

Magic Quadrant for Personal Firewalls, 1Q06

Gartner RAS Core Research Note G00139942, John Girard, 27 June 2006, R1901 06302007

Personal firewalls extend company firewall policy to block attacks against workstations and mobile devices that travel outside the company perimeter, and they will slow or stop attacks from infected systems. This market drives buying decisions into larger endpoint defense suites.

WHAT YOU NEED TO KNOW

In 2010, personal firewalls (PFWs) will be an integral part of client computing. Over time, all end users' workstations – desktops, laptops, PDAs or phones – will be equipped with PFWs. Basic firewall functionality (inbound port defenses) is available today in Windows XP Pro, Windows 2003 and Windows Vista. But buyers are willing to spend extra money and effort to gain comprehensive two-way protection that adapts to multiple network contexts (that is, in the office, traveling, wireless, and so on) In 2006, enterprises view PFWs as components of larger suite-style integrated endpoint intrusion prevention systems (IPSS).

Market Overview

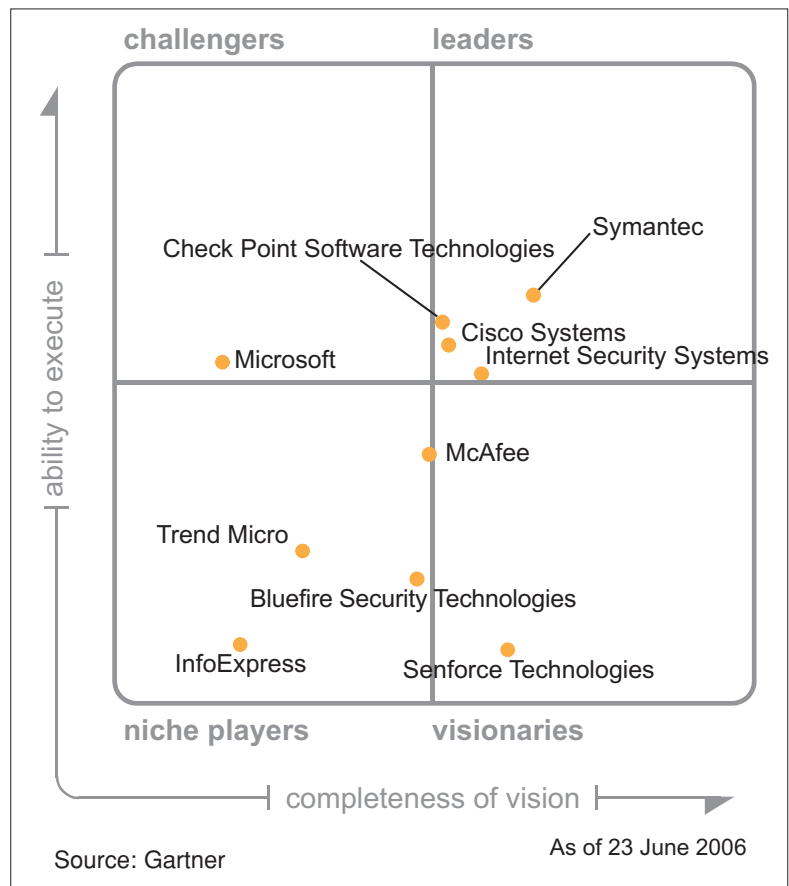
PFWs are the first line of defense at the device level. PFWs are needed because PCs, PDAs and smartphones increasingly require local defense of their network services and applications. They are used outside the purview and protection of company firewalls and in-building wired LANs. Individual remote and mobile end-user computing devices have become targets for attacks that cannot be consistently prevented by corporate firewalls because wireless and mobile systems are highly connectable – they can associate with a variety of networks as well as to each other without benefit of the isolation of an enterprise LAN.

The PFW market in 2006 is transitioning from best-of-breed products to endpoint security suites that combine PFW with malicious code defenses, such as antivirus and anti-spyware,

and policy enforcement based on physical device port defense and some form of network access control (NAC). Seven of the 10 vendors tracked for this document – Bluefire Security Technologies, Check Point Software Technologies, Internet Security Systems (ISS), McAfee, Symantec, Senforce Technologies and Trend Micro – offer PFWs as part of larger endpoint security suites under a single management console, and they are moving away from selling stand-alone PFW products. The typical enterprise is weary of maintaining separate consoles and policies for antivirus, anti-spyware, PFW, device port defense and other related endpoint security processes. However, the PFW component of security suites is most likely to drive suite purchases. If the enterprise buyer does not find the PFW component

MAGIC QUADRANT

Figure 1. Magic Quadrant for Personal Firewalls, 1Q06



to be compelling, stand-alone products will still be purchased.

