently, the vendor is not visible on Gartner client shortlists for internal data center segmentation of east-west traffic, or in software-defined perimeter use cases.

Forcepoint

Forcepoint (https://www.forcepoint.com/) was recently created in 2015 by Raytheon and Vista Equity Partners as a joint venture that combined Websense and Raytheon Cyber Products (and the more recently acquired firewall business from Intel/McAfee). Forcepoint's offerings include SWGs, data loss prevention (DLP), secure email gateways, network sandboxing, user and entity behavior analytics (UEBA), and security analytics. The portfolio is backed by a common threat intelligence platform. The Forcepoint Stonesoft NGFW brand is the firewall formerly owned by Stonesoft, later by Intel McAfee. The firewall product has a good range of models (scaling up to 120 Gbps), including a virtualized version, and has performed well in third-party testing.

In addition, Forcepoint has another line of firewalls, Forcepoint Sidewinder, targeted toward the U.S. federal government. This firewall is developed and supported separately from Stonesoft.

Forcepoint Stonesoft NGFW is assessed as a Niche Player for enterprises. It is a good NGFW, and will hopefully will enter a period of stability under Forcepoint; however, Gartner believes a succession of acquisitions and brand name changes have slowed product progress. Gartner believes the Forcepoint Stonesoft NGFW will primarily sell alongside other Forcepoint security products, rather than beating Leaders in shortlists.

STRENGTHS

The Stonesoft firewall is a good contender for current Forcepoint SWG clients that value a single vendor relationship. We expect this positioning to be stronger in the future, with some integration between products .

The Stonesoft firewall has long been a leader in high-availability technology, and it has very reliable clustering and active/active configuration, and a high throughput rate of SSL/Transport Layer Security (TLS) termination.

Stonesoft focused early on anti-evasion technology, and as attacks evolved, it protected customers well by including firewall and deep inspection evasiveness.

With R&D mostly in Europe, the firewall is a good option for EMEA enterprises and governments.

CAUTIONS

Gartner believes that Forcepoint may be more focused on U.S. federal sales than its competitors, but a firewall known as being made in Europe will not resonate as well with the current Forcepoint/Raytheon base.

Although the company has rebranded, its association with Raytheon may cause some customers outside the U.S. to hesitate to move forward with Forcepoint Stonesoft.

Forcepoint partners with Intel Security for important capabilities such as threat intelligence (Threat Intelligence Exchange) and cloud-based advanced threat detection (Advanced Threat Defense). Gartner advises Forcepoint customers to monitor these capabilities carefully to ensure that the capabilities remain fully integrated and useful with Forcepoint firewalls.

Forcepoint is a new brand name in a mature market, and is rarely seen on Gartner client network firewall shortlists.

Fortinet

Fortinet (https://www.fortinet.com/) is a network security vendor that is headquartered in Sunnyvale, California. FortiGate, its main product line, serves as a firewall for enterprise's service providers and SMBs. Its product portfolio also includes endpoint protection, web application firewall and wireless access points. Fortinet has leveraged hardware design expertise to continually improve purpose-built firewall appliances, relying on a combination of its sixth generation of Network Processor (NP6) to accelerate packet processing, a ninth generation of Content Processor (CP9) for deep packet inspection and off-the-shelf CPUs.

Fortinet's presence is strong across all regions, with a very large channel and heritage from its long history with SMB organizations. Fortinet is quickly gaining market share in the enterprise firewall market, being outpaced in growth only by Palo Alto Networks. For enterprise deployments, Fortinet is no longer constrained to distributed organizations and data center use cases. It is frequently cited in enterprise firewall shortlists within the Gartner customer base.

Fortinet is assessed as a Challenger because the most frequent reason for displacing its leading competitors is its better price. Fortinet also struggles to convince enterprise buyers on vision because of its competitive focus on price and performance strengths, rather than on the creation of new capabilities as a result of a unique vision on how to meet the future needs of enterprise firewall customers.

STRENGTHS

Fortinet frequently wins customers because it can offer similar features with better performance than its competitors while meeting budget expectations.

Gartner clients praise Fortinet's hardware quality, and frequently cite good channel support as a decisive reason for renewing with Fortinet.

Fortinet's enterprise wins across several verticals have helped built a stronger base of enterprise peer references, especially in the EMEA and Asia/Pacific regions, where Fortinet is more frequently cited in the final firewall shortlist.

The vendor provides a cost-effective alternative to a sandboxing subscription with its FortiSandbox appliance, which can be shared across branch firewalls and used by other Fortinet products.

FortiView, the recent evolution of Fortinet's reporting solution, includes promising features with easy drill-down from top view to detailed events, and the ability to build custom reports at large scale.

