Magic Quadrant for Enterprise Network Firewalls

15 April 2014 ID:G00258296

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

VIEW SUMMARY

"Next generation" capability has been achieved by the leading products in the network firewall market, and competitors are struggling to keep the gap from widening too much. Buyers must consider their own operational realities and the burden of switching.

Market Definition/Description

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. These products are accompanied by highly scalable 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. 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; but also as demonstrated by the features dedicated to solve enterprise requirements.

As the firewall market continues to evolve, other security functions (such as network intrusion prevention systems [IPSs], application control, full stack inspection and extrafirewall intelligence sources) will also be provided within an NGFW. The Secure Sockets Layer (SSL) VPN market has largely been absorbed by the firewall market. Eventually, the NGFW will also subsume much of the stand-alone network IPS appliance market at the enterprise edge. This will not be immediate, however, and some enterprises will choose to have best-of-breed IPSs embodied in next-generation IPSs (NGIPSs). Although firewall/VPNs and IPSs (and sometimes URL filtering) are converging, other security products are not.

All-in-one or unified threat management (UTM) products are suitable for small or midsize businesses (SMBs), but not for the enterprise. The needs for 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, they will need to truly integrate 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 within the same appliance.

Return to Top

Magic Quadrant

Figure 1. Magic Quadrant for Enterprise Network Firewalls

STRATEGIC PLANNING ASSUMPTIONS

Virtualized versions of enterprise network safeguards will not exceed 10% of unit sales by year-end 2016.

Through 2018, more than 75% of enterprises will continue to seek network security from a different vendor than their network infrastructure vendor.

Less than 20% of enterprise Internet connections today are secured using next-generation firewalls (NGFWs). By year-end 2014, this will rise to 35% of the installed base, with 70% of new enterprise edge purchases being NGFWs.

Fewer than 5% of enterprises will deploy all-virtual firewalls in data centers through 2016.

Fewer than 2% of deployed enterprise firewalls will have Web antivirus actively enabled on them through 2016, although more than 10% of enterprises will have paid for it.

ACRONYM KEY AND GLOSSARY TERMS

ADC	application delivery controller
AFM	Advanced Firewall Manager
ASA	Adaptive Security Appliance
ATA	advanced targeted attack
AWS	Amazon Web Services
DMZ	demilitarized zone
FIPS	U.S. Federal Information Processing Standards
FPM	firewall policy management
GUI	graphical user interface
IP	Internet Protocol
IPS	intrusion prevention system
IPv6	Internet Protocol version 6
MFE	McAfee Firewall Enterprise
MSSP	managed security service provider
NGFW	next-generation firewall
NGIPS	next-generation IPS
P2P	peer-to-peer
SMB	small or midsize business
SSL	Secure Sockets Layer
UTM	unified threat management
VE	Virtual Edition
WAF	Web application firewall

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 2013 "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, they ignored the question, there was poor grammar, they were unable to explain key concepts, they were unable to provide high-quality explanations of use cases, and they 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

Source: Gartner (April 2014)

Return to Top

Vendor Strengths and Cautions

AhnLab

South Korea-based AhnLab is a long-established security vendor. Known mostly for antivirus software, AhnLab's network security offerings include firewalls and IPSs. Five years ago, AhnLab began offering a firewall product under the TrusGuard brand, and now there are 10 models. The firewall is Common-Criteria-certified EAL4, but does not yet have other third-party evaluations (such as ICSA Labs, NSS Labs or FIPS PUB 140-2) that could raise its profile.

AhnLab is assessed as a Niche Player for enterprises, because most of its wins are within a specific geography and/or are associated with an expansion of the endpoint security business, not because the vendor competes only on features.

Strengths

- South Korea clients should consider AhnLab for their firewall shortlists, given its significant local market share.
- The model range is very broad; the engine was designed to minimize distributed denial of service, including features optimized for handling smaller packet sizes.
- AhnLab's endpoint product customers can have the same vendor provide them with their network firewall solution.

Cautions

- The TrusGuard firewall is not often seen in enterprise selections in the Gartner client base. AhnLab was not listed by any vendor we surveyed as a significant enterprise competitive threat.
- Since AhnLab is an antivirus company, having antivirus in the firewall places TrusGuard at a disadvantage versus enterprise competitors; however, it does position TrusGuard well in SMBs or Type C enterprises (see Note 1).
- AhnLab only offers one level of support, which is inadequate to most enterprise use cases.
- The TrusGuard firewall is a relatively new product and does not yet have some features, such as multiple firewall instances, application control within HTTPS or a virtual version.

Return to Top

Arkoon+Netasq

Arkoon+Netasq, headquartered in France, has been a pure-play network security vendor for more than a decade, selling UTM systems (the U series) and enterprise firewalls (the NG series) with integrated IPSs and vulnerability management. In 2012, Airbus Defence and Space — CyberSecurity (formerly Cassidian CyberSecurity, a subsidiary of EADS Group) acquired Netasq. In April 2013, it acquired Arkoon, another French security company with firewalls. Gartner expects Arkoon and Netasq to maintain somewhat operational independence, even if they share common top management and marketing presence.

Arkoon+Netasq products mostly appeal to EU-based SMBs and enterprises. Virtual versions are also available with the V series, and on the Amazon Web Services (AWS) Marketplace.