This document will be the last PFW Magic Quadrant. Starting in 2007, the Magic Quadrant will shift to examine converged PFW and host intrusion prevention system (HIPS) solutions, and their role within endpoint security suites.

Market Definition/Description

We define PFWs as software utilities added to a workstation (laptop or desktop) or smaller device (PDA or smartphone). PFWs detect and minimize the threat of malicious access to system resources through inbound and outbound network connections. Network access may be fully blocked, or allowed for certain operations, applications, network connections or Transmission Control Protocol (TCP) ports. Because the PFW runs on a user platform, it can combine host and network protection. Competitiveness is driven by the ability to recognize and block new forms of suspicious network activities and to track attacks to specific applications using a combination of newer behavioral analysis techniques and signatures. PFWs can be independent of, bundled with, or integrated with the operating system (OS) or other anti-malicious software (anti-malware), such as antivirus.

Ten companies appear on the Magic Quadrant for 2006. All of the companies ranked or mentioned in this document can shield your systems from common port attacks and provide client firewall policy management features. One company specializes in PDA/smartphone firewalls, and nine concentrate on Windows platforms.

Inclusion and Exclusion Criteria

Inclusion Criteria

PFW companies that meet the market definition and description were included according to the strength of these attributes:

- A PFW product was sold in 2005 for a sufficient length of time to gather market attention. Products released in the first quarter of 2006 may contribute to vision.
- Seats sold and under contract are reported or estimated at 500,000 or more for major vendors, although smaller vendors may be considered for outstanding vision on a case-by-case basis.
- Gartner analysts have a generally favorable opinion about the company's ability to compete in the market.
- Gartner clients generate inquiries and feedback about the company.
- The company regularly appears on shortlists for final selection.
- The company demonstrates competitive presence and sales to Gartner analysts.
- Gartner analysts consider that aspects of the company's product execution and vision are important enough to merit inclusion.

Exclusion Criteria

PFW companies that were not included in the document might have been excluded for one or more of the following conditions:

- Companies that were invited to participate but did not reply to an annual request for information and do not otherwise meet the inclusion criteria
- Companies with minimal or negligible apparent market share among Gartner clients, or with no shipping products

The Magic Quadrant is copyrighted June 2006 by Gartner, Inc. and is reused with permission. The Magic Quadrant is a graphical representation of a marketplace at and for a specific time period. It depicts Gartner's analysis of how certain vendors measure against criteria for that marketplace, as defined by Gartner. Gartner does not endorse any vendor, product or service depicted in the Magic Quadrant, and does not advise technology users to select only those vendors placed in the "Leaders" quadrant. The Magic Quadrant is intended solely as a research tool, and is not meant to be a specific guide to action. Gartner disclaims all warranties, express or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

© 2006 Gartner, Inc. and/or its Affiliates. All Rights Reserved. Reproduction and distribution of this publication in any form without prior written permission is forbidden. The information contained herein has been obtained from sources believed to be reliable. Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information. Although Gartner's research may discuss legal issues related to the information technology business, Gartner does not provide legal advice or services and its research should not be construed or used as such. Gartner shall have no liability for errors, omissions or inadequacies in the information contained herein or for interpretations thereof. The opinions expressed herein are subject to change without notice.

- Companies that are not the original manufacturer of PFW products

Two companies were considered but not added to the 2006 report:

- Tiny Software's PFW has been excluded in previous reports for lack of market influence. CA acquired this product, but it did not market the product as an enterprise solution in 2005, and in the time frame of this report, it had not released a bundled IPS product containing a PFW.
- Danware Data introduced a new stand-alone PFW in 2005. However, it has neither generated client inquiry nor competitive response from incumbent vendors.

Added

No new vendors were added to the 2006 report.

Dropped

Two vendors have been removed from the report:

- Credant Technologies has stopped selling its product as a PFW, instead concentrating on its core market for mobile data protection.
- Sygate Technologies was acquired by Symantec, so the PFW is now ranked under the name of Symantec.

Evaluation Criteria

Ability to Execute

Execution considers factors related to getting products sold, installed, supported and in users' hands. 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, nor is it primarily about sales. In a mature market, such as PFWs, strong functionality and interoperability with other security and management products/systems are essential.