CAUTIONS

Surveyed clients frequently mentioned issues or unexpected user experience changes when upgrading firmware. They also report that new features might have unequal quality.

In a competitive assessment, Fortinet's sandboxing subscription received mixed reviews from Gartner clients for its detection rate.

FortiManager, despite its ability to operate at large scale and the recent addition of policy workflow support, still has not achieved a reputation for ease of use.

Fortinet can't leverage the advantages conferred by its purpose-built hardware in SDN and other software deployment use cases, such as IaaS. This might explain why it has very low visibility in competitive evaluations where these use cases are prominent.

While Fortinet's marketing mix became much more enterprise-focused in 2014 and has remained so, previous UTM-oriented marketing has created a lingering brand disadvantage with some enterprise security buyers.

Hillstone Networks

Based in Beijing and Sunnyvale, California, Hillstone Networks (http://hillstonenet.com/) is a pure-play security vendor. With 23 firewalls offered on a global basis and 47 offered in China, Hillstone's firewall portfolio is composed of three product lines — T-Series (intelligent NGFW), E-Series (NGFW) and X-Series (data center firewall) — with firewall throughput ranging from 1 Gbps to 360 Gbps. Hillstone has added network behavior anomaly detection into its firewall, and now offers virtual versions of CloudEdge, for virtual data center and public cloud support, and CloudHive, a virtual east/west microsegmentation solution.

Although it has laid some groundwork to increase sales in more regions by expanding its worldwide partner ecosystem, Hillstone is assessed as a Niche Player because it is visible to Gartner only in one region, with a majority of its sales in China.

STRENGTHS

Hillstone has a strong presence in China, and offers dedicated firewall models for this market. Surveyed customers in China give good scores to direct vendor support.

Chinese customers indicate that they like that Hillstone offers a functional virtual firewall, unlike many of its regional competitors.

Hillstone's recent release of the CloudHive east-west cloud microsegmentation solution indicates a motivation to bring further innovation to the enterprise firewall market.

Hillstone integrates with FireMon and AlgoSec policy management software, which can facilitate purchase decision for international companies willing to use a local vendor in the Asia/Pacific region.

CAUTIONS

Hillstone Networks' firewalls are not yet seen in enterprise selections among the Gartner client base outside of Asia/Pacific. Gartner also observes increasing competition for Hillstone in China from local and regional vendors.

Though they like that Hillstone has a virtual firewall, surveyed customers indicate that it is not at feature parity with the physical version.

Surveyed users still cite management interface as an area that requires improvement.

Huawei

Shenzhen, China-based Huawei (http://www.huawei.com/en/) 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 that business to firewalls. Unified Security Gateway (USG) is the primary enterprise line, and Eudemon is the model line for carriers and service providers. 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 service gateway to implement virtual multitenant separation.

Huawei is assessed as a Niche Player for enterprises over the evaluation period, because we see it mostly in a narrow geographic segment, and because we did not see it frequently displacing Leaders or Challengers based on vision or features.

STRENGTHS

Customers whose networks are based primarily on Huawei infrastructure products can include Huawei firewalls, especially in the Asia/Pacific region where the majority of sales occur. Huawei customers like that firewalls are well-integrated with Huawei's infrastructure components.

Most appliance models offer a great variety of port configuration option mixes of Gigabit Ethernet (GbE), 10GbE and small form-factor pluggable (SFP).

The top end of the Huawei firewall line has a very high throughput, and is a good shortlist candidate for carriers and service providers. Most Huawei firewall deployments Gartner observes are higher-throughput deployments.

Huawei has put extensive effort into achieving firewall certifications.

CAUTIONS

Huawei has limited competitive visibility outside the Asia/Pacific region; however, there is some increasing competitive presence and growth in EMEA.

Interviewed users consistently asked for better reporting.

Huawei 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.

Huawei does not have embedded or cloud-based advanced threat detection, and cloud-based sandbox options are not available.

Juniper Networks

The SRX Series firewall offerings of Sunnyvale, California-based Juniper Networks (http://www.juniper.net/us/en/) comprise 28 different hardware models, and the virtualized version of SRX (vSRX). The Juniper SRX Security Service Gateway offers routing as a basic firewall element, and runs the same Junos operating system as other Juniper infrastructure components. Gartner considers advanced routing in the firewall to be of interest to a very limited segment of customers. Juniper has AppSecure for application control and visibility, integrated IPS, threat intelligence feeds (called Spotlight Secure), and a new cloud-based malware sandbox (Sky ATP). Juniper's Junos Space Security Director is the current security management platform. While very late to market, Juniper has also recently released a significant update to its firewall range, bringing them closer to feature parity to the majority of the market in terms of NGFW features.