Arkoon+Netasq is assessed as a Niche Player for enterprises, mostly because it best serves midsize businesses and agencies in portions of EMEA.

likely reply would have been (usually, this is 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, and each reference customer was supplied with a structured survey. References are scored on the basis of their quality and what they tell us. For each vendor, we take into account the comments from that vendor's references as well as what other vendors' customers say about that particular vendor. Vendors can be notably affected by the inability to have a sufficient number of reference customers providing input.

NOTE 1
TYPE 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 for 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 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
FPM TOOLS

Third-party FPM 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, the customers requiring help with complexity are the very largest, and the market is growing. Additionally, very large enterprises may have firewall products from different vendors — usually by accident via acquisition, rather than through choice, because a single-vendor solution is usually the best choice. 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

Strengths

By not using traditional signatures and instead focusing on heuristics, Arkoon+Netasq has innovated an IPS path that is different from mainstream firewall vendors. This has positioned it more uniquely to counter new kinds of attacks.

Arkoon+Netasq is a European vendor and benefits from local certifications, such as the "EU Restricted" or specific assessment from the French government, which is of interest to EU governments and agencies looking for simpler procurement or a local provider.

Arkoon+Netasq gets a good score from clients for ease of use and vendor support. Users report that they like its policy-based management and real-time policy warning.

The new entity adds endpoint protection and encryption solutions to Netasq's portfolio.

Cautions

The majority of Arkoon+Netasq's penetration, visibility and channel is focused on EMEA, especially France. The vendor has not been part of NGFW selections that Gartner has seen.

Arkoon+Netasq faced two major organizational changes in the past two years (an acquisition and a merger), as well as the need to handle two overlapping firewall product lines. Gartner analysts have observed some impacts on Arkoon+Netasq's execution — for example, the latest meaningful version of the Netasq product that targeted enterprises was released in 2011.

Gartner believes that Arkoon+Netasq firewalls, based on former Netasq technology, do not yet fully meet the expectations of buyers for large data centers. The vendor's integrated approach toward the IPS feature might be seen as risky by some of these clients.

Return to Top

Barracuda Networks

Barracuda Networks has been focused primarily on selling to midsize businesses and lower enterprise markets at low prices. It had an initial public offering (IPO) in November 2013. The Barracuda NG Firewall family targets enterprises, whereas the Barracuda Firewall series targets SMBs. The NG Firewall has application control and reputation services, while the Barracuda NG Firewall Vx is a virtual version, and there is a Windows Azure instance.

Barracuda is assessed as a Niche Player for enterprises because it serves mostly one geographic region, and the enterprise is not Barracuda's primary market.

Strengths

The Barracuda NG Firewall is a good option for customers that already have other Barracuda products.

The Barracuda NG Firewall's worldwide support staff offers good local language support, especially in Germany, Switzerland and Austria.

Barracuda clients report to Gartner that they like the management console and the new interactive live connection view.

The Barracuda NG Firewall is a strong competitor in situations where price is highly weighted in the selection.

Cautions

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

Barracuda's product naming is confusing for enterprise clients. The Barracuda Firewall series targets SMBs, while the Barracuda NG Firewall series targets enterprises.

No vendor we surveyed listed Barracuda as a significant enterprise competitive threat. Barracuda has not yet been visible on the firewall shortlists of Gartner customers. Rather, most interest has come from incumbent customers that have other Barracuda products.

The Barracuda NG Firewall has improved on several features, like application control, but remains behind the competition on IPv6 or active/active high availability. Barracuda's IPS in the firewall has not yet been scrutinized by independent testing labs; however, Gartner believes the product is currently in evaluation with NSS Labs.

Return to Top

Check Point Software Technologies

Check Point Software Technologies is a well-known pure-play security company with the largest firewall installed base, as well as strong and broad channel support.

The majority of its customers choose to use Check Point-branded appliances, although options are also available for a software install on self-sourced servers, an AWS instance, and a virtual machine install (Secure Gateway Virtual Edition [VE]). Blue Coat's Crossbeam is an appliance partner. Check Point now has one unified operating system that brings together the IPSO and SecurePlatform operating systems under the GAiA release. Users with whom Gartner has spoken have reported a very successful transition to GAiA overall. GAiA was operationally important for customers because it conjoined the two widely deployed operating systems, IPSO and SecurePlatform, rather than selecting one and announcing the end of life for the other.

Check Point uses the term "Software Blade" to refer to its preloaded software modules, which are enabled through subscription keys. Gartner believes that the blades, which match NGFW features (for example, IPS, user identity, application control and anti-bot), will continue to have high attach rates, whereas we see little demand for some blades that enable other features (for example, email security, Web antivirus and data loss prevention), except in lower-end UTM offerings for SMBs. Check Point has increasingly moved to packages of blades, which brings them closer to competitors' offerings. The recent addition of the 13500 and 61000 models and modules expands the higher end of the model line.

Check Point is assessed as a Leader for enterprises, mostly because we continually see it competing and winning in demanding selections, providing an NGFW development path that customers are asking for, and retaining customers based on its features and channel strength.

Strengths

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.

Check Point scored high as a significant enterprise competitive threat by all vendors Gartner surveyed. Gartner has observed that Check Point is on most shortlists in which security protection is weighted highly, or in environments handling the most sensitive data and/or in high-compliance environments.

The Check Point management console is consistently ranked highest by customers with a large number of firewalls with differing configurations or a significant compliance burden, and it remains the de facto "gold standard" against which other consoles are measured. Check Point continues to invest considerable intellectual property into the console, in recognition of the importance that configuration has to administrators in enterprise deployments. Gartner surveyed Check Point clients that were consistently managing complex environments with many firewalls and users, or had "lean forward" postures and were looking to limit compliance and operational risk, or had very narrow firewall change windows.