Product/Service compares the completeness and appropriateness of core PFW products sold for use in the enterprise remote-access market. The PFW market defined in this document is product-focused, but related service areas may contribute, including consulting services and managed service resellers, and so on. This factor is critical to demonstrating that the vendor can generate market awareness.

Overall Viability considers company history and demonstrated commitment in the PFW market, and the difference between a company's stated goals for the evaluation period vs. the company's actual performance compared with the rest of the market. Growth of the customer base and revenue derived from sales are also considered. All vendors were asked to disclose comparable market data, such as PFW revenue, number of unique companies under contract, and information about seats sold year by year (defined as concurrent active license seats deployed on sold products).

Sales Execution/Pricing compares the strength of sales and distribution operations in the vendors as well as discounted list pricing for investments in seats ranging from fewer than 100 to more than 10,000. Pricing was compared in terms of first-year cost-per-concurrent active license seats, including cost of all hardware and support. Low pricing increasingly contributes to client interest; however, buyers want demonstrable peace of mind more than they want bargains, and they respond more strongly to sales techniques led by case studies and return on investment (ROI) projections.

Market Responsiveness and Track Record, and Marketing Execution rate competitive visibility as the key factor, including which vendors are most commonly considered top competitive threats – generally during the request for proposal (RFP) process – and also, which are considered top threats by each other. In addition to buyer and analyst feedback, this ranking considers which vendors consider each other to be direct competitive threats. Strong ratings mean that a company has demonstrated to Gartner analysts that it can get in RFPs early and ultimately win a large percentage in competition with other vendors.

Customer Experience is subjectively rated from client feedback to analysts; from opinions of Gartner analysts in security, network and platform research groups; and from vendor-supplied references, where needed.

Operations consider the ability of a vendor to pursue its goals in a manner that enhances and grows its influence in all execution categories.

Table 1. Ability to Execute Evaluation Criteria

Evaluation Criteria	Weighting
Product/Service	standard
Overall Viability (Business Unit, Financial, Strategy, Organization)	standard
Sales Execution/Pricing	standard
Market Responsiveness and Track Record	standard
Marketing Execution	standard
Customer Experience	standard
Operations	standard

Source: Gartner

Completeness of Vision

Market Understanding and Marketing Strategy are assessed through direct observation of the degree to which a vendor's products, road maps and mission anticipate leading-edge thinking about buyers' wants and needs. Gartner makes this assessment subjectively by several means, including interaction with vendors in briefings, and by reading planning documents, marketing and sales literature, and press releases. 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 market directions change. Also considered are the vendor's partnerships with vendors in related endpoint security markets, including antivirus, anti-spyware, configuration management, authentication, device identification, virtual private network (VPN), data encryption, gateway firewalls, and so on.

Sales Strategy examines the vendor's strategy for selling products, including sales messages, techniques, marketing, distribution and channels. This topic is considered in execution; it does not apply to product vision, which is ranked in terms of investment in functionality.

Offering (Product) Strategy is ranked through an examination of the breadth of functions, platform and OS support for the PFW client. R&D investments are credited in this category.

Business Model takes into account a vendor's underlying business objectives for its products and its ongoing ability to pursue R&D goals in a manner that enhances all vision categories.

Vertical/Industry Strategy considers a vendor's ability to communicate a vision that appeals to specific industries and verticals. This Magic Quadrant doesn't consider verticals as a distinctive ranking factor; therefore this category is irrelevant.

Innovation takes into consideration the degree to which vendors invest in core requirements for successful use of their products.

Geographic Strategy takes into account a vendor's strategy to direct resources, skills, products and services globally. All vendors are ranked in this Magic Quadrant for their performance as a whole, and in the frame of reference of Gartner clients, therefore, this category is not required.

Table 2. Completeness of Vision Evaluation Criteria

Evaluation Criteria	Weighting
Market Understanding	standard
Marketing Strategy	standard
Sales Strategy	no rating
Offering (Product) Strategy	standard
Business Model	standard
Vertical/Industry Strategy	no rating
Innovation	standard
Geographic Strategy	no rating

Source: Gartner

Leaders

Leaders demonstrate balanced progress and effort in all execution and vision categories. Their actions raise the competitive bar for all products in the market, and they can change the course of the industry. A leading vendor is not a default choice for every buyer, and clients are warned not to assume that they should buy only from vendors in the Leaders quadrant. Some clients may actually feel that leaders are spreading efforts too thinly and not pursuing their special needs.

