Magic Quadrant for Enterprise Network Firewalls

15 March 2010

Greg Young, John Pescatore

Gartner RAS Core Research Note G00174908

The enterprise network firewall market has entered an evolutionary period, as disruption is brought on by increasingly sophisticated and targeted threats, virtualization, and business process changes. Vendors vary in their rate of innovation toward next-generation firewall capabilities.

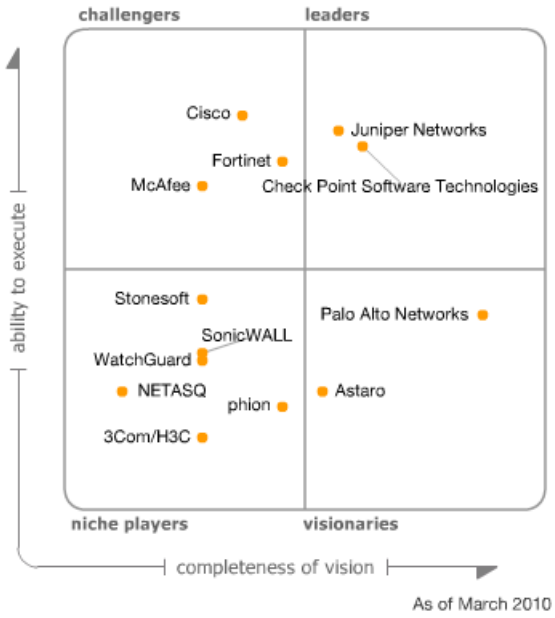
What You Need to Know

The enterprise firewall market is one of the largest and most mature security markets. It is populated with mature vendors, and shortlists are fairly homogeneous among horizontal and vertical markets. Innovation has been limited, and opportunities for reducing firewall unit costs have increased because of fewer points of differentiation among competing products and virtualization. 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

Magic Quadrant

Figure 1. Magic Quadrant for Enterprise Network Firewalls



Source: Gartner (March 2010)

Return to Top

Market Overview

By providing a single point of security policy enforcement that is not controllable by users or IT administrators, firewalls have long provided the most cost-effective means of protecting vulnerable PCs, servers and infrastructure from external attacks to enable secure business use of the Internet. Firewalls are a "check the box" requirement in

Acronym Key and Glossary Terms

ASA	Adaptive Security Appliance
ASIC	application-specific integrated circuit
CSM	Cisco Security Manager
DMZ	demilitarized zone
EU	European Union
EMEA	Europe, the Middle East and Africa
ePO	Enterprise Policy Orchestrator
FPM	firewall policy management
FIPS	Federal Information Processing Standard
Gbps	gigabits per second
IPS	intrusion prevention system
ISP	Internet service providers
ISR	Integrated Services Router
MFE	McAfee Firewall Enterprise
MSSP	managed security service provider
SMB	small or midsize business
SPLAT	SmartCenter on Secure Platform
SSL	Secure Sockets Layer
SWG	secure Web gateway
UTM	unified threat management
VPN	virtual private network
WOC	WAN optimization controller

Note 1
Firewall Policy Management Tools

Third-party firewall policy management (FPM) vendors (such as AlgoSec, Exaprotect, RedSeal Systems, Tufin Technologies, Secure Passage and Skybox Security) 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 usually have firewall products from different vendors — usually by accident via acquisition, rather than through choice, because a single vendor solution

many compliance regimes for any enterprise to define trust boundaries. As threats have gotten more targeted and more complex, firewalls have begun to incorporate deep packet inspection intrusion prevention system (IPS) features to inspect the connections allowed through the firewall.

However, business demands have changed the way IT capabilities are developed and delivered. The traditional model of users sitting at PCs on the LAN (physically and logically via virtual private network [VPN] connections) and accessing critical business data and applications from the internal data center while occasionally surfing the Web has changed. The rapid growth of business applications moving from the internal data center to external software as a service (and someday cloud services), along with the impact of what Gartner calls "the consumerization of IT," has rapidly changed the definition of a "trust boundary" and the types of security controls that are required at that boundary.

In 2009, Gartner saw market pressures accelerate the demand for next-generation firewall platforms that provide the capability to detect and block sophisticated attacks, as well as enforce granular security policy at the application (versus port and protocol) level. A further disrupting factor is the rate of change within enterprise networking — inexorably increasing throughput, more Web-based applications, more complex connections within applications, more complex data centers and more data being presented to customers means that firewalls have had to keep up with features and performance to meet these changing needs.

Branch-office firewalls and small and midsize business (SMB) firewalls continue to diverge as increasingly distinct products, with enterprises looking to their primary firewall vendors to provide the branch-office devices, along with the management tools to handle them.

Although the firewall market has a relatively slow percentage of growth (appliance revenue grew 5.4% from $5.4 billion in 2007 to $5.7 billion in 2008), the market is large, and there was a lot of market activity in 2009. Firewall sales have also included a significant software, support and subscription revenue component that is not captured as part of appliance market sizing.