Juniper is assessed as a Niche Player for enterprises, mostly because we see it selected in concert with other Juniper network infrastructure offerings and it is less expensive than competitive alternatives. In addition, Juniper does not displace competitors based on its vision or features, and we continue to see it replaced in enterprise environments more often than we see it selected. Juniper is, however, shortlisted and/or selected in mobile service provider deployments and large-enterprise data center deployments primarily because of price and high throughput on its largest appliances.

STRENGTHS

Customers whose networks are already standardized on Juniper's Junos-based infrastructure products can benefit from the Space Security Director because it is part of the Junos Space Network Management Platform.

Good options exist for high-throughput, purpose-built appliances, especially in the higher-end SRX models, because Gartner sees Juniper mostly deployed in large data centers. The vSRX 2.0 offering is highly rated for performance relative to other virtual firewalls. Interviewed users often selected the firewalls with throughput as a highly rated criterion.

Juniper has a strong range of branch-office firewalls complementing the enterprise products. These branch-office firewalls include WAN and cellular backup technologies.

Juniper has articulated a strong SDN security story around vSRX and the Juniper Contrail SDN framework.

Juniper offers a threat intelligence service that also supports third-party threat intelligence feed integration. This now integrates with Juniper's Sky ATP cloud-based malware detection offerings. This integration will appeal to enterprises that want multiple threat intelligence feeds to help them identify emerging threats while being able to leverage their existing Juniper investments.

CAUTIONS

Gartner notes that Juniper has been late to market with various security functions and features; for example, Juniper's cloud-based malware sandbox solution was released in 2015, well behind most firewall vendors.

Juniper also lags competitors in such areas as public cloud support and VMware integration. As a result, Gartner clients lack confidence in Juniper's security vision.

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

Juniper has continued losing security market share in the past year, and has experienced declining year-over-year revenue in a growing market, though the situation began to stabilize in the second half of 2015. The company must more effectively address fundamental sales and marketing challenges and demonstrate that it can win back customers and market share with its newer capabilities.

Palo Alto Networks

Palo Alto Networks (https://www.paloaltonetworks.com/) is a Santa Clara, California-based pure-play security company that has been shipping enterprise firewalls since 2007. Palo Alto Networks is known mostly for its innovations in application control, for improving integrated IPS in firewalls and for introducing cloud-based malware detection to the NGFW space. The firewall product line includes 19 models, with a maximum throughput of 200 Gbps for the PA-7080, released in 2015. With the acquisition of Cyvera (rebranded as Traps), Palo Alto Networks now offers a second endpoint product, in addition to the existing GlobalProtect. Palo Alto's malware analysis environment, WildFire, a component of its Threat Intelligence Cloud, continued to see high attach rates for new and existing customers in 2015. Palo Alto Networks' work with VMware NSX has provided customers another option for placing Palo Alto Networks products in virtualized data centers.

Palo Alto Networks is assessed as a Leader mostly because of its NGFW focus and its record of delivering NGFW features ahead of competitors, and because of its consistent visibility in Gartner shortlists for advanced firewall use cases, frequently beating its competition on feature granularity and depth.

STRENGTHS

Quality and ease of use for the Palo Alto Networks App-ID and IPS are the two most-cited factors cited for selecting Palo Alto Networks over other competitors.

The firewall and IPS are closely integrated, with App-ID implemented within the firewall and throughout the inspection stream. This "single pass" is assessed as a design advantage by Gartner clients, as opposed to the unnecessary inspection time that can occur in competing products that process traffic in serial order.

In the survey to vendors, Palo Alto Networks was most-mentioned as the strongest competitor. Palo Alto Networks consistently continues to appear on most NGFW competitive shortlists seen by Gartner.

The roadmap focus on extending the VM server into multiple cloud and SDN frameworks displays strong leadership toward solving clients' future problems. Palo Alto shifted focus correctly to east-west segmentation, rather than whole data center firewall virtualization.

The WildFire advanced threat cloud service is a popular add-on with new and incumbent Palo Alto Networks firewall customers, providing them an option versus third-party advanced threat appliance solutions.

CAUTIONS

Palo Alto Networks lagged behind other leading vendors in producing a virtual firewall version for Microsoft Azure deployments.

Like other vendors with leading products, Palo Alto Networks is challenged to win selections in which price is weighted more than security features, as in Type C enterprises (see Note 1). Palo Alto has one of the highest prices per protected gigabit of any enterprise firewall vendor.

Gartner clients have noted the need for better log handling at scale and more effective active/active high availability. Palo Alto management is cited as good, and beats Challengers; however, Gartner does not see Palo Alto beating other Leaders in deals in which security management is highly weighted and involves a hands-on evaluation.