Check Point has a strong array of product options, such as Virtual Systems for virtualized firewalling, VE for running in virtualized environments, and its SmartEvent correlation product. The wide availability of appliance models and software options enables Check Point to meet the requirements for complex enterprise networks. Check Point has performed favorably in third-party IPS testing, and Gartner clients have commented that the IPS is a significant improvement over previous Check Point IPS products.

Check Point has a good capability for meeting large enterprise and data center requirements. Gartner believes that Check Point also has a leading high-end appliance design strategy, especially for traffic aggregation in the backplane. However, unlike some of its competitors, Check Point has not been observed pushing enterprises to add Web antivirus/content filtering into firewalls, with the resulting poor performance and failed proofs of concept.

Check Point continues to have a strong third-party ecosystem of security products that integrate with its management platform. Gartner has received overall positive feedback from clients regarding the stability and use of Check Point's GAiA operating system release.

Cautions

Gartner believes that Check Point struggles with effective marketing to new prospects, instead targeting mostly expansions with existing customers. Even when Check Point is first to market or has a significant feature released, its low-key or indirect marketing approach makes little impact on awareness, especially versus competitors with much greater marketing effort.

High price is a common reason provided by Gartner customers for replacing or considering replacing Check Point firewalls. Price alone is not an issue in new placements in which a premium firewall function is required and, therefore, justifies the investment. In other firewall selections and support renewals, Gartner often hears that support pricing is complex and price negotiations are difficult, which creates friction during renewals and causes some customers to consider replacement.

Gartner views the Check Point Software Blade architecture as having too many options (that is, blades). Enterprises are cautious about adding new functions to firewalls. Check Point sells blade bundles, however, with 12 blades now available for the Check Point firewall. Gartner believes that Check Point's charging for features that are included by competitors is challenging and can appear "UTM-like"; also, enterprises may be confused by Check Point's "a la carte" proposals versus the integrated offerings of some competing firewalls.

Return to Top

Cisco

Cisco has an exceptionally broad network security product portfolio across the network security, Web security and email security tiers. The firewall offering is primarily via the Adaptive Security Appliance (ASA) brand, which has appended the "X" designator as a suffix to newer models that include an IPS (but most no longer require the IPS add-in hardware module).

The primary console offering, the new Cisco Prime Security Manager (PRSM), can function as an on-the-device single-instance manager, or as a stand-alone multidevice management platform. The PRSM supplants the Cisco Security Manager, which is, however, still supported and in wide use. For more information, see "Vendor Rating: Cisco."

Cisco recently acquired Sourcefire (see "Cisco Commits to Security With Sourcefire Buy, but Alignment Will Take Time").

Cisco is assessed as a Challenger for enterprises over the evaluation period, mostly because we did not see it frequently displacing Leaders based on vision or feature; also, it does not effectively compete in the NGFW field that is visible to Gartner. Instead, Gartner sees Cisco winning firewall procurements mostly through sales/channel execution or aggressive discounting for large Cisco networks when firewall features are not highly weighted evaluation criteria (that is, as part of a solution sell in which security is one component). Cisco's large firewall market share is a testament to the success of this strategy.

Strengths

Cisco has significant market share in security. The Enterprise License Agreement (ELA) for security software and hardware is of interest to 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 of other products from Cisco as the most important factor in their selection of the vendor.

Cisco offers a wide choice in firewall platforms. The primary offering is the stand-alone firewall ASA, but firewalls are also available via the Firewall Services Module blade for 6500 series switches, on Cisco's ASA 1000V Cloud Firewall, and on Cisco's Internetwork Operating System (IOS)-based Integrated Services Router. Gartner views the Platform Exchange Grid (pxGrid) initiative to allow third-party components onto the ASA as the most promising development in the Cisco firewall road map; however, it has not been in the visible forefront of Cisco's security efforts.

The integration of reputation features across Cisco security products is a differentiator that is often missed in enterprise selections. Although many competitors have reputation features, the breadth of the Cisco reputation feed provides high quality.

Gartner expects the acquisition of Sourcefire to improve the quality of the ASA IPS and application control.

Cautions

Cisco firewall products are selected more often when security offerings are added to a Cisco infrastructure, rather than when there is a shortlist with competing firewall appliances. In the survey to vendors, Cisco's product was the second most frequently listed as the one vendors claimed to replace the most, and it did not appear on the list of their top competitive threats.

Cisco's security console offerings consistently score low versus competitors in assessments conducted by Gartner clients. The Sourcefire FireSIGHT console could be a foundation for future improvements. Gartner does not believe, however, that the former Sourcefire firewall will have a future under Cisco, given the large installed base and established road map of ASA, and given how little relative market share the Sourcefire product has to date.

Cisco ASA does not have a firewall console integration of a local sandbox-based advanced targeted attack (ATA) appliance, such as those offered by leaders; however, FireAMP and Web Security Appliance are opportunities for other ATA integration. Gartner inquiries see Cisco mentioned more as a contender for replacement than selection, which highlights the challenge facing infrastructure vendors versus pure-play firewall vendors during this current phase of the firewall market's evolution.