The firewall market saw its first initial public offering (IPO) in years, as Fortinet went public in late 2009. Several high-profile acquisitions occurred as well, with McAfee buying Secure Computing, and Barracuda acquiring a controlling share of phion. Check Point Software Technologies closed on its acquisition of the Nokia network security appliance platform. HP's ProCurve unit announced a new firewall product; however, a few months later, HP announced that it was buying 3Com, which owns both the Tipping Point IPS appliance and the H3C firewall product. Taking a next-generation firewall approach to the market, Palo Alto Networks saw rapid growth in 2009 and meets the inclusion criteria for this edition of the Gartner Magic Quadrant for Enterprise Network Firewalls.

Overall, 2009 enterprise firewall revenue growth has been affected negatively due to delayed firewall refresh — driven by economic conditions rather than on any requirements changes or trends. Gartner forecasts that the enterprise firewall appliance market will have grown less than 5% in 2009. While price pressure has continued (the average price per gigabit per second [Gbps] of firewall throughput dropped to $5,000), firewalls are still sticky and are not commoditized. However, there are many threats to the firewall industry that can further erode margins:

- **The cloud —** Options for off-site firewall infrastructure are not for every enterprise, but along with the success of cloud-based solutions, some share of the firewall market will go into the carrier cloud. This share will be mostly new placements, rather than replacing Internet-facing enterprise firewalls. However, off-premises firewalling will see an increase.
- **Virtualization —** Network firewalls will continue to be dominated by hardware appliances, especially at higher-throughput rates. The best-performing products are on highly customized hardware. The general-purpose hardware of servers appears cost-effective but will, in practice, not deliver high network firewall throughput, and especially not when deep inspection capabilities are enabled. Nonetheless, tactical solutions for firewalls in virtualized environments will be assessed as part of selections, and appliance vendors that also have a VMware option will be scored higher. There are exceptions. For example, hosting companies or enterprise IT that operates like a hosting company will seek an all-virtualized firewalling environment.
- **Milking the installed base —** Established vendors that are attempting to continuously increase prices without delivering proportional value in new features or just creating marketing doublespeak have been seeing displacement to more value-based vendors. In security, the new economics are that enterprises expect some increase in functionality in exchange for the vendor continuing to stay in place, often at a similar price point. Firewall policy management tools (see Note 1) make it easier to migrate between firewall vendors.
- **Globalization —** Geography is playing an increasing role in network security selection, because local support is increasingly valued, and threat sources become regionalized. New vendors from Asia/Pacific could be a significant threat if the current vendors take their positions and market share for granted in the face of this competition.

The IPsec VPNs in firewalls are somewhat commoditized and rarely play a role in shifting selections. Secure Sockets Layer (SSL) VPNs have remained primarily within stand-alone appliances, except for the SMB market. Small and lower-end midsize businesses (approximately 100 to 500 users) usually are served by the SMB multifunction firewall market. Using the same firewall vendor for main and branch offices provides a management and support advantage, rather than bringing in a second vendor focused on smaller appliances. Branch-office firewalls are distinct from SMB firewalls. The branch device is centrally managed, often has a WAN optimization controller (WOC), and does not use some safeguards that are already provided elsewhere in the enterprise (for example, anti-spam).

To counteract the trends above and maintain margins, most enterprise firewall vendors will need to show how their firewall products deal with advanced threats and how they seamlessly integrate with other security products, such as secure Web gateways (SWGs), vulnerability assessments and network access control. Most of the vendors in this market sell multiple network-based security products, and have seen higher growth rates in other markets. However, the ones that manage to maintain focus on increasing the value of the network firewall will see the highest growth rates and the highest margins in 2009.

Return to Top

Market Definition/Description

The enterprise network firewall market represented by this Magic Quadrant is composed primarily of purpose-built

is usually the best choice. All FPM vendors support multiple firewall products, whereas almost no firewall vendor will manage a competing product and is expanding into managing other network security devices.

Vendors Added or 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 appearing 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. This may be a reflection of a change in the market and, therefore, changed evaluation criteria, or a change of focus by a vendor.

Evaluation Criteria Definitions

Ability to Execute

Product/service: Core goods and services offered by the vendor that compete in/serve the defined market. This includes current product/service capabilities, quality, feature sets and skills, whether offered natively or through OEM agreements/partnerships, as defined in the market definition and detailed in the subcriteria.

Overall viability (business unit, financial, strategy, organization): Viability includes an assessment of the overall organization's financial health, the financial and practical success of the business unit, and the likelihood of the individual business unit to continue investing in the product, to continue offering the product and to 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 and track 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 in order 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, 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), the availability of user groups and service-level agreements.

Operations: The ability of the organization to meet its goals and commitments. Factors include the quality of the organizational structure, such as 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 product 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

appliances for securing corporate networks. Products must be able to support single enterprise firewall deployments and large deployments, including branch offices. These products are accompanied by highly scalable management and reporting consoles/products.

As the firewall market continues to evolve, other security functions, such as network IPSs, will also be provided within a next-generation firewall. The next-generation firewall market will eventually subsume the stand-alone network IPS appliance market at the enterprise edge. This will not be immediate, however, because enterprise firewall vendors have IPSs within their firewall products that are competitive with stand-alone IPS appliances. Although firewall/VPN and IPS are converging (and sometimes URL filtering), other security products are not. All-in-one or unified threat management (UTM) products are suitable for SMBs but *not* for the enterprise. Branch-office firewalls are becoming specialized products, diverging from the SMB products.

