

Magic Quadrant for Enterprise Network Firewalls, 2H07

Greg Young, John Pescatore

The enterprise network firewall market is mature yet significantly dynamic. The demands made on network firewalls are changing, and firewalls need to interoperate as part of the larger security ecosphere.

WHAT YOU NEED TO KNOW

Many viable firewall providers exist, but the leading vendors provide a path to more-effective inspection and blocking capabilities at higher speeds and at lower price points. Product selection decisions should be driven by organization-specific requirements in areas such as the relative importance of firewall capabilities, ease and speed of the deployment, the acquisition costs, the IT organization's support capabilities, and integration with the established security and network infrastructure.

MAGIC QUADRANT

Figure 1. Magic Quadrant for Enterprise Network Firewalls, 2H07



Source: Gartner (September 2007)

Market Overview

The Network Firewall Market

The enterprise firewall market is driven primarily by the requirement to provide network policy enforcement and intrusion prevention at trusted boundary points. Network firewalls are often the first line of defense and the primary implementers of a positive security model policy of "deny all except that which is expressly allowed." They are the enforcement points for creating demilitarized zones (DMZ) for external connections. Rather than disappearing, the network perimeter has become deeper and more complex. The increasing requirement for network defense against more-complex threats has increased the placements of firewalls and driven vendors to provide products that support complex deployments and rule sets. A counterbalancing effect on the quantity of firewalls sold has been the emergence of virtual firewall platforms that enable many separate firewall appliances to be replaced with a single firewall switch or blade server running multiple virtual firewalls.

Changes in threats and the dynamic nature of enterprise technology are forcing firewalls to evolve. Business connections are becoming more complex, driving firewalls to have increasingly rich management and configuration solutions, as well as to provide deeper and broader inspection and blocking capabilities. Technology and business changes, such as virtualization and server consolidation, have driven firewalls to support virtual firewall capabilities and more-complex DMZs. Common requirements driving selection include the ability to carve the one physical firewall into multiple logical firewalls (reducing box count and license costs), supporting deeper layers of inspection and blocking from the Internet-facing edge of the network into the data center and remote offices, and reducing the overall acquisition and operation cost of the firewalls. Equally important is doing all the above in a changing threat and technology environment, while maintaining security posture visibility with firewall administrators, security managers and auditors.

Revenue in the firewall market is primarily driven by two trends:

- **Firewall refresh:** As firewalls reach their end of life (typically three to five years), enterprises replace them with faster products with deeper inspection and blocking capabilities, typically looking to reduce the cost per firewall even while gaining functionality. Incumbent vendors have strong advantages when firewall refresh drives the procurement, but vendors with advanced offerings and migration support strategies can break the incumbent vendors' hold.
- **New Internet connectivity:** As small or midsize businesses (SMBs) move to broadband connectivity, the installed base of firewalls increases. Smaller firewall vendors with lower total cost of ownership (TCO) offerings or a strong presence with managed security service providers (MSSPs) have opportunities here. The trend for larger enterprises to enable remote/branch offices to have local Internet connectivity also increases the installed base of firewalls, but the incumbent vendor of the headquarters' firewall has a significant advantage in this scenario because there is usually the need for firewall-to-firewall virtual private network (VPN) capabilities between headquarters and the remote offices.

Based on data gathered for this market study, Gartner assessed the enterprise network firewall market in 2006 to have been approximately \$2.5 billion for product, maintenance and service revenue, representing approximately 7% growth over 2005 revenue. Note that revenue is not included in the enterprise totals for companies servicing only SMBs or using general-purpose server platforms as appliances but not sourced through a firewall vendor.

The average maximum throughput for the vendors surveyed was 2.5 Gbps Internet mix (typical network traffic), which was about half of the advertised optimal throughput for most products. The intrusion prevention system (IPS) throughput of products was considerably less. On average, it provided only 945 Mbps Internet mix. The average price per Gbps of enterprise firewall throughput was \$9,760.

Most vendors include maintenance with support. Combined support and maintenance percentages were, on average, 22.5%, with the best rates being about 17% and the highest about 40%. These rates tended to correspond to the features offered, with the feature-rich products charging more. Enterprises need to look at the TCO (purchase price plus annual support plus full-time-equivalent needs) when comparing products, because considerable differences exist among vendors about what is included.