Return to Top

Dell SonicWALL

Dell sells enterprise network firewalls under the Dell SonicWALL name. Although the majority of Dell SonicWALL's business had been selling UTM to SMBs, its SuperMassive line is aimed at the high end, and at very competitive price/performance points. Other Dell SonicWALL security products include SSL VPNs, email security gateways, clean wireless offerings, data encryption offerings, identity management offerings, managed security service provider (MSSP) offerings and backup/recovery offerings. The company's firewall offerings are in four branded lines: SuperMassive, E-Class Network Security Appliance (NSA), NSA and TZ.

Dell SonicWALL is assessed as a Niche Player for enterprises, mostly because it hasn't offered a full set of enterprise-ready features (such as integrations with third-party firewall rule management vendors), and its sales channels and marketing programs haven't effectively reached the enterprise buyers.

Strengths

Dell SonicWALL's broad model range is a good option for distributed enterprises with many remote-office deployments requiring many smaller devices, such as in retail or franchise outlets, or with Type C enterprises (see Note 1). Gartner has observed that the Dell SonicWALL channel has migrated the core firewall business into more midsize organizations, or into organizations that already have a strong Dell SonicWALL relationship.

For current Dell SonicWALL customers that want to have fewer security vendors, Dell SonicWALL is a good choice because of its wide range of products and available feature set.

The SuperMassive line has achieved market traction in high-throughput firewall deployments, such as carriers and service providers, in which firewall throughput, low latency, and price per protected megabits-per-second are foremost.

Clients that Gartner surveyed consistently ranked having other products from Dell SonicWALL as the top reason for its selection.

Cautions

As reported by Gartner clients, Dell SonicWALL is not yet widely viewed as an enterprise strategic security player; rather, it is perceived as an SMB brand. Gartner rarely sees Dell SonicWALL in most Type A and Type B enterprise firewall selections.

Dell SecureWorks presents a potential channel conflict for sales to other MSSPs, which can view Dell SonicWALL as part of a competitor. Gartner analysts have observed competitors using this argument to gather channel partners from Dell SonicWALL.

Dell SonicWALL scored low as a significant enterprise competitive threat by the vendors we surveyed.

Return to Top

F5

Seattle-headquartered F5 is an infrastructure vendor that is focused on application delivery controllers (ADCs). It has security products enabled as add-ons to its primary products. Recently, F5 introduced the Advanced Firewall Manager (AFM) module for Big-IP. AFM is not to be confused with Application Security Manager (ASM), which is F5's Web application firewall (WAF) module (see Note 2). AFM has received certification from ICSA Labs. SSL VPN is available in the F5 Access Policy Manager (APM) module.

F5 is assessed as a Niche Player for enterprises, mostly because its network firewall solution fits a narrow set of deployments.

Strengths

Current F5 Big-IP users can easily add a firewall, and at less cost than a stand-alone product. In addition to browser-based management, AFM is managed under the F5 Big-IQ suite, and uses the same iRules customization language, which makes it familiar to F5's ADC staff.

F5's experience in the data center is evident in high firewall throughput. AFM also leverages the high availability and reliability of the F5 Viprion chassis and Big-IP appliances.

Deployments such as those in Web hosting companies, or businesses in which the data center security is distinct from enterprise security, can quickly add high-throughput firewall services.

Increasing focus on security has improved customers' perception of quality of F5's overall offerings.

Cautions

AFM mostly addresses some niche deployments, such as in front of data centers, but not yet between WANs and internal and external networks, nor in branch offices, in-depth or in layers within the data center that are beyond the Web layer (for example, application and data servers). Therefore, AFM is not usually used in cases where the customer wants to avoid the administrative

complexity of multiple firewall brands (see "One Brand of Firewall Is a Best Practice for Most Enterprises").

The firewall does not have the next-generation features (such as IPS) of most firewall competitors, nor does it have application control. Having the firewall console within the ADC console can be a model with which auditors and higher-security enterprises may not be comfortable. Interviewed users requested better reporting, and wanted more ease in getting security assistance through support.

F5 was not listed as a competitive threat by any of the vendors surveyed.

Return to Top

Fortinet

California-based Fortinet has long focused on using purpose-built hardware to produce UTM appliances at strong price/performance points. It now offers a broader network security portfolio and is expanding toward network infrastructure with ADCs, wireless access points and 3G/4G network extenders. Although the firewall features in its UTM products met most of the needs of firewall-focused large-enterprise buyers, Fortinet's approach and philosophy continue to be focused on "everything in one box."

Fortinet also continues to make progress within the Gartner customer base, usually by expanding out from branch office or retail deployments to capture the primary or core firewalls; in addition, it has been seen winning some data center implementations in which high-performance, low-latency stateful firewalls are the primary need. Fortinet is a significant threat to competitors in this market because of its hardware expertise, competitive pricing and steady revenue growth. It is a viable shortlist contender for certain enterprise firewall use cases.

Fortinet has been expanding its support offerings to be better aligned with the enterprise, including options for dedicated technical account managers and an ATA appliance, as well as the ability to manage wireless access points from the firewall management console. Fortinet continues to invest significantly in obtaining and completing certifications.

Fortinet is assessed as a Challenger, mostly because we see it displacing competitors on value and performance, but not often beating Leaders in mainstream enterprise selections based on features and vision, nor causing Leaders to react to Fortinet.

Strengths

Fortinet has a large R&D team and uses it to go to market quickly with new features. Fortinet continually delivers new features in the application-specific integrated circuit and operating system, providing extensive pressure on competitors and pleasing the channel.