As part of increasing the effectiveness and efficiency of firewalls, firewalls will need to add more blocking capability as part of the base product, and go beyond port/protocol identification and move toward a service view of traffic.

Return to Top

approach to product development and delivery that emphasizes differentiation, functionality, methodology and feature set 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 industries.

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.

Inclusion and Exclusion Criteria

Inclusion Criteria

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

- Gartner analysts assess that the company has an ability to effectively compete in the enterprise market.
- Gartner clients generate inquiries about the company.
- 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 are important enough to merit inclusion.
- The vendor has achieved enterprise firewall product sales (not including maintenance) in the past year of more than $10 million and within a customer segment that is visible to Gartner.

Exclusion Criteria

Network firewall companies that were not included in this report may have been excluded for one or more of the following conditions:

- The company didn't supply sufficient information for assessment or did not meet the inclusion criteria.
- The company has minimal or negligible apparent market share among Gartner clients, or is not actively shipping products.
- The company is not the original manufacturer of the firewall product. That includes hardware OEMs, resellers that repackage products that would qualify from their original manufacturers, as well as carriers and Internet service providers (ISPs) that provide managed services. We assess the breadth of OEM partners as part of the evaluation of the firewall, and 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 multifunction firewalls or those for small office/home office placements, are not targeted at the market this Magic Quadrant covers (enterprise) and are excluded.
- The company has primarily a network IPS with a nonenterprise-class firewall.
- The company has personal firewalls, host-based firewalls, host-based IPSs and Web application firewalls — all of which are distinctly separate markets.

Stand-alone network IPS appliances are a distinct market and are covered in Gartner's Magic Quadrant for Intrusion Prevention Systems.

Return to Top

Vendors Added

- Palo Alto Networks
- 3Com/H3C

Return to Top

Vendors Dropped

No vendors were dropped. Name changes did occur as a result of acquisitions, with Secure Computing changed to McAfee. Although phion was acquired by Barracuda, the phion brand is still being maintained as distinct in the primary sales base. Gartner examined several vendors that did not meet the inclusion criteria, or were nonresponsive and did not have any significant visibility within the market.

Return to Top

Evaluation Criteria

Ability to Execute

- *Product or service:* This includes service and customer satisfaction in 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 continuously deployed in enterprises, and the company wins a large percentage in competition with other vendors. Companies that execute strongly generate pervasive awareness and loyalty among Gartner clients, and 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 is foremost over revenue. Key features are weighted heavily, such as virtualization, console quality, low latency, range of models, secondary product capabilities (logging, event management, compliance, rule optimization and workflow), and being able to support complex deployments and modern demilitarized zones (DMZs). Having a low rate of vulnerabilities in the firewall is important.

- *Overall viability:* Overall business viability includes overall financial health, prospects for continuing operations, company history, and demonstrated commitment in the firewall and security market. 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 is compared to Gartner data on such competitions held by our customers), and devices in deployment. The number of firewalls shipped or the market share is not the key measure of execution. Instead, we consider use of these firewalls to protect the key business systems of enterprise clients and presence 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. Pre- and post-sales support are evaluated. Pricing is compared in terms of a typical enterprise-class deployment, including 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) was assessed, as was the pricing model for (1) conducting a refresh while staying with the same product and (2) replacing a competing product without intolerable costs or interruptions.
- *Market responsiveness and track 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.
- *Market execution:* Competitive visibility is a key factor, including which vendors are most commonly considered top competitive solutions, during the RFP and selection process, and which are considered top threats by each other. In addition to buyer and analyst feedback, this ranking looks at which vendors consider each other to be direct competitive threats, such as driving the market on innovative features copackaged within the firewall, or offering innovative pricing or support offerings. A next-generation firewall 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 the inability of a product 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:* This includes management experience and track record, as well as the depth of staff experience specifically in the security marketplace. The greatest factor in this category is customer satisfaction throughout the sales and product life cycle. Also important is low latency, throughput of the IPS capability, and how the firewall fared under attack conditions. 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/Service	High
Overall Viability (Business Unit, Financial, Strategy, Organization)	Standard
Sales Execution/Pricing	Standard
Market Responsiveness and Track Record	Standard
Marketing Execution	Standard
Customer Experience	High
Operations	Standard

Source: Gartner (March 2010)

Return to Top

Completeness of Vision

- *Market understanding and 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 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 an aggressive future goal; they must put a plan in place, show that they are following their plan and modify their plan as they forecast the market directions will change.
- *Sales strategy:* Sales strategy includes pre- and post-product support, value for pricing, and providing clear explanations and recommendations for detection events. Building loyalty through credibility with 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 to do so in a technically direct manner, rather than selling just fear.
- *Offering strategy:* This criterion focuses on a vendor's product road map, current features, next-generation firewall integration, virtualization and performance. Credible independent third-party certifications include

the Common Criteria for Information Technology Security Evaluation. Integrating with other security components is also weighted, as well as product integration into other IT systems. We also evaluate how the vendor understands and serves the enterprise branch office.

- *Business model:* This includes the process and success rate for developing new features and innovation, and R&D spending.
- *Vertical, industry and geographic strategy:* This includes the ability and commitment to service geographies and vertical markets, such as 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
  - Firewall virtualization and securing virtualized environments
  - Integration with other security products
  - Management interface and clarity of reporting — the more a product mirrors the workflow of the enterprise operation scenario, the better the vision

Products that are not intuitive in deployments or operations are difficult to configure or have limited reporting, and they are scored accordingly.