The Next-Generation Firewall and the Absence of a Unified Threat Management Product

Driven by changing threats, network security managers favor best-of-breed security and management features when selecting firewalls. The latency-sensitive safeguards of firewall and network intrusion prevention are converging into the next-generation firewall (NGFW). Firewall vendors have been slow to adopt this trend because of their delay in reacting to market changes and securing their firewalls with IPS technology (and performance) as good as that in stand-alone IPS appliances. The firewall vendors have started to react, although slowly, with positive indications, such as Check Point Software Technologies acquiring IPS company NFR Security. All the leading firewall vendors offer NGFW capabilities in their main products. The IPS vendors that do not have an enterprise-class firewall product will be forced to move away from the network edge into the internal network "cloud" and become security switches or in-line network access control (NAC) enforcement points.

The NGFW is different from a unified threat management (UTM) product. Security convergence at the enterprise is based on maintaining low latency while performing increasingly complex inspection and blocking. Latency-sensitive safeguards, such as IPS and firewalls, will converge into the NGFW, and messaging and other generally latency-insensitive safeguards are following distinct convergence paths (see "Findings: Next-Generation Firewalls and E-Mail Security Boundary Gateways Will Evolve Separately"). The exception to this convergence is with branch-office and SMB security products, where the lowered performance requirements mean many safeguards are present in the same platform.

Branding enterprise firewall products as UTM or antivirus firewalls is simply bad marketing. Enterprises will not be doing antivirus scanning with their primary firewalls in the near term. However, firewalls are required to block more attacks and interoperate with the larger network security landscape. The days when port = protocol = application are behind us. An increasing percentage of enterprise network traffic is being funneled through a few well-known ports, more port-hopping or dynamic application content, such as Web 2.0 and other mashups. In many cases, traffic is being encrypted.

Merely having an IPS in the same appliance as the firewall is not an NGFW. The products must be tightly coupled, interoperate and have intelligent traffic handling, traffic inspection and blocking. Most enterprise firewalls are not fully featured NGFW but, rather, early versions. This slowness to market has opened the door to the competition, such as that from startups — for example, Palo Alto Networks offers a purpose-built NGFW with a service view of traffic, rather than a port-only view.

True UTM or security multifunction appliances (MFAs) that combine many point solutions within a single appliance are appropriate for SMBs and some branch offices. Branch-office firewalls are diverging somewhat from UTMs as they become optimized for the branch-office environment.

The bottom line is that enterprises usually choose branch-office firewalls from the same vendor as their central firewall.

Market Definition/Description

The enterprise network firewall market represented by this Magic Quadrant is composed of purpose-built software and appliances for securing corporate networks. Products must be able to support single-firewall deployments as well as large deployments and high throughput. These products are accompanied by branch-office firewalls and management and reporting products.

As the firewall market evolves, other security functions, such as network IPS and malicious software prevention, will also be provided within an NGFW. The NGFW 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 been slow to imbue the IPS within their NGFW products with the same capabilities as the stand-alone firewall appliances they offer, and many IPS vendors do not have firewalls in their products that can compete with current enterprise-class firewalls. Additionally, new network security technologies are often provided through separate appliances before being included in other offerings. Although many firewalls may be accompanied by an IPS, close integration is not present in many of these products.

As part of increasing the effectiveness and efficiency of firewalls, enterprises need to add more blocking capability to them as part of the base product, go beyond port/protocol identification and move toward a service view of traffic. Firewalls and intrusion-prevention products need to evolve as threats evolve and provide mechanisms for detecting and blocking targeted attacks.

Inclusion and Exclusion Criteria

Inclusion Criteria

Network firewall companies that meet Gartner's market definition and description were considered for this Magic Quadrant under the following conditions:

- Gartner has a generally favorable opinion about the vendor's ability to effectively compete in the enterprise market.
- Gartner clients generate inquiries about the vendor.
- The vendor regularly appears on enterprise shortlists for final selection.
- The vendor demonstrates competitive presence in enterprises and in worldwide sales.
- Gartner considers that aspects of the vendor'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 within a customer segment that is visible to Gartner.