Fortinet offers very low price and high port density combined with a wide model range, including bladed appliances for large enterprises and carriers, as well as SMB and branch office solutions.

Fortinet is well-suited to deployments, such as in carriers, data centers, service providers and distributed enterprises (for example, retail and franchises).

Fortinet announced several partnerships with firewall policy management (FPM) vendors.

Cautions

Management capability compared with the competition was most often listed by Gartner clients as the reason why Fortinet was shortlisted by, but not selected in, enterprises. However, where multiple firewalls share the same policy, the Fortinet console is competitive.

Fortinet introduced almost 30 new devices in the past 18 months. The number and naming of available firewall appliances can confusing when combined with model ID and revision.

Fortinet was one of the first firewall vendors to offer cloud-based sandboxing (in December 2012 with FortiOS 5), but it offers narrow coverage compared with leading brands in this area. Gartner believes that Fortinet's attempt to hide UTM features from the management console with its recent "Feature Select" is insufficient when enterprise clients use application control and user context.

Fortinet's UTM-oriented marketing focus is at a disadvantage compared with the marketing of its enterprise-focused competitors.

Return to Top

Hillstone Networks

With headquarters in Beijing and new operations in the U.S., Hillstone Networks is a firewall pure-play company that has been shipping firewall products since 2008. It has 12 firewall models divided into two lines: the Intelligent Next-Generation Firewall (INGFW) and the Data Center Firewall line.

Hillstone Networks is assessed as a Niche Player for enterprises because it operates only within a specific geography.

Strengths

It has a full-featured next-generation firewall with a very broad range of models and a specific focus on the enterprise.

China-based clients should consider Hillstone for their firewall shortlists, given the significant local market share and presence.

The model range is very broad. The Data Center Firewall line is designed with features specifically for multitenant firewall placements.

Cautions

Hillstone Networks' firewalls are not yet seen in enterprise selections among the Gartner client base outside of Asia/Pacific. Hillstone Networks was not listed by any vendor we surveyed as a significant enterprise competitive threat.

Gartner-surveyed users requested better features, such as improvements for managing firewall patching and upgrades, as well as better physical interface options for appliances.

Return to Top

HP

California-headquartered HP has two lines of firewalls. The first is the new TippingPoint Next-Generation Firewall (NGFW) line; the second line is composed of F5000 and F1000, formerly of H3C Technologies in China. These two lines are on distinct code bases, are under different consoles and are supported by different groups within HP. The TippingPoint firewall is built on a different hardware platform than the TippingPoint IPS, so, currently, there is no direct hardware upgrade path from the IPS to the NGFW.

HP is assessed as a Niche Player, mostly because the new firewall product was released only recently and Gartner has not yet seen it competing with significance on shortlists (see "Vendor Rating: HP" for more information). HP has the potential to be a disruptive influence and a market challenger through continued product advancement and utilization of the HP channel.

Strengths

- The TippingPoint IPS brings a very good quality of IPS to the new NGFW line, which is of interest to incumbent TippingPoint IPS deployments that are looking to replace a firewall, or to those deployments in which IPS needs are more highly ranked than other firewall features.
- There is a good range of models in the new firewall line, meaning new adopters are less likely to have to wait for new models to consider deployments.
- The TippingPoint firewall and IPS are managed under the HP TippingPoint Security Management System (SMS) console, which will already be familiar to HP IPS customers.

Cautions

- The TippingPoint firewall is new, and enterprise firewall buyers are often hesitant to invest in something that doesn't have a proven track record in this market. However, incumbent HP customers may still find this to be a shortlist option.
- The firewall currently lacks certifications and third-party testing, such as Common Criteria for Information Technology Security Evaluation (which is usually seen in enterprise contenders). As is often the case with new products, the surveyed HP users most often cited that the console needs improvement.
- HP needs to more aggressively rationalize its two firewall lines if it wishes to compete with the Challengers and Leaders in this aggressive market.
- HP does not currently present a natively developed advanced-threat-solution add-on product that can integrate with its firewall products.

Return to Top

Huawei

China-based Huawei has been shipping firewall products for almost a decade (for more information, see "Vendor Rating: Huawei"). The range of 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 line for carriers and service providers. The majority of Huawei firewalls are sold to carriers, ISPs, and cloud and service providers.

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

Strengths

- Gartner assesses Huawei as having a very good overall network security strategy and a large security research team.
- Customers whose networks are based primarily on Huawei infrastructure products can include Huawei firewalls. Users report to Gartner that Huawei appliances perform as expected under load.
- The top end of the Huawei firewall line has a very high throughput and is a good shortlist candidate for carriers. Most deployments Gartner observes are higher-throughput deployments.

Cautions

- Huawei has limited competitive visibility outside the Asia/Pacific region; however, there is some increasing competitive presence in EMEA.
- Interviewed users reported that they would like to see better features in the Web graphical user interface (GUI) console, and consistently asked for better reporting.
- Despite a recent burst of firewall hardware and software releases, most of Huawei's enterprise security road map is still on schedule to be delivered through 2014 and 2015.
- 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, primarily North America.

Return to Top

Juniper Networks

The firewall offerings of California-based Juniper Networks are in multiple model lines: SRX, SSG, ISG and the virtualized version of SRX Firefly Perimeter. 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 routing in the firewall as being of interest to a limited segment of customers. Juniper has AppSecure for application control and visibility, as well as IPS. Juniper's Junos Space Security Design is the successor product to the current security management within Juniper Network and Security Manager (NSM).