Challengers

Challengers have solid products that address the typical needs of the market with strong sales, visibility and clout that add up to higher execution than niche players. Challengers are good at winning contracts, but they do so by competing on basic functions rather than on advanced features. Challengers are efficient and expedient choices to narrowly defined access problems. Many clients consider challengers to be the conservative safe alternative to niche players.

Visionaries

Visionaries invest in the leading/"bleeding"-edge features that will be significant in the next generation of products and will give buyers early access to improved security and management. Visionaries can affect the course of technological developments in the market, but they lack the execution influence to outmaneuver challengers and leaders. Clients pick visionaries for best-of-breed features, and in the case of small vendors, they may enjoy more personal attention.

Niche Players

Niche players offer viable, dependable solutions that meet the typical needs of buyers. Niche players are less likely to appear on shortlists but fare well when given a chance. While they generally lack the clout to change the course of the market, they should not be regarded as merely following the leaders. Niche players may address subsets of the overall market, and often they can do so more efficiently than the leaders. Clients tend to pick niche players when stability and focus on a few important functions and features are more important than a wide and long road map.

Vendor Comments

Bluefire Security Technologies

Bluefire Security is the only company ranked in 2006 that specializes exclusively in PDA and smartphone platforms, and it has no real competition from the major Windows players. Bluefire Mobile Security (BMS) is a comprehensive security platform combining PFW, VPN, URL filtering and mobile data encryption. Interoperability has been tested with eight mobile antivirus vendors, and a partnership with Symantec is used to improve sales into laptop

accounts and to provide support for Cisco Network Admission Control (CNAC) and Microsoft Network Access Protection (NAP). Early growth was fueled by government buyer concerns over Bluetooth, because BMS can eliminate, enforce and audit Bluetooth usage. 2005 sales were stimulated by a large (500,000 seat) original equipment manufacturer deal with Motorola, which brought total seats under maintenance to a respectable 595,000. Bluefire also captured users seeking an alternative to Certicom's movianVPN, which was discontinued in the fourth quarter of 2004. Bluefire could be challenged if mobile data protection vendors begin to flaunt their firewalling features, but overall, BMS is the most complete security suite on a small device and, therefore, deserves inclusion in the report.

Check Point Software Technologies

Check Point invests broadly in its functional vision to protect against different types of attacks and continues to build on Zone Labs' technology, including expanded features for on-demand protection as well as integration of the PFW, Integrity management and SmartCenter management across all product lines. Sales are growing, but Check Point struggles to get visibility on Gartner client shortlists because it doesn't aggressively market against its competition. Check Point relies on a combination of direct and co-branded marketing with distributors and resellers. Check Point has positioned its Integrity products to not be perceived as a lock-in solution, and its PFW integrates easily with VPNs. But the fact that Check Point sells its own VPN hardware lines puts it in competition with other vendors, particularly Secure Sockets Layer (SSL) VPN vendors, which are in a position to license and resell independent software vendors' (ISVs') Windows PFWs and on-demand security products. Cisco faces a similar situation because it owns VPN hardware lines, but its endpoint security products were never in a position to challenge ISVs. In contrast, Check Point purchased Zone Labs, ending Zone Labs' run as an ISV.

Cisco Systems

Cisco Systems' Cisco Security Agent (CSA) has behavioral blocking, physical port controls and learning capabilities that form the basis for a leader vision ranking. Good general visibility, network industry clout and sales growth earned Cisco a

leader execution rating. CSA is integrated with CNAC via the Cisco Trust Agent (CTA), but it is not a broad HIPS suite capable of challenging a company such as Symantec. Cisco's view of network-centric IPS is understandable given its history, but it masks some of the important work it has done on application execution policies. Cisco's on-demand protection suite (Cisco Secure Desktop) counted minimally toward vision because it is kept separate and captive in the WebVPN product line. Cisco claims that its rule-based system does not require updates to maintain endpoint protection; however, that message has confused some potential buyers, because the agent policies are designed to be updated, and should be updated, in our opinion, particularly when new application-specific threats appear. Clients report that some sales presentations continue to suggest that CSA is a replacement for antivirus/anti-spyware protection. That is too radical a step for typical desktop security buyers, and Cisco should emphasize its ability to work within enterprise end-user IT frameworks.