Exclusion Criteria

Companies with insufficient information for assessment or those that did not meet Gartner's inclusion criteria were excluded from the Magic Quadrant based on the following conditions:

- The vendor has minimal or negligible apparent market share among Gartner clients or is not actively shipping products.

- The vendor is not the original manufacturer of the firewall product, which includes hardware OEMs, resellers that repackage products that would qualify from their original manufacturers, and carriers and Internet service providers that offer managed services. We assess the breadth of OEM partners as part of the evaluation of the firewall and do not rate platform providers separately.
- Products sold as network firewalls but do not have the capability, scalability and ability to directly compete with the larger firewall product/function view are not included. Products suited for SMBs, such as MFAs or small office/home office products, are not targeted at the market this Magic Quadrant covers.
- Products that are primarily network IPSs and are without an enterprise-class firewall (not NGFW) are not included.
- Personal firewalls, host-based firewalls, host-based IPSs and Web application firewalls, all of which are distinct markets, are not included.
- Stand-alone network IPS appliances are a distinct market and are covered in "Magic Quadrant for Network Intrusion Prevention System Appliances, 2H06."

Added

None

Dropped

- Symantec effectively exited the network firewall market to concentrate its efforts on other security offerings (see "Avoid New Purchases of Symantec Network Security Appliances").
- iPolicy Networks was acquired by Tech Mahindra and is expected to focus on the service provider and carrier markets. Post-acquisition, iPolicy has maintained its majority business with a few large customers.
- BorderWare Technologies is no longer competing in the enterprise firewall market. Instead, it is focusing on e-mail security (see "Magic Quadrant for E-Mail Security Boundary, 2006").

Evaluation Criteria

Ability to Execute

- Product or Service: This also includes customer satisfaction in deployments and considers factors related to getting products sold, installed, supported and in users' hands. Strong execution means that a company has demonstrated to Gartner that its products are successfully and continuously deployed in enterprises and win 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. 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, such as virtualization, console quality, low latency, range of models, secondary product capabilities (logging, event management and compliance), and being able to support complex deployments and modern DMZs, are weighted heavily.

- **Overall Viability:** This 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 vs. key competitors (which is compared to Gartner data on such competitions held by our customers) and devices in deployment. Firewalls shipped are not a key measure of execution. Instead, we consider use of these firewalls to protect the key business systems of Gartner enterprise clients.
- **Sales Execution/Pricing:** This includes pricing, deal size, the installed base (and use by enterprises, carriers and MSSPs), the strength of sales and distribution operations in the vendors. Pre- and post-sales support are evaluated. Pricing was 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. TCO over a typical firewall life cycle (three to five years) was assessed, as was the pricing model for conducting a refresh, while staying with the same product and replacing a competing product without intolerable costs or interruptions.
- **Market Responsiveness and Track Record:** This includes the 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 provider's history of responsiveness.
- **Market Execution:** This addresses awareness of the product in the market. We recognize companies that are consistently identified by Gartner clients and often appear on their preliminary shortlists.
- **Customer Experience and Operations:** This includes management experience and track record and 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 IPS capability and how the firewall fared under attack conditions.

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

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 and an

overall understanding and commitment to the security market (specifically the network security market). 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 yearly 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 that market directions will change.

- **Sales Strategy:** This includes pre- and post-product support, value for pricing, and 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.
- **Offering Strategy:** The emphasis is on the vendor's product road map, current features, NGFW integration, virtualization and performance. Credible independent third-party certifications, such as Common Criteria, are included. Integrating with other security components is also weighted, as well as product integration into other IT systems. As threats change and become more targeted and complex, we highly weight vendors with road maps toward being able to move beyond pure signature-based, deep-packet inspection techniques.
- **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 product innovation, such as R&D, and quality differentiators, such as performance, virtualization, 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 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, 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

Evaluation Criteria	Weighting
Geographic Strategy	standard

Source: Gartner

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. 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 options for hardware acceleration.

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 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. 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.

Visionaries

Visionary vendors have the right designs and features for the enterprise, but they lack the sales base, strategy or financial means to compete with the leaders and challengers. Most visionary products have good NGFW 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.

Niche Players

Most vendors in the Niche Players quadrant are smaller vendors of enterprise firewalls or UTM 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-adverse" 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.