Juniper is assessed as a Challenger for enterprises, mostly because we see it selected in concert with other Juniper offerings, rather than displacing competitors based on its vision or features. Juniper is, however, sometimes shortlisted and/or selected in mobile service provider deployments and 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 Design console because it is part of the Junos Space

network management platform. Interviewed users commonly reported having other Juniper network products, and they selected the firewalls with throughput weighted highly in their selection.

Good options exist for high-throughput, purpose-built appliances, especially in the higher-end SRX models, because Gartner sees Juniper mostly deployed in data centers.

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

Juniper SRX is a good shortlist candidate in deployments for service providers or hosters where stateful firewall throughput is valued foremost and price is weighted highly.

Cautions

Gartner does not assess Juniper as currently having a highly compelling or differentiated security vision, or one that is well-known to non-Juniper customers. Juniper's emphasis on evasion and WebApp Secure, in conjunction with its current firewall offerings, has not been seen as effective with network buyers in competing with the NGFW messaging of Leaders.

Some Gartner clients have cited a need for support improvements.

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

Juniper has lost security market share in the past year, which supports the observation in Gartner's client base that Juniper firewalls are being replaced and rarely considered on shortlists by customers looking for an NGFW. In the survey to vendors, Juniper was listed most often as the one vendors replace, and we see Juniper mentioned more often by clients that are looking to replace a firewall.

Return to Top

McAfee

Intel firewalls are within the McAfee business unit. McAfee obtained its firewall products through two acquisitions: from Secure Computing with the former Sidewinder product, now renamed McAfee Firewall Enterprise (MFE); and in 2013 from Finland-based Stonesoft, whose product is now called the McAfee Next Generation Firewall (NGFW). Both product lines have a good range of models and virtualized versions. The MFE is certified for use on several third-party platforms, including the Crossbeam X-Series blades. The McAfee NGFW has performed well in third-party testing.

Gartner believes the MFE will be maintained for a period; however, the former Stonesoft Firewall is the primary firewall for enterprises to consider. Gartner believes that, in the near future, McAfee will have a single hardware platform supporting the MFE, NGFW and McAfee Network Security Platform (NSP, which is the IPS product).

McAfee's collective firewall offering, taking into account MFE and NGFW, is assessed as a Niche Player for enterprises because the MFE proxy firewall is acceptable mostly to a subset of government agencies, and because the newly acquired NGFW has yet to establish a significant presence outside Europe.

Strengths

The breadth of the McAfee threat intelligence and reputation feeds is a positive quality element and leverages the McAfee footprint on endpoints, secure Web gateways, email security gateways and IPSs. Stonesoft has a long legacy with high-availability technology, and it has very reliable clustering and active/active deployability. Stonesoft focused early on anti-evasion technology, and protected customers well as attacks evolved to include firewall and deep inspection evasiveness. Almost all Stonesoft clients that were surveyed ranked these features as important in their selections.

The former Stonesoft products are a significant improvement over the incumbent firewall offerings, and McAfee is restructuring to lead with these new products rather than attempting to meld platforms together. Enterprise clients that already have other McAfee security products should consider the new McAfee firewalls on a shortlist.

Although not yet integrated into all firewall consoles, the visibility of ePolicy Orchestrator (ePO) host information within the firewall reporting and console tools is of interest to current McAfee ePO customers.

Cautions

Gartner believes that having the McAfee network security unit within a primarily host-based security company — which is itself within a large endpoint-focused chip manufacturer — remains a significant challenge. Gartner also believes the business unit name change from McAfee to Intel Security will impede competitiveness in network security from a marketing perspective.

McAfee currently has three different network IPS engines across the MFE, NSP and former Stonesoft products. Rationalizing and centrally administering these from one management console will present challenges.

McAfee is rarely seen on Gartner client network firewall shortlists, and Gartner estimates that the market share is small at approximately 2%. Intel and McAfee were not listed by any vendor we surveyed as a significant enterprise competitive threat.

Return to Top

Palo Alto Networks

Palo Alto Networks is a California-based pure-play network security company that has been shipping enterprise firewalls since 2007. While being a relatively new firewall vendor, Palo Alto Networks continues to deliver on an enterprise-focused road map with its recent EAL4+ certification; also, it has a partnership with Citrix and VMware. Palo Alto Networks has become well-known for its innovations in application control and for pushing forward in IPS quality. Gartner sees the shortlists including Palo Alto Networks changing from its base of smaller enterprises and Internet-facing deployments. Now, with an expanding market share, Palo Alto Networks is navigating the transition to larger opportunities, as well as the hurdles of RFPs and formal selections that the transition entails. The PA-7050 appliance was recently released and provides a better top end to the options.

Palo Alto Networks is assessed as a Leader, mostly because of its NGFW focus, because it set the direction of the market along the NGFW path, and because of its consistent visibility in shortlists, increasing revenue and market share, and its proven ability to disrupt the market.