The more a product mirrors the workflow of the enterprise operation scenario, the better the vision. 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 category. 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	Standard
Marketing Strategy	Standard
Sales Strategy	Low
Offering (Product) Strategy	High
Business Model	Standard
Vertical/Industry Strategy	Standard
Innovation	High
Geographic Strategy	Standard

Source: Gartner (March 2010)

Return to Top

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 rules/policy minimization. A next-generation firewall 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 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 a next-generation firewall 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. Challenger products are often well-priced and, because of their strength in execution, vendors can offer economic security product bundles that others cannot. Many challengers hold themselves back from becoming leaders because they are obligated to place security or firewall products as 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 visionary products have a good next-generation firewall capability but lack the performance capability and support network. Savings and high-touch support can be achieved for organizations willing to update products more frequently and switch vendors if required. Where firewalling is a competitive element for an enterprise, visionary vendors are good shortlist candidates.

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 attempting to break into the enterprise market. Many niche companies 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 niche products, although other models from leaders and challengers may be more suited. If local geographic support is a critical factor, then niche products can be shortlisted.

Return to Top

Vendor Strengths and Cautions

3Com/H3C

China-based H3C (see www.h3c.com) was formed as a joint partnership between Huawei and 3Com, and became wholly owned by 3Com in 2007. Recently, HP announced the acquisition of 3Com. Shipping firewalls since 2003, H3C firewalls have been seeing increased placement, usually as part of H3C's network infrastructure projects. H3C SecPath firewalls will be of interest to China-based enterprises, especially where other H3C, 3Com or Huawei networking equipment is used. H3C is assessed as a niche vendor primarily due to its geographic sales and presence.

Return to Top

Strengths

- H3C has a strong regional presence in China and the Asia/Pacific region.
- It has a wide model range, including branch-office and blade-based firewalls, as well as a flat-fee URL model.
- It has broad IPv6 support.

Return to Top

Cautions

- All of H3C's placements are in the Asia/Pacific region.
- Its firewall lacks certifications and third-party testing, such as Common Criteria for Information Technology Security Evaluation, which is usually seen in enterprise contenders.
- H3C's high patch rate is a concern for high-assurance placements.
- HP has not clearly delineated a long-term strategy in the network security market.

Return to Top

Astaro

Headquartered in Germany, Astaro (see www.astaro.com) has been shipping firewall products since 2001. The majority of its customers are in Europe, the Middle East and Africa (EMEA); however, the greatest growth is in the U.S., as a result of expanded operations out of the Boston, Massachusetts, area. Astaro leverages open-source components and focuses on software. Astaro represents a long-term competitive threat, because it targets midsize requirements and growth with those customers. Its competitiveness on price will be of interest where budgets are tight and the security requirements are not exceptional. Astaro is assessed as a visionary vendor for enterprises mostly because it wins over leaders in some selections based on features but does not have broad market reach or channel strength.

Return to Top

Strengths

- Users like Astaro's clustering features and price, and ease of installation is reported as a strong point. The Astaro Security Gateway supports a high number of concurrent connections.
- Astaro's leverage and integration of a wide range of open-source components provide an attractive price point. There is no extra charge for the management product and, of great interest, it offers a free basic firewall version for use in VMware.
- Astaro was early in having a VMware-certified version of its firewall. Additionally, the Astaro Security Gateway is available as an appliance or software load.
- It has exhibited strong growth in its firewall business, and Astaro has SWG and mail security gateway offerings. Customer satisfaction is generally high, especially with post-sales technical support.

Return to Top

Cautions

- Astaro has limited visibility outside of EMEA and limited channel strength.
- Users would like improved reporting, and Astaro's VPN does not have Federal Information Processing Standard (FIPS) 140-2 certification.
- Its UTM focus is less a match for enterprises and better for SMBs. Astaro is short on enterprise features (such as supporting multiple firewall instances in the same appliance) and usually competes with other SMB

firewall vendors.
- Astaro was not listed by any vendor we surveyed as a significant enterprise competitive threat.

Return to Top

Check Point Software Technologies

Check Point Software Technologies (see www.checkpoint.com) is a well-known, pure-play security company with a well-entrenched installed base and a strong, established channel. Check Point has had two critical events occur since the last issue of this Magic Quadrant: completing the acquisition of the Nokia security products unit, and the R70 release. The Nokia unit acquisition and hardware line expansions for UTM-1 and Power-1 lines put pressure on owners of platforms provided by the remaining Check Point platform partners to migrate to Check Point-branded appliances. Gartner believes that Check Point will, over time, blend the IPSO and SmartCenter on Secure Platform (SPLAT) operating systems into a new SPLAT version. Check Point is assessed as a leader for enterprises because we continuously see the vendor competing and winning in demanding selections, and displacing competitors based on its features and channel strength.