Gartner has still not seen Palo Alto reproducing its firewall success with its entry into the endpoint market. Gartner hears from few clients who use Traps, and see Traps in few new deals. The endpoint is more effectively addressed through Palo Alto's third-party ecosystem. Gartner believes that Palo Alto's focus on the endpoint sometimes alienates the network operations buying center, and could prove a distraction to Palo Alto's core business — network security.

Sangfor

Headquartered in Shenzhen, China, and founded in 2000, Sangfor (http://www.sangfor.com/) provides WAN optimization, access management and network security solutions, including firewall, SSL VPN, and internet access management. Sangfor started shipping its enterprise firewall product line (Next Generation Firewall) in 2011. The Next Generation Firewall integrates WAF functionality in its enterprise firewall, the Next Generation Application Firewall (NGAF)

Platform, a unique feature among the vendors evaluated. It now features 16 models, for a firewall throughput of up to 80 Gbps. Sangfor released several new product enhancements in 2015, including heuristic anti-malware, full SSL inspection, automated threat intelligence service and a virtual NGAF.

Sangfor has support for AWS public cloud, and it has some SDN capabilities.

Sangfor is evaluated as a Niche Player for enterprise firewall because it serves a narrowed segment of the market and operates mostly in China.

STRENGTHS

- Sangfor clients like the ease of installation, the reporting on security and high performance, and price.
- Surveyed customers cite presence of WAF as a primary criterion for selecting the Next Generation Firewall.
- Cloud-based sandboxing and active vulnerability scanning are available on Sangfor's firewall at no additional charge.

CAUTIONS

- Gartner does not see Sangfor firewalls being shortlisted outside of China. Internationalization of the Sangfor firewall product line is still an ongoing process.
- 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's enterprise firewall is new compared with most of its competitors, and several features are still unproven, but with a quickly growing number of deployments. Virtual firewalls, first launched in 2015, have limited history and market uptake.

Sophos

Sophos (http://www.sophos.com/) is a security company headquartered in Oxford, U.K., that initially entered the security market as an endpoint security vendor. Today, its product portfolio consists of a range of network, endpoint, gateway and server security solutions.

Sophos sells its enterprise firewall portfolio as the Sophos XG Series and also as Cyberoam Next-Generation (NG) and ia Series. Sophos XG Series includes 16 models (11 models for enterprise and SMBs and five desktop models). Cyberoam NG series has six models for enterprises, and ia Series has three main models. Sophos also offers SG series of UTM firewalls. Sophos firewalls are available in software/virtual format and can run on AWS.

The Sophos XG firewalls are certified by ICSA Labs and German Common Criteria, and NSS Lab-tested. Sophos appliances also have regional certifications from multiple countries, as per their local standards. It is not FIPS-certified.

Sophos' Niche Player position in this Magic Quadrant reflects its focus on upper-midmarket and smaller enterprises, in combination with the limited visibility for Sophos firewalls on data center and larger enterprises' shortlists.

STRENGTHS

With the new XG models including enhancements from the acquired Cyberoam firewalls, Sophos has an improved centralized manager called Sophos Firewall Manager (SFM). The SFM comes free of charge to Sophos partners, while to the end customers it is free to manage up to five devices.

With the integration of iView (Cyberoam's logging and reporting solution) into the XG firewall series, the existing reporting features have been updated and enhanced.

Sophos Central Cloud management combines mobile, endpoint, web, server and network management, and appeals to vastly distributed enterprises and organizations with a large mobile workforce. Enterprises that already have the Sophos endpoint products deployed should shortlist the Sophos firewall.

Sophos is growing in the market in AWS cloud deployments, and is a frequent selection for AWS-only placements.

CAUTIONS

Sophos maintains multiple product lines for enterprise firewalls. Clients shortlisting the Cyberoam firewall series should ensure the continuity of support and services for the devices for the complete duration of their usage, and have clarity about the roadmap of feature enhancements on these models.

Sophos XG firewalls do not offer support for SDN environments.

No vendor we surveyed listed Sophos as a significant enterprise competitive threat. Although we see them in upper midsize deals as a part of existing Sophos endpoint customers, Sophos is not visible on the firewall shortlists of Gartner enterprise clients. Gartner assesses this as being part of Sophos' strategy to focus on the midsize business, and those enterprises having similar security capabilities as midsize businesses.

Stormshield

Based in France, Stormshield (https://www.stormshield.eu/) results from the merger of two 15-year-old French security providers (Arkoon and Netasq) in 2014. It primarily provides UTM and enterprise firewalls to EMEA organizations with its Stormshield Network Security appliances. Its portfolio also includes host IPS (Stormshield Endpoint Security) and data-at-rest encryption software (Stormshield Data Security). The vendor also provides virtual firewall appliances for AWS and Microsoft Azure IaaS platforms. For log management and reporting, Stormshield offers a virtual appliance built on the Elasticsearch, Logstash and Kibana (ELK) stack, and a cloud subscription (Stormshield Network Cloud Reporting).