Strengths

- The vendor's focus on enterprise NGFW features and messaging is viewed positively by enterprise firewall operators.
- Gartner clients consistently rate the Palo Alto Networks App-ID and IPS higher than competitors' offerings for ease of use and quality.
- The firewall and IPS are closely integrated, with App-ID implemented within the firewall and throughout the inspection stream. This "single pass" is a design advantage, as opposed to the unnecessary inspection that can occur in competing products that process traffic in serial order.
- The Panorama management console is often ranked highly in selections, and scores well in selections seen by Gartner against all competitors (except Check Point).
- Palo Alto Networks was consistently on most NGFW competitive shortlists seen by Gartner, and in the survey to vendors, it was most mentioned as the vendor with which these vendors compete.
- A simple pricing structure helps in procurements versus competitors that charge for features that Palo Alto includes.
- The WildFire advanced threat appliance and cloud service are popular add-ons with incumbent Palo Alto Networks firewall customers, giving them an option versus third-party advanced threat appliance solutions.

Cautions

- Recently, Gartner has seen Palo Alto Networks' direct sales and resellers being overly optimistic about the performance impact of turning on antivirus (that is, Web anti-malware) when being pressured by lower-cost UTM competition, resulting in poor performance during proofs of concept, client skepticism and low selection scores, especially in larger enterprises or data centers.
- The company has limited products in adjacent security markets, which limits cross-selling opportunities.
- The company has room to develop a better third-party product support ecosystem.
- Palo Alto Networks lacks an entry-level platform for small offices that would be price-competitive for distributed enterprise with small branches.
- Gartner clients are increasingly asking about Juniper Networks' patent lawsuit against Palo Alto Networks. However, Gartner has not seen this item alone shift a deal away from Palo Alto Networks.
- 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).
- The clients we interviewed would like to see better log handling at scale. Also, the client complaints we receive regarding Palo Alto Networks usually relate to management console issues at scale, or anecdotes of long commit times.

Return to Top

Sophos

Security company Sophos has co-headquarters in the U.K. and the U.S. Its network security products were derived from the acquisition of Astaro in 2011, but have evolved considerably since then. Sophos recently announced the acquisition of India-based Cyberoam, giving Sophos new geographic coverage, but with considerable immediate overlap in product lines. The Sophos UTM lines necessarily target SMBs. Gartner has observed Sophos usually scoring high where price is the primary factor and where Sophos products are already in place. Cyberoam is mostly seen on shortlists in India and nearby geographies.

Sophos is assessed as a Niche Player for enterprises, mostly because it wins over competitors in some selections based on some specific features, or because it has a very specific channel serving primarily the midsize businesses and smaller enterprises, or specific geographies. The Sophos and Cyberoam firewalls are available as an appliance or a software load.

Strengths

- Surveyed users consistently comment on the ease of installation as a strong point. The Sophos UTM console scores very well in selections that Gartner has observed.
- A free firewall is available in the "UTM Essential Firewall" edition; it includes firewall, network address translation, routing and Web GUI. The free edition runs on a PC, within a virtual machine or in the VMware vSphere Editions.
- The Sophos blog has been a visible medium in the security ecosystem for establishing Sophos as a broader security participant, and Cyberoam has had a technical focus and depth of discussion on competitive performance that is popular with firewall buyers.
- Sophos' endpoint product customers can have the same vendor provide them with their network firewall solution.

Cautions

- The Sophos firewall is not often seen in enterprise selections among Gartner's client base. As a UTM product, it is not a match for most enterprises, and instead is seen more often in SMBs. The Sophos and Cyberoam products usually compete with other SMB firewall vendors' solutions; however, they are good shortlist candidates for Type C enterprises (see Note 1).
- Sophos and Cyberoam were not listed by any vendor we surveyed as a significant enterprise competitive threat, and they have not been highly visible on NGFW shortlists among Gartner clients. Recent efforts in supervisory control and data acquisition (SCADA) security might become another enterprise niche for Sophos.
- Upcoming product line integration/rationalization could cause confusion among customer prospects, and may dilute focus on improving the products and delivering new features.

Return to Top

WatchGuard

WatchGuard is a Seattle-based network security company that has primarily seen success in selling UTM products to midsize enterprises. Its XTM 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. A well-established, security-focused company,

WatchGuard also has products that include SSL VPN and the Extensible Content Security (XCS) email and Web security line.

The XTM-branded firewall models fall into two categories: The XTM 2 Series and XTM 5 Series are UTM, while the XTM 8 Series and the XTM 1520 and above are targeted at the enterprise. Since WatchGuard's introduction of the "NGFW Bundle" option for appliances in 2011, the company has offerings that better suit enterprise buyers than the UTM-only approach.

WatchGuard is assessed as a Niche Player for enterprises, mostly because it serves SMBs and distributed enterprises. However, we do not often see it displacing Leaders for the edge firewall use case based on features; also, it is not present on data center shortlists.

Strengths

- WatchGuard's strong price/performance points have enabled it to win price-sensitive competitions across retail, branch office, remote office and Type C enterprise deployments.
- WatchGuard continues to invest in enterprise use cases, with three new high-end models (XTM 1520, 1525 and 2520) released in 2013, and new software features such as dynamic protocol routing and WAN failover.
- Users report high satisfaction with the WatchGuard management console. Enterprise models are correctly targeted at NGFWs rather than UTM functionality.
- 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, or via an MSSP.

Cautions

- Gartner rarely sees WatchGuard in most Type A and Type B enterprise firewall selections. Enterprise-class channels and support will need to be expanded if WatchGuard wishes to compete in a broader segment of enterprises.
- The most common criticism Gartner receives about WatchGuard has to do with IPS quality.
- WatchGuard scored low as a significant enterprise competitive threat by the vendors we surveyed, and it has low visibility in Gartner's customer base.
- WatchGuard lags behind the Leaders in advanced malware detection capabilities; however, Gartner expects it to introduce features in this segment soon.