Return to Top

Strengths

- Check Point scored high as a significant enterprise competitive threat by the vendors Gartner surveyed.
- Provider-1 is valued highly by customers with a large number of firewalls, and overall, Check Point firewalls are most often seen in large and complex networks.
- The R70 release had a significant number of features and improvements, which increased competitive pressure significantly across the firewall market.
- Check Point has a strong field of product options, such as VSX for virtualized firewalling and its Eventia correlation product. SecurePlatform allows for a loading of the firewall, along with a hardened operating system onto off-the-shelf server hardware. The wide availability of appliance and software options enables Check Point to meet the requirements for complex enterprise networks.
- Its SmartCenter management console is a strong and mature interface with the ability to handle complex DMZ deployments and large numbers of devices. Check Point always scores very high in console quality in selections. Provider-1 users we surveyed generally report a high level of satisfaction.
- Check Point has good capability for servicing large enterprises with the combination of its Power-1 appliance line, having a VMware-certified version (VPN-1 VE) and VPN-1 UTM running in a container on ESX and Provider-1.

Return to Top

Cautions

- Price is the primary reason that Gartner customers provide for replacing or considering replacing Check Point firewalls. This is not an issue where a premium firewall function is required.
- The Check Point Software Blade architecture will not be viewed as different from a software key or existing competitive offerings until Check Point takes steps to further link hardware and the Software Blade function.
- Check Point remains secretive about its road map and longer-term strategies, sometimes leaving its customers guessing and vulnerable to replacement by competitors.
- The vendor remains challenged in succeeding with network security products outside the firewall market, limiting the opportunities to bring firewall to customers as an expansion of existing spending. Check Point has diluted the possibility of a broader network security focus as it tries to attack desktop security. Check Point is missing significant growth opportunities in e-mail, stand-alone IPS and Web security, and will continue to be challenged by replacement by competing vendors.
- Gartner believes that Check Point has invested significantly in its IPS; however, we still have not seen significant Gartner customer deployments of the IPS software blade. Check Point needs to demonstrate to the market that the IPS software blade is an improvement from SmartDefense and demonstrate a broader next-generation firewall capability.

Return to Top

Cisco

Although marketed otherwise, Cisco (see www.cisco.com) security products do not require Cisco networking equipment to be present, nor does having Cisco networking equipment mandate Cisco security products. Through its acquisition of IronPort, Cisco has strong product offerings across the network security, Web security and e-mail security tiers. Cisco has continued to consolidate its security products into a single business unit. Gartner believes that Cisco is in a strong position to launch "security as a service" and data-center-specific security offerings. Cisco firewalls have not seen any noteworthy changes in 2009; however, Gartner forecasts that changes within the Cisco security unit will be realized with increased competitiveness from 2H10 through 2011. Cisco is assessed as a challenger for enterprises because we do not see it continuously displacing leaders based on vision or feature, but instead through sales/channel execution or aggressive discounting for large Cisco networks when firewall features are not in high demand.

Return to Top

Strengths

- Cisco has significant market share in security (including having the largest market share for firewall appliances), has wide geographic support and is viewed as a significant (second-highest) enterprise competitive threat by the vendors we surveyed.
- The Cisco support network is a strong positive for larger customers.
- Its Adaptive Security Appliance (ASA) has the option to add an IPS module (AIP-SSM) to replace a

stand-alone IPS. The ASA is available in four editions, which clearly define what safeguards are being purchased.
- Cisco offers a wide choice in firewall platforms. The primary offering is the stand-alone firewall/VPN ASA, with firewalls also available via the Firewall Services Module blade for Catalyst switches, and on Cisco's IOS-based Integrated Services Router (ISR).
- The vendor has strong channels, broad geographic support and the availability of other security products.
- The integration of reputation features across Cisco security products is a highly significant feature differentiator that is often missed in enterprise selections.

Return to Top

Cautions

- Cisco remains elusive on competitive firewall shortlists by Gartner customers. Cisco firewall products are selected more often when security offerings are added to Cisco's infrastructure, rather than when there is a shortlist with competing firewall appliances. Cisco was listed by competitors as the product they most replace. This is likely to change as the PIX replacement cycle ebbs. This is not a strong caution, given Cisco's market share.
- Where Cisco firewalls were shortlisted, but not selected, quality and usability of the management console, Cisco Security Manager (CSM), were consistently the factors most often cited.
- Cisco firewall and security products continue to have one of the highest rates of published product vulnerabilities. Although Cisco is a high-profile target, security products must have a higher level of assurance than general-purpose products.
- The requirement to add a hardware module (the AIP-SSM) to add IPS capability to the ASA firewall appliance remains a barrier to deployment and a competitive disadvantage for branch-office deployments. The add-in module does, however, provide processing help with the deep inspection load. If the SSM module is used for IPS, then it cannot be used for other content inspection.
- Two products (usually CSM and CS-MARS) are required for most management functions, whereas competitors have a single product.
- The ASA line is becoming somewhat dated and, although Gartner expects Cisco to introduce new models, Cisco often is excluded from placements with high throughput. Cisco's Firewall Services Module (FWSM) and ISR have been on a separate firewall development stream (closer to the PIX code base) and haven't benefited from ASA advances.

Return to Top

Fortinet

Although SMBs have been the primary market for Fortinet firewalls from this California-based company (see www.fortinet.com), unlike most SMB competitors, Fortinet has high-end appliances and a hardware engineering capability. Fortinet had its IPO in late 2009, which provides increased visibility into the company and greater financial resources. Although the move into the enterprise is slow within the Gartner customer base, Fortinet remains a significant threat to competitors in this market because of its high-end hardware and steady revenue growth. Unlike other SMB-focused firewall vendors, Fortinet is a viable shortlist contender for a good segment of the enterprise firewall market. Fortinet is assessed as a challenger mostly because we see it displacing competitors, although on value and performance and not in classic enterprise selections.