While it is still easy to find remnants of the former product lines, the new Stormshield brand is consistently used and clearly defined across all the product lines. Airbus Defence and Space Cybersecurity, its mother company, collaborates with Stormshield by sharing its facilities and offering limited sales support.

Stormshield is assessed as a Niche Player for enterprises because it primarily serves clients in Western Europe, and its investor commitment and good growth do not convert into accelerated roadmap execution or more innovations for enterprises.

STRENGTHS

Once limited in its ability to compete in larger environments, Stormshield firewalls now provide appliances that can scale up to 130 Gbps.

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.

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.

Surveyed clients cite good performance with IPS enabled, Internet Protocol Security (IPsec) VPN and flexible pricing as reasons to select Stormshield.

CAUTIONS

Stormshield lags behind market leaders in some functional areas — how it integrates application control in the security policy and support of only a limited number virtual systems within a single hardware appliance. It just released a first version of cloud-based sandboxing in April 2016, but Stormshield lacks threat intelligence feeds, and has yet to build an offering for SDN use cases.

Large distributed organizations often cite centralized management as a competitive weakness. The vendor has massively invested in building a new centralized management solution, with a first version available to clients in the first half of 2016. The solution is still unproven, and further improvements might be needed to pass a competitive examination.

Despite being a longtime known issue for Stormshield, Gartner clients continue to mention that the integrated IPS engine initially triggers a lot of false alerts and requires a lot of fine-tuning. The most experienced Stormshield resellers proactively handle this issue with custom profiles, but many clients outside of France still mention false positives as the main reason for unsuccessful proof of concept.

Even though Stormshield gets support from the large Airbus Defence group, the majority of Stormshield's penetration, visibility and channel remains focused on EMEA, especially France.

Gartner believes that Stormshield's emphasis on the integration between its network and endpoint solutions (multilayer collaborative security) could work with midmarket organizations, but creates an additional burden for enterprises evaluating Stormshield's firewalls.

WatchGuard

WatchGuard (http://www.watchguard.com/) is a Seattle-based network security company that has primarily seen success in selling UTM products to midsize enterprises. Its XTM Firebox M series of products spans performance and feature ranges demanded by large enterprises; however, WatchGuard's branding, channel support and management capabilities tend to be more oriented toward SMBs, which are served by WatchGuard's Firebox T Series. WatchGuard also has products that include SSL VPN, email and web security.

Since WatchGuard's introduction of the "NGFW Bundle" option for appliances in 2011, and the 2014 release of APT Blocker (WatchGuard's cloud-based malware detection offering using Lastline technology), the company has solutions that better suit prospective enterprise buyers than the UTM-only approach, though we still have not seen much enterprise uptake (aside from distributed enterprises).

WatchGuard is assessed as a Niche Player for enterprises, mostly because it more often serves SMBs and distributed enterprises. We do not often see it displacing Leaders for the edge firewall use case based on features, and do not see it developing innovative features ahead of its enterprise firewall competitors.

STRENGTHS

WatchGuard's strong price/performance points have enabled it to win price-sensitive competitions across retail, branch office, remote office and Type C distributed enterprise deployments. Surveyed users report high satisfaction with value received.

WatchGuard continues to invest in enterprise use cases, with enhanced reporting. Clients report liking the Application Control visibility.

Users continue to report high satisfaction with the WatchGuard management console and with quality of customer support.

The cloud-based reporting solution WatchGuard Dimension, with its executive dashboard and traffic heat maps, is a good addition to the set of features that is targeting areas where many firewalls will be deployed, such as in franchises or retail stores. The interactive heat map view (FireWatch) is useful to quickly identify network issues created by a specific user or application.

CAUTIONS

WatchGuard is primarily focused on the SMB and distributed enterprises, meaning Gartner rarely sees them in most other enterprise use cases. Enterprise-class channels and support will need to be expanded if WatchGuard wishes to compete in a broader segment of enterprises. For example, WatchGuard does not have the option for large enterprises to deploy a WatchGuard resident engineer, a requirement for some enterprise deployments.

WatchGuard scored low as a significant enterprise competitive threat by the vendors we surveyed, and it has low visibility in Gartner's client base.

WatchGuard lags behind the Leaders in articulating a comprehensive data center strategy and in including SDN in its roadmap.

WatchGuard does not currently ship virtual models for deployment in AWS or Microsoft Azure.

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

Forcepoint was added the Magic Quadrant, as it acquired Intel Security's firewall business (the former Stonesoft and Sidewinder firewall lines).