Vendor Strengths and Cautions

Astaro

Strengths

- Astaro's leverage and integration of a wide range of open-source components provide an attractive price point.
- It focuses on the requirements of enterprise customers.
- Its Novell relationship feeds its pipeline.

Cautions

- Astaro has limited visibility outside of Europe, the Middle East and Africa (EMEA) and outside of its Novell channel.
- Its UTM focus is less a match for enterprises and better for SMBs. Astaro is short on enterprise features.
- Astaro has broad capabilities (such as e-mail security features) that often exceed enterprise needs.

Check Point Software Technologies

Strengths

- Check Point Software Technologies is a well-known pure-play security company with a well-entrenched installed base and channel partners.
- Check Point is primarily a software provider, with a broad range of third-party platform providers, led by companies such as Nokia and Crossbeam Systems. SecurePlatform can be loaded onto off-the-shelf servers, and Check Point has a new appliance for midsize businesses.
- It has a strong field of product options, such as VSX for virtualized firewalling and its Eventia security information and event management (SIEM) product.
- Check Point has a strong and mature management interface with the ability to handle complex DMZ deployments and large numbers of devices.
- The vendor recently added a stand-alone IPS product in IPS-1. Although it is not an on-the-firewall option, it is a good competitive move. This technology was based on the NFR acquisition (see "NFR Deal Will Bring Check Point Into IPS Market").

Cautions

- Although Check Point has lowered prices on models aimed at small businesses, enterprise prices are high. Products may be expensive for enterprises with low-end requirements or static networks/users.
- The SmartDefense deep inspection option needs an update; however, Gartner expects Check Point to provide competitive IPS capabilities using the acquired NFR technology.
- Check Point is overly secretive about its road map and longer-term strategies, leaving its customers guessing.

- Dealing with the platform provider as a middleman can be frustrating. Service complaints about Check Point from Gartner customers are more common than from users of competing products.

Cisco

Strengths

- Cisco offers a single invoice, high discounts and a vendor relationship for "all-Cisco" networks, and it has a large market share.
- Adaptive Security Appliance (ASA) is a good replacement for PIX, and an add-in IPS module can replace a stand-alone IPS.
- Cisco offers a wide choice in platforms, with ASA, Firewall Services Module blade for Catalyst switches and Integrated Services Router.
- The vendor has strong channels, broad geographic support and the availability of other security products, such as the Cisco Security Agent; its Monitoring, Analysis and Response System SIEM; and IPS products.

Cautions

- 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.
- The vendor's management and consoles are not as rich as competing offerings.
- Like most competitors, Cisco offers limited integration between the firewall and the IPS.
- Future feature improvements for Cisco's enterprise firewall products are an unknown, which can provide openings for competitors after the initial successes of its ASA product.

Fortinet

Strengths

- Fortinet has increased its wins against market leaders.
- It has good performance from purpose-built hardware and a wide model range, including bladed appliances for large enterprise and carriers, as well as SMB and branch-office solutions.
- Fortinet is price-competitive, especially with multiple virtual domains.
- It offers ease of deployment.

Cautions

- Like most competing enterprise firewalls, Fortinet does not have a mature NGFW.
- It has experienced anecdotal support and delivery pains resulting from growing at a fast rate.
- Marketing using UTM and antivirus firewall labels undervalues its enterprise offerings.

- Fortinet has limited support by MSSPs outside the Asia/Pacific region.

Juniper Networks

Strengths

- Juniper Networks has a strong enterprise option in Juniper Secure Services Gateway for high-end, purpose-built appliances.
- It has a good branch-office firewall and recognizes that enterprises want the same vendor for central and branch deployments.
- It has good networking support for routing, protocol support and port composition.
- Juniper has strong NAC integration across firewalls and the rest of its product line.
- Customers report good support from Juniper.

Cautions

- As a network infrastructure vendor rather than a pure-play security vendor, Juniper faces heavy competition from 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.
- Juniper is generally high priced and often allows competitors an opening on price alone.

NETASQ

Strengths

- NETASQ has a good mix of advanced features in comparison to competitors in class.
- It is focused on the requirements of enterprise customers and provides good channel support.