Return to Top

Strengths

- Users consistently like the continued pace of development and delivery of Fortinet's new features and products, and report easy deployment. By developing rather than using OEMs for most safeguards, Fortinet has been able to maintain road map agility. This also has allowed Fortinet to expand its portfolio of nonfirewall network security offerings, which provides increasing cross-selling opportunities.
- Fortinet is increasing its wins against market leaders, and it gained additional footholds in emerging areas, such as in-the-cloud firewalls and with carriers/ISPs.
- Its firewalls have good performance from purpose-built hardware and a wide model range, including bladed appliances for large enterprises and carriers, as well as SMB and branch-office solutions.
- The new dual application-specific integrated circuit (ASIC) strategy used in newer models is a significant performance enabler. The AMC expansion slot options for the enterprise-class models include an onboard security ASIC with additional ports, or a hard drive providing investment preservation without having to resort to only appliance replacement, like many competitors.
- Fortinet is price-competitive, especially when using multiple virtual domains, and appliance reliability is reported as very high.

Return to Top

Cautions

- Where Fortinet was shortlisted but not selected in enterprises, the IPS was most often listed as the reason. Post-sales service and support did not get high ratings from users. Gartner believes this is because of the high growth rate of Fortinet and the challenge in growing the support network at the same pace.
- Marketing focused on using UTM for enterprises undervalues Fortinet's enterprise offerings and steers away larger customers.
- Gartner rarely sees Fortinet in most traditional enterprise firewall selections.
- Its IPO will be a distraction for the management team.

Return to Top

Juniper Networks

Juniper Networks' (see www.juniper.net/us/en) firewalls have continued to progress since the acquisition of NetScreen Technologies in 2004. Unlike Cisco, Gartner sees Juniper firewalls being selected independently from the network infrastructure business by enterprises that are not otherwise Juniper customers. The move to Junos from ScreenOS, along with the SRX model line, are the most significant changes in the Juniper firewalls. Juniper is assessed as a leader for enterprises, because we continuously see it competing and winning in demanding selections, and displacing competitors based on its vision or features.

Return to Top

Strengths

- Performance, range of models and technical support were most often listed by users as what they like about Juniper firewalls. Post-sales support was rated highly by users, although first-line support satisfaction is more mixed. Firewall deep inspection is rated as satisfactory by users but is not competitive with most stand-alone IPSs. Juniper was listed by the majority of vendors as the greatest competitor.
- Good options exist for high-end, purpose-built appliances, especially in the higher-end SRX models, and Juniper expresses a clear road map for firewall and security customers. Juniper has shown development and security discipline in keeping the rate of vulnerabilities in the product low.
- Juniper has strong branch-office firewalls, complementing the enterprise products. Its branch-office firewalls include WOC and an Avaya voice gateway.
- Having routing in the firewall is of interest to a narrow segment of customers.

Return to Top

Cautions

- The Adaptive Threat Management messaging doesn't resonate in the market, and Juniper needs to get back to competing on price, performance and features. Juniper remains competitive but generally did not drive the market from a vision perspective in 2009 relative to competitors.
- As a network infrastructure vendor, rather than a pure-play security vendor, Juniper is at a disadvantage selling into Cisco networks, where buying any Juniper equipment can be resisted as a Cisco network equipment replacement.
- Like most competitors, integration between IPS and the firewall is limited, although Juniper has one of the better in-the-firewall IPSs on the market.
- Juniper is generally high-priced and often allows competitors an opening on price alone; however, customers report that they recognize the value/price proposition.

Return to Top

McAfee

Although primarily a host-based security company, McAfee (see www.mcafee.com/us) has had success in the network security market, notably with its network IPS. McAfee obtained its firewall products through the acquisition of Secure Computing in late 2008. The Sidewinder product has been renamed to the McAfee Firewall Enterprise (MFE). Today, the road map for MFE is more important for consideration than the current features in the product. Re-engineering the MFE to gain feature and hardware parity is not a trivial task. However, Gartner believes that, if McAfee maintains the road map and focus on network security, then it could, in the midterm, become the next significant firewall market disrupter and a potential market leader. A re-engineered MFE integrated with the McAfee IPS on a purpose-built hardware platform will be the milestone for which to watch. McAfee is assessed as a challenger for enterprises, because we do not see it continuously displacing leaders based on vision or feature, but instead through sales execution or value when features are not in high demand.

Return to Top

Strengths

- McAfee could have a road map toward a next-generation firewall by embedding the Sidewinder firewall with the McAfee IPS, and onto a more purpose-built hardware, although this will not occur in the short term.
- The TrustedSource feature blocks known bad IP addresses (from a dynamically updated list source) from connecting to the firewall, and is a significant differentiating feature.
- Having a good record as being free from vulnerabilities, the MFE offers strong features for government, military and other "security first" requirements.
- The vendor's integration of reputation services across network, Web and e-mail security product lines provides a strong cross-selling opportunity. The larger McAfee sales and channels have already increased MFE presence in the market, while changes to the product are under way.
- McAfee has more network security products across multiple markets than almost any competitor. The prospect of integrating these products represents potential "glue" between silo products, which few competitors can yet promise.