Dropped

Intel Security (McAfee) was dropped from the Magic Quadrant, as its firewall assets were acquired by Forcepoint.

F5 was dropped, as it has chosen not to compete in the enterprise firewall market.

The HP TippingPoint network security business was bought by Trend Micro, which opted to begin the end of life (EOL) process for the TippingPoint firewalls, so HP was dropped.

Inclusion and Exclusion Criteria

Inclusion Criteria

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

- Gartner analysts have assessed that the company has the ability to effectively compete in the enterprise firewall market.
- The company regularly appears on shortlists for selection and purchases.
- The company demonstrates a competitive presence in enterprises and sales.
- Gartner analysts consider that aspects of the company'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 companies may have been excluded from this research for one or more of the following reasons:

- The company has minimal or negligible apparent market share among Gartner clients, or it is not actively shipping products.
- The company 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 company'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 company primarily has a network IPS with a non-enterprise-class firewall.
- The company has personal firewalls, host-based firewalls, host-based IPSs and WAFs (see Note 2) — 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 company'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 (May 2016)

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	Medium
Innovation	High
Geographic Strategy	Low

Source: Gartner (May 2016)

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 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 east/eest 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 changes in enterprise network speed and complexity. Firewalls have high adoption and penetration rates in all markets, with North America, Western Europe and mature Asia/Pacific leading. 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 3).

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.

Because it is saturated, the firewall market is driven by refresh cycles of four to five years. We have seen some common patterns in the firewall market as enterprises with three- to five-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 (see "Defining Next-Generation Network Intrusion Prevention").
- Organizations look to extend their on-premises firewall vendor into infrastructure as a service (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 NGFWs in Enterprises

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, but it is mostly restricted to two use cases: distributed Type C enterprises (mostly in the retail industry), and stateful firewall for network segmentation at low cost. However, the UTM approach fails to convince Type A and Type B enterprises that require mature NGFW 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.

Virtualized Firewalls: Hype Accelerates, and Demand Stirs Slowly

As data center virtualization has continued and SDN projects start, 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) 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.

Gartner market data indicates that in 2015, the number of virtual versions of firewalls sold remained flat at less than 2%. Among the 72 reference customers surveyed for this Magic Quadrant, 8% (up from 0% last year) listed "virtual version available" as a top-three reason they selected their current vendor, whereas 47% selected "management console/reporting" as a top-three reason, and almost as many selected "throughput/speed" (47%). Approximately 40% of respondents selected "price" (38%) and "high availability/clustering" (38%), while 25% chose "IPS."

While client market inquiries show a stirring of interest in virtual firewall, no dynamic shift toward virtual appliances will occur until a fundamental change to the current network security virtualization market is made and demand drives vendor innovation.

The Firewall Market Is Roiled by Acquisitions and Remains Dynamic

Acquisitions, divestments and market exits in the firewall space accelerated in 2015, up from 2014's standstill pace. In October, Trend Micro agreed to acquire HP's TippingPoint business, and later decided to EOL the TippingPoint NGFW line; also in October, Intel Security sold its firewall business to Raytheon/Websense, which later renamed itself as Forcepoint. Despite this turmoil, growth remained robust.

In 2015, the firewall market grew 22% to $9.2 billion. For 2016, Gartner estimates the firewall market will grow approximately 12%. We also forecast that this market will reach a compound annual growth rate of 11.9% through 2019, and will be elevated by the addition of standard firewall add-ons such as IPSs and URL filtering, and by existing and new advanced threat defenses. Gartner believes that the firewall market is "at capacity": This is the largest security product market (it should exceed $10 billion by year-end 2016), 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.

But 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 four 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 to the vendor-hosted cloud 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").

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 most NGFW vendors (such as Check Point, Dell SonicWALL, Fortinet and Palo Alto Networks) 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 too 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

Firewall technology continues to be a fundamental element of the network security strategy for Asia/Pacific (APAC) organizations. APAC already represents just over 11% of the total enterprise network firewall market in 2015, and is expected to be the fastest-growing region in 2016. This region has a different competitive landscape to other geographies due to its size and geopolitical alignments (see "Forecast: Information Security, Worldwide, 2013-2019, 4Q15 Update").

There are two usage profiles in Asia/Pacific concerning firewall acquisition and deployed features: Technologically more advanced Asia/Pacific countries (such as Japan, Singapore and Australia) have a similar feature adoption rate to the U.S. and Europe, embracing more recent trends such as firewall integration with the software-defined network (SDN); meanwhile, emerging Asia/Pacific countries (China, Indonesia and others) are still moving through adoption of next-generation firewall (NGFW) and features such as cloud-based sandboxing.