Return to Top

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.

Return to Top

Added

AhnLab, F5 and Hillstone.

Return to Top

Dropped

Stonesoft was acquired by McAfee and included under that vendor's entry.

Return to Top

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.

Return to Top

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.

Return to Top

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 foremost over 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 quality, breadth and the 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 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. 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 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 (April 2014)

Return to Top

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" road map. 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 road maps. 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 road map and delivery of NGFW is 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 providing clear explanations and recommendations for detection 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 road map, current features, NGFW integration, 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. Innovation, such as introducing practical new forms of intelligence to which the firewall can apply policy, is highly rated.

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 international 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 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 (April 2014)

Return to Top

Quadrant Descriptions

Leaders

The Leaders quadrant contains a mix of large and midsize vendors, with the common element of making products that are built for 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. An NGFW capability is an important element as enterprises move away from having dedicated IPS appliances at their perimeter and remote locations. Vendors in this quadrant lead the market in offering new safeguarding features, providing expert capability rather than treating the firewall as a commodity, and having a good track record of avoiding vulnerabilities in their security products. Common characteristics include handling the highest throughput with minimal performance loss and offering options for hardware acceleration.

Return to Top

Challengers

The Challengers quadrant contains vendors that have achieved a sound customer base, but they are not leading with features. Many Challengers are slow to work toward, or do not plan for, an 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 are obligated 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.

Return to Top

Visionaries

Visionaries have the right designs and features for the enterprise, but they lack the sales base, strategy or financial means to compete with Leaders and Challengers. Most Visionaries' products have good NGFW capabilities, but lack the performance capability and support network. Savings and high-touch support can be achieved for organizations that are willing to update products more frequently and switch vendors if required. If firewalling is a competitive element for an enterprise, then Visionaries are good shortlist candidates. Vendors that do not have NGFW capabilities are adding 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 identification of malicious protocols at multigigabit-per-second rates.

Return to Top

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 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) 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.

Return to Top

Context

The enterprise firewall market is one of the largest and most mature security markets. It is populated with mature vendors and some more recent entrants. Changes in threats, as well as increased enterprise demand for mobility, virtualization 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.

Return to Top

Market Overview

As the first line of defense between external threats and enterprise networks, firewalls need to continually evolve to maintain effectiveness, responding to changes in threats as well as changes in enterprise network speed and complexity. The firewall market is highly penetrated in the larger markets (North America and Western Europe), which 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. FPM products are increasingly being used to manage complexity (see Note 3).

Return to Top

Next-Generation Firewalls

One key area of firewall evolution has been supported for what Gartner (in 2009) called "NGFW features" — namely, integrated deep packet inspection intrusion detection, application identification and granular 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 policy enforcement in approximately the top 25 business applications. Identity-based policy enforcement, or the ability to enforce policy on thousands of applications, has been highly touted, but rarely used.

Because it is highly penetrated, the firewall market is driven by refresh cycles. We have seen some common patterns in the firewall market as enterprises with three- to five-year-old firewalls and IPSs evaluate replacement:

- 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, 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" [Note: This document has been archived; some of its content may not reflect current conditions]).

Return to Top

UTM Is Not Ready for Enterprise Prime Time

Historically, UTM vendors targeted SMB clients. However, in the past few years, the large UTM vendors tried to expand beyond their traditional use case. They now try to sell UTM to enterprise clients that

score price competitiveness higher than security. Gartner sees some limited success for Type C enterprises, but it is 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 NGFW capabilities and do not consolidate Web antivirus on the Internet-facing firewall.

UTM vendors also face difficulties in building a strong sales and support channel for enterprises (similarly, enterprise firewall vendors would 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.

Return to Top

Virtualized Firewalls: The Myth Doesn't Stand Up to the Numbers

As data center virtualization has continued, demand for virtual appliance 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 firewall vendors, because the need for separation of duties drives reluctance from clients to trust the infrastructure to protect itself. As other virtualization platforms, such as Xen and Hyper-V, gain traction, managing heterogeneous virtualized 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 2013, the number of virtual versions of firewalls sold remained flat at less than 2%. No dynamic shift will occur until a fundamental change to the current network security virtualization market is made.

Return to Top

The Firewall Market Is Never Dull

Acquisitions continued during the evaluation period (for example, Cisco acquired Sourcefire, McAfee acquired Stonesoft and Sophos acquired Cyberoam), but there were also new entrants into the firewall market that this Magic Quadrant assesses.

During the evaluation period, the firewall market grew 9% to $8.7 billion in 2013. This is within 1% of our estimate in the 2013 "Magic Quadrant for Enterprise Network Firewalls." For 2014, Gartner estimates the firewall market will grow approximately 9% to reach $9.4 billion. We also forecast that this market will reach a compound annual growth rate of 10% through 2016, and will be elevated by the addition of firewall add-ons such as IPSs and advanced threat defenses. Gartner believes that the firewall market is "at capacity": Although the growth rate is in the single digits, this is the largest security product market, 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.

Return to Top

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 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 and WAF technologies converging because they are for different tasks at different placements. Most traffic to enterprise Web servers remains encrypted until it reaches the ADC, meaning the owners of firewalls and IPSs face the difficult 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").

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 share until they can provide competitive firewalling for all enterprise placements. They can, however, serve a very niche set of placements, such as in cases where the data center is a separate business with its own firewall operations staff.

Return to Top