Return to Top

Cautions

- Gartner believes that firewall manageability will be decreased if McAfee tries to focus on migrating firewall and IPS management under its desktop-oriented Enterprise Policy Orchestrator (ePO) console; however, McAfee has not done this with its other network security products and is disciplined in maintaining the current road map.
- MFE has low firewall market visibility against market leaders. Gartner rarely sees McAfee firewalls competing in enterprise customer shortlists.

- McAfee has a small range of models. The former SnapGear firewall renamed to McAfee UTM is designed more for SMBs than enterprise branch offices.

Return to Top

NETASQ

Headquartered in France, NETASQ (see www.netasq.com) has been a pure-play network security vendor for more than 10 years. With an all-in-one or UTM approach, NETASQ appeals to midsize companies and EU-based enterprises. NETASQ is assessed as a niche vendor for enterprises, mostly because it best serves midsize businesses and agencies in portions of EMEA or when the leaders are otherwise not welcome. We do not see NETASQ frequently displacing leaders otherwise.

Return to Top

Strengths

- NETASQ has a good mix of features in comparison to competitors in its class. Users report that they like its policy-based management and real-time policy warning.
- It is VPN-certified under for use for "EU restraint" for the European Union (EU), which is of interest to governments and agencies looking for simpler procurement.
- NETASQ is focused on the requirements of midsize customers and provides good channel support.
- Users report that NETASQ's appliance throughput lives up to its performance claims, likely due to the ASQ inspection handling engine.
- An EU-based vendor will be attractive to EU users, especially in France, and support is viewed very positively by Gartner clients.

Return to Top

Cautions

- NETASQ has a narrow international base, with almost all its deployments in EMEA, especially France.
- The product focus is less a match for large enterprises and better for SMBs. Like most SMB-focused firewall companies, NETASQ does not offer a high end of appliances for larger enterprises; however, its sales success has been on serving organizations of less than 1,000 employees.
- NETASQ was not listed by any vendor we surveyed as a significant enterprise competitive threat.
- Marketing against a vulnerability signature-based approach for IPS is viewed skeptically by enterprises that have not used the product.

Return to Top

phion

Previously headquartered in Austria and Switzerland, and shipping firewalls since 2002, a controlling ownership in phion (see www.phion.com) was established by Barracuda in 2009. In the short term, the deal provides assurances of viability for phion, and Barracuda appears keen on moving forward with phion as an enterprise product, and it could form the base for Barracuda attempting to move upmarket. Phion is assessed as a niche vendor for enterprises, mostly because it serves a set of placements well, usually in portions of EMEA or when the leaders are otherwise not welcome, and we do not see phion frequently displacing leaders otherwise.

Return to Top

Strengths

- Focused on enterprises, phion is a good alternative to established large competitors, especially in continental Europe.
- Enterprise customers have well-established local support in Germany, Switzerland and Austria, and increasingly elsewhere in EMEA.
- The phion firewall has features that make it an MSSP-friendly design.
- Post-sales service and customer loyalty are strong, and the quality of its technical support is rated high. The phion road map continues to align itself with the pragmatic realities of firewall administrators.

Return to Top

Cautions

- The de facto acquisition by Barracuda is an awkward fit. Barracuda is primarily an SMB company based in North America and does not have the channels usually suited for enterprise network security.
- The netfence firewall has a narrow international market share and visibility, with almost all placements in EMEA.
- No vendor we surveyed listed phion as a significant enterprise competitive threat.
- An IPS is notably absent from the offering, as is FIPS 140-2 certification for the VPN.

Return to Top

Palo Alto Networks

Palo Alto Networks (see www.paloaltonetworks.com) has been selling firewalls since approximately 2007. Although essentially a startup, Palo Alto Networks is not a typical startup, because the company is well-backed,

including first-tier venture capitalists; the founders are alumni from other firewall companies; and the CTO invented stateful protocol inspection. The company's application ID feature was one of the first in the firewall market to categorize applications within HTTP/HTTPS. Palo Alto Networks is highly disruptive within the firewall market because the product has been designed as a next-generation firewall and has competitors being forced to change road maps and sell defensively. Palo Alto Networks is assessed as a visionary vendor mostly due to its next-generation firewall design, redirection of the market along the next-generation firewall path, and market disruption forcing leaders to react.

Return to Top

Strengths

- Palo Alto Networks was early to introduce effective application identification (App ID), allowing for categorizing, blocking and rate-shaping of applications, primarily within HTTP and HTTPS, and it generally leads in application categorization.
- Active Directory integration allows for firewall rules based on user and resource roles, rather than IP addresses.
- Gartner customers report that Palo Alto Networks' appliance performance is good.
- Palo Alto Networks often enters enterprises via URL-filtering selections, where its per-box charge does better than most competitors that charge a per-user fee.
- The company has also linked the Application ID feature to Active Directory, meaning that reporting and setting the application policy can be by name and organization, rather than by IP address alone.
- The firewall and IPS are closely integrated, with App ID implemented within the firewall, obviating unnecessary IPS deep inspection.
- Palo Alto Networks generated the most firewall inquiries among Gartner customers in 2009.