Asia/Pacific includes regions, such as Greater China, with multiple local firewall players delivering regional support and services to clients, providing competitive vendor selection choices. Technically advanced countries enjoy a good mix of regional and international vendors with strong technical support and services choices. APAC still sees technically emerging countries — such as India, Thailand and Malaysia — that hardly have any local firewall vendors, and struggle with technical support and service availability of international vendors, making vendor selection very difficult.

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 (with reporting, at a minimum) and technical support.

With the steady transition to application and intrusion prevention systems (IPSs) delivered by current-generation firewall, vendors also need to support social networking and browser applications that are heavily used in Asia/Pacific, although not prevalent in the product's home country of development. Examples include Tencent (QQ, WeChat, QQ Browser), Weibo, Line, KakaoTalk, Viber and PPS Entertainment. Deep understanding of this application ecosystem and subsequent ability to filter are product differentiators in the Asia/Pacific market.

In the emerging Asia/Pacific countries (such as India, Malaysia, Thailand and China), security-conscious enterprises are primarily adopting international vendors providing the best-of-breed technology, as seen globally. However, some are still struggling with partial vendor presence, and with technical support and services issues. Whereas price is a strong driver for midsize enterprises, the market is continuing to show that products delivering a majority of "good enough" features at a palatable price are their firewall of choice. As a subsegment of the firewall market, high throughput is also an important factor in the telco/ISP vertical in the Asia/Pacific's heavily populated countries, due to the significant amount of 3G/4G mobile usages. Some countries are already or are very close to rolling out 5G, meaning the telco-class firewall market is still vibrant.

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 counties in the region for integrated advanced threat detection capabilities, leading to an increased attach rate in NGFW sales. Vendors that offer this feature to advanced Asia/Pacific customers as part of their overall architecture will be more successful than point product vendors (see "Predicts 2015: Infrastructure Protection").

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.

AhnLab

South Korea-based AhnLab is a long-established security vendor in East Asia. Its firewall is Telecommunications Technology Association Internet Protocol version 6 (TTA IPv6)-verified, which is a regional (South Korean) 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.

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

AhnLab is mostly considered by SMB organizations in South Korea and other East Asian nations that are looking for a regional player with regional technical support, and an incumbent vendor to their existing endpoint security solution.

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. On the other hand, Gartner clients in emerging Asia/Pacific countries, such as India, Malaysia and Thailand, have consistently reported lack of regional technical support and quicker issue resolution as a major limitation that prevents them from considering Check Point as a shortlist candidate.

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

Check Point should be considered by security-conscious organizations that select vendors based in Asia/Pacific region due to its mature centralized management, breadth of security content and range of appliances.

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 formidable vendor in this market due primarily to its large channel and cross-selling opportunity for Asia/Pacific partners and clients.

Cisco has APAC technical support centers in 12 geographies: Australia, China, Hong Kong, India, Indonesia, Japan, Korea, Malaysia, Philippines, Singapore, Taiwan and Thailand.

Cisco competes as a shortlist candidate in the Asia/Pacific region for midsize and large enterprises that value a single vendor for networking and security solutions, as well as Asia/Pacific wide-field coverage and channel support.

Dell SonicWALL

Dell SonicWALL lags behind many enterprise firewalls in regional market presence.

It has four technical support centers in APAC: in China, Japan, India and Australia.

In the Asia/Pacific region, SonicWALL is most considered by clients that are already running Dell infrastructure, or midsize customers that are looking for price as a competitive option along with local technical support.

Fortinet

Fortinet is one of the rarest international vendors: It has a strong presence in almost all 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. In Japan, NTT Communications selected Fortinet for its managed firewall service in 2015. Fortinet has also invested in Asia/Pacific, with R&D in Beijing, a threat research center in Singapore and a support center in Malaysia. This fosters its local presence as well as its product localization efforts.

It has four technical support centers in APAC: in Malaysia, Japan, China and Australia.

Fortinet is considered by both midmarket and large clients in APAC due to its range of features on a single appliance, competitive pricing/performance and local support for the Asia/Pacific region.

Hillstone Networks

Hillstone Networks is a firewall vendor headquartered both in China and the U.S. Since 2014, Hillstone has set up operations and distributors/resellers networks in most regions globally, including Southeast Asia. Hillstone has a broad portfolio of network security products, but a majority of revenue comes from firewall, targeting both carriers and enterprises. Hillstone's customer base is mostly in China.

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

Hillstone has two technical support centers in APAC: in China and Singapore.

Hillstone is considered by clients based mostly in China as a price-competitive local provider, with a reputation for high performance and stability.