Cautions

- The vendor has a narrow international base, with almost all its deployments in EMEA.
- Its UTM focus is less a match for enterprises and better for SMBs.

phion

Strengths

- Designed for enterprises, phion is a good alternative to established large competitors.
- Enterprise customers have well-established local support in German-speaking countries and Eastern Europe.
- The vendor has an MSSP-friendly design.
- It has developed NGFW capabilities, although with a limited IPS signature set.

Cautions

- It has a narrow international base, with most deployments in EMEA.
- The vendor has limited market visibility for its Netfence firewall.
- Its product family includes Web optimization controller capabilities that may divert resources from main network security areas.

Secure Computing

Strengths

- Secure Computing has increased its market visibility, product set and potential for execution after its CipherTrust acquisition (see "CipherTrust Buy a Bold but Challenging Move for Secure Computing").
- It 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 strong cross-selling opportunity.
- It has a reputation of producing secure products, having greatly improved support and being a well-established firewall player.

Cautions

- Secure Computing is slow to innovate and respond to the wider firewall market from its established base.
- It has low market visibility against market leaders as a result of positioning itself as a second-line firewall and as an alternative to stateful inspection firewalls.

SonicWALL

Strengths

- SonicWALL's competitive prices have resulted in good solutions for wide remote-office deployments and SMBs.
- It has the reputation and track record of strong channel support.
- The vendor's aggressive acquisitions provide rapid technology refresh, such as its recent Aventail Secure Sockets Layer VPN acquisition.
- It has shipped a large number of appliances.

Cautions

- SonicWALL's product focus has been on SMBs. Its products are not competitive in most enterprises. "Enterprise" has really meant "midsize companies" in SonicWALL's product portfolio.
- Its acquisitions can divert attention and resources from the main network security market.

Stonesoft

Strengths

- Enterprise focus makes StoneGate firewalls distinct from most European competitors, which focus on SMBs.
- It has a StoneGate firewall version for IBM zSeries mainframes.
- Stonesoft provides support for clustering and high availability for the few enterprises that do not provide for this in the infrastructure outside the firewall.
- It has a robust performance and feature set relative to company resources.

Cautions

- Stonesoft has limited market visibility outside of EMEA.
- Its company size is small relative to competitors in the enterprise market.
- It's missing a few features that bigger competitors have, such as Layer 2-mode support.

WatchGuard Technologies

Strengths

- WatchGuard Technologies' competitive prices have resulted in good solutions for wide remote-office deployments.
- After taking the company private, its new management team is well-focused on the core competence of servicing the SMB market.

Cautions

- WatchGuard is in a rebuilding mode. Gartner expects continued product focus on SMB products because its current firewall offerings are not enterprise-class.

RECOMMENDED READING

"Understand the Critical Issues Involved in Securing Your Network"

"Magic Quadrant for Network Intrusion Prevention System Appliances, 2H06"

"Magic Quadrants and MarketScopes: How Gartner Evaluates Vendors Within a Market"

Acronym Key and Glossary Terms

ASA	Adaptive Security Appliance
DMZ	demilitarized zone
EMEA	Europe, the Middle East and Africa
IPS	intrusion prevention system
MFA	multifunction appliance
MSSP	managed security service provider

NAC	network access control
NGFW	next-generation firewall
SIEM	security information and event management
SMB	small or midsize business
TCO	total cost of ownership
UTM	unified threat management
VPN	virtual private network

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, skills, etc., 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 pre-sales activities and the structure that supports them. This includes deal management, pricing and negotiation, pre-sales 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), availability of user groups, service-level agreements, etc.

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 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 Web site, 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 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 verticals.

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.

REGIONAL HEADQUARTERS

Corporate Headquarters

56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters

Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters

Gartner Australasia Pty. Ltd.
Level 9, 141 Walker Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Japan Headquarters

Gartner Japan Ltd.
Aobadai Hills, 6F
7-7, Aobadai, 4-chome
Meguro-ku, Tokyo 153-0042
JAPAN
+81 3 3481 3670

Latin America Headquarters

Gartner do Brazil
Av. das Nações Unidas, 12551
9º andar—World Trade Center
04578-903—São Paulo SP
BRAZIL
+55 11 3443 1509