Return to Top

Cautions

- The PA series of firewalls does not yet have the third-party certifications that are important to this market, such as Common Criteria for Information Technology Security Evaluation and FIPS.
- Palo Alto Networks has a limited number of models.
- Opportunistic selling into the SWG and URL-filtering market can confuse some customers that Palo Alto Networks is not a firewall company.
- Palo Alto Networks has limited geographic support, with almost all sales in North America, although its international channel is growing.

Return to Top

SonicWALL

SMBs are the primary market for SonicWALL firewalls from this California-headquartered company (see www.sonicwall.com). SonicWALL firewalls are candidates for smaller enterprises, or for nonstandard deployments (for example, highly distributed deployments without the classic central monolithic firewall), kiosks and enterprises with low reliance on technology. The SonicWALL Aventail SSL VPN product is a popular enterprise product but has not accelerated a firewall segue into enterprises. SonicWALL is assessed as a niche vendor for enterprises because it serves a set of placements other than classic enterprise firewall deployments well, and we do not see it often displacing leaders.

Return to Top

Strengths

- SonicWALL's competitive prices have resulted in strong solutions for wide remote-office deployments (such as in retail outlets) and SMBs.
- The company has the reputation and track record of strong channel support.
- The Aventail SSL VPN acquisition brought an enterprise sales force into SonicWALL.
- The NSA series is a good option for nontraditional deployments, such as an all-in-one firewall for an in-the-cloud provider. SonicWALL recently added application identification/inspection as an included feature, under the name Application Firewall. Performance monitoring by core provides good device capacity management.
- Being a public company allows SonicWALL transparency for customers rating its viability.

Return to Top

Cautions

- SonicWALL's firewall product line has been primarily SMB-focused and not competitive in most enterprises. "Enterprise" has really meant a midsize company in SonicWALL's product portfolio.
- SonicWALL is short on enterprise features (such as supporting multiple firewall instances in the same appliance). It usually competes with other SMB firewall vendors.
- SonicWALL scored low as a significant enterprise competitive threat by the vendors we surveyed, and it has low visibility in the Gartner customer base.

Return to Top

Stonesoft

Headquartered in Finland, Stonesoft (see www.stonesoft.com) has been expanding operations into North America.

Stonesoft is focused on network security and was one of the first firewall vendors to support virtualized environments. Stonesoft is assessed as a niche vendor for enterprises because it serves a set of placements well — usually, high availability is key or when the leaders are otherwise not welcome.

Return to Top

Strengths

- An enterprise focus makes Stonesoft firewalls distinct from most European competitors, which focus on SMBs. Although the majority of Stonesoft's business is in EMEA, North American sales and visibility have been growing.
- Stonesoft has a pragmatic range of security offerings that reflect the buying and operations realities in enterprises, with firewalls with IPsec VPNs, stand-alone IPSs and SSL VPNs.
- Stonesoft offers a virtualized StoneGate version that is certified for VMware. Both can be run under the StoneGate Management Center.
- Stonesoft offers support for clustering and high availability for enterprises that do not provide for this in the infrastructure outside the firewall. Support pricing is slightly lower than the industry average.
- Its appliances have a robust performance and feature set relative to company resources, and it has a loyal customer base, especially those looking for high availability. Its software quality is reported as being high, with no vulnerability-related patches in 2007.

Return to Top

Cautions

- Stonesoft has limited market visibility and channel strength outside of EMEA, and it has low visibility within the Gartner customer base, although its firewall revenue has increased.
- It is a small company.
- Stonesoft is missing a few features that bigger competitors have, such as Layer 2 support.
- Its pricing sometimes gets StoneGate excluded.

Return to Top

WatchGuard

SMBs have been the primary market for WatchGuard firewalls from this Seattle-based company (see www.watchguard.com). WatchGuard firewalls are candidates for smaller enterprises, or for nonstandard deployments (for example, highly distributed deployments without the classic central monolithic firewall), kiosks and enterprises with low reliance on IT. WatchGuard is assessed as a niche vendor for enterprises because it serves a set of placements other than classic enterprise firewall deployments well, and we do not see it often displacing leaders.

Return to Top

Strengths

- WatchGuard's competitive prices have resulted in strong solutions for wide remote-office deployments.
- WatchGuard has been active in developing new features and models, such as HTTPS inspection. Users report high satisfaction with the reporting function in the WatchGuard management console.
- It has better-than-market-average integration between the IPS and the firewall, such as having IPS blocks result in subsequent source blocking at the firewall. It has a low rate of product vulnerabilities.
- The WatchGuard management team has taken a customer-focused approach. Having a specific management console for MSSPs is a competitive factor. A software key to unlock appliance performance for some models can minimize appliance downtime when upgrading.

Return to Top

Cautions

- IPS signature quality is not competitive at the enterprise level. Certifications, such as FIPS 140-2 for the VPN and Common Criteria for Information Technology Security Evaluation are not yet in place.
- WatchGuard is short on enterprise features (such as supporting multiple firewall instances in the same appliance) and usually competes with other SMB firewall vendors.
- WatchGuard scored low as a significant enterprise competitive threat by the vendors we surveyed and has low visibility in the Gartner customer base.

Return to Top