Huawei

Huawei is one of the few Chinese network security companies that has expanded its foothold outside the region in a significant way. More than half of Huawei's firewall revenue comes from outside of China, but the rest of Asia/Pacific is relatively a small market in Huawei's overall revenue split. Huawei's security products are sold widely to both enterprises and telecom operators, mostly as a part of big Huawei network infrastructure deals. Although Huawei security is part of its networking and security division, Huawei security has its own security sales team and dedicated channel partners.

Huawei has one technical support center in APAC, located in China.

Huawei security solutions should be considered by clients valuing the same network and security vendor, by prospects within China, and where price is a primary buying consideration.

Juniper Networks

Juniper Networks does a greater percentage of its firewall business in Asia/Pacific than most global vendors, continuing its longtime legacy of serving regional customers' firewall needs. Juniper Networks has a proven networking channel in the region, which it has leveraged to sell its SRX product line. Gartner believes that recent upgrades to its firewall will be well received by the existing Juniper client base, and will start to allow it to be more competitive on features as well as in new business.

Juniper has six regional technical support centers in APAC: Beijing and Dalian, China; Australia, Japan, South Korea and Hong Kong. It also has two global technical support centers in India.

Asia/Pacific clients have reported the ease of use and availability of Juniper's technical support and services in the region as key factors for their vendor selection.

New H3C Group

New H3C Group was established in November 2003 and is headquartered in Hangzhou, China. Other than firewall, unified threat management (UTM) and VPN products, New H3C Group also has other security products, such as IPS, application control, load balancer (LB) and Web application firewall (WAF), as well as network function virtualization (NFV) security, secure Web gateway (SWG) and distributed denial of service (DDoS) protection. New H3C Group has also developed its own SDN-based security with container technology, rather than using a VMware

platform. The solution targets specifically the multitenancy environment, which is a major requirement of telecom operators and public cloud providers. New H3C Group's clientele includes verticals such as government, financial, enterprise, education and operations.

New H3C Group has its multiple technical support centers based on the China mainland and in Hong Kong. The number of technical support centers is not disclosed by the vendor.

New H3C Group should be considered by the clients primarily in China, or by existing H3C networking clients.

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 presence through channel, which has improved its presence particularly in emerging Asia/Pacific countries. It has added a local WildFire cloud in Japan. The adoption rate of WildFire cloud-based service in technically mature countries is positive. However, the clients in emerging Asia/Pacific countries are cautious about adopting WildFire's cloud-based service, since Palo Alto Networks does not have local data centers to support the service, which raises data privacy concerns in the region.

Palo Alto Networks has two technical support centers in APAC region.

Security-conscious enterprises with no budget constraints and that are looking for a strong international vendor with regional channel support should consider Palo Alto Networks Firewall.

Sangfor

Sangfor is a Chinese firewall vendor, with a strong presence in Greater China through strong channel relationships.

Sangfor firewalls provide support for public cloud, including the regional public clouds AliCloud and Tencent Cloud.

Sangfor has two technical support centers in APAC, in China and Malaysia. Sangfor is aggressively going after the Association of Southeast Asian Nations (ASEAN) market, which it has expanded its partners to hundreds.

Clients in Greater China looking for a local vendor with regional support service should consider Sangfor for the breadth of solutions along with the firewalls it provides.

Sophos

Sophos is not traditionally a large player in the Asia/Pacific enterprise, but with its February 2014 acquisition of India-based Cyberoam, it has bolstered its presence in the region, especially South Asia. Sophos is still selling Cyberoam product lines separately in South Asia. Clients should carefully assess the availability and technical support of the Cyberoam product line of devices.

Sophos has four technical support centers in APAC: in Australia, the Philippines, Japan and India.

Clients in South Asia, especially India, consider Sophos because of the availability of multiple features in a single appliance with a very competitive pricing, along with a low-cost regional service and support options.

WatchGuard

WatchGuard's regional presence in terms of the number of its Asia/Pacific customer mix is about on par with its extra-regional competitors. Over the past several years, WatchGuard has grown its presence in the region, with additional staff in addition to consistent improvements in its product range, including a very competitive log visualization tool called Dimension; this suits smaller and midmarket customers, regardless of vertical, in Asia/Pacific.

WatchGuard has one regional technical support center in the APAC region, located in Japan.

WatchGuard should be considered by midmarket and geographically dispersed Asia/Pacific businesses that require a mix of good security features at a competitive price.

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, total), 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
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.

Note 2
Buyers' 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 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 3
Firewall Policy Management Tools

Third-party firewall policy management (FPM) 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 FPM 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. All FPM vendors support multiple firewall products, whereas no firewall vendor will effectively manage a competing product. In addition, FPM vendors are expanding into managing other network security devices, such as IPSs.

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.

(http://gtnr.it/1KsfgQX)