InfoExpress

Info Express did not return our survey but has been ranked as a niche player from client and analyst feedback. The company is focusing its R&D efforts on NAC products and is using CyberArmor as a value-added component of CyberGatekeeper 4.0. The PFW itself has not changed appreciably since 2005, but it is still advertised and sold as a stand-alone PFW and offers solid baseline protection.

Internet Security Systems

ISS enjoyed strong PFW sales during the past three years and deservedly earned an increase in execution. However, client inquiry and feedback was minimal; ISS is not readily recognized by clients as a major player in the PFW market. ISS has transitioned to the new Proventia enterprise product name, and we are hopeful that product names will not be changed again, so that the company can rebuild brand awareness. ISS is developing on-demand security technologies, but it is a year behind our expectations. Still, ISS has a compelling day zero "protection story" in its full Windows client, owing to both an efficient behavior blocking method that requires neither rules nor signatures and a well-designed virtual patch service to help clients stay ahead of new Windows vulnerabilities. ISS could

improve vision by engaging in more partnerships with vendors in related security and device management markets, by adding more wireless network awareness, and by expanding to non-Windows platforms.

McAfee

McAfee's Desktop Firewall vision has improved because of strengthening of its functions and progress on its larger endpoint IPS product. The company has moved the stand-alone PFW to end of life and is transitioning to a bundled HIPS product (McAfee Host Intrusion Prevention 6.0), which was released in late February 2006 – too late to drive execution sales ranking for this report. McAfee's ePolicy Orchestrator will manage Symantec's antivirus and anti-spyware products as a convenience to the buyer. McAfee is also building out support for NAC, both for its own product and also for third parties. McAfee could improve vision as well as sell-through execution opportunities by increasing interoperability and partnerships with vendors in related security markets, because clients increasingly state interoperability and console consolidation to be important purchasing decisions. Gartner clients do not indicate in feedback to analysts that the PFW component is a driver for McAfee purchases. To improve execution for 2007, McAfee needs to compete aggressively on the firewall defenses built into its new HIPS product, which creates a foundation for a strong play in future desktop protection.

Microsoft

Microsoft's Windows XP Firewall doesn't measure up to third-party products. It can block inbound port scans and has limited rules to block suspicious events or data. Administrators may quickly update blocking policies for systems connected to the LAN. However, the process is one-way, lacking comprehensive central reporting or analysis, and it requires an online Active Directory connection to distribute Group Policy updates. The user agent may incorrectly tell users that software such as antivirus is out of date. A company that cannot afford to buy a third-party product should at least turn the XP Firewall on, and it can be used on desktops connected to a LAN as a minimal line of defense. Senforce and Symantec are the only PFW companies that will distribute updates to the

Windows XP Firewall, verify the updates are installed and enforce a policy requiring use of the Windows Firewall. Other vendors either ignore the Windows XP Firewall or call for it to be shut down on the assumption that their product will replace it. Microsoft continues to earn a strong niche ranking for the XP Firewall, but vision will be hampered in the near future, because the upcoming Vista Firewall will face similar problems, and Microsoft's decision at this point in time is to default-disable outbound firewall protection.

Senforce Technologies

Senforce continues to earn high vision marks for superior tactical PFW functionality, including the ability to manage the Windows Firewall and the beginnings of an on-demand security toolset. Execution remains low because sales efforts and visibility are not generating awareness among Gartner clients polled during inquiries, and seat deployments are at the low end of the market range. "Mind share" through case studies is hampered by confidentiality demands from Senforce's clients. Senforce has increased its press coverage for technology, but what is needed most is solution-oriented marketing and sales. Senforce is below the report threshold of installed seats for major vendors but needs recognition for vision. Senforce will need to grow sales substantially to be included in future rankings.

Symantec

Symantec made two acquisitions in 2005 that not only earned it the top vision rating, but also challenged other vendors to show improved vision. First, it acquired Sygate, which easily held the lead for early and aggressive investments in on-demand security and application policy, integration with third parties, comprehensive network access controls, and control of the Windows Firewall. Second, it acquired WholeSecurity, which held the lead for predictive, behavioral profiling of malicious code. Symantec published a 2006 road map that melds all of its full-client and on-demand endpoint protection products into a single line, from small mobile devices, through laptops and on to desktops. Short-term execution has suffered for clients that were in the middle of moving into and between Symantec and Sygate products, but Symantec will recover quickly to offer the most complete set of protections across the largest number of platforms and OSs.

Trend Micro

Trend Micro's greatest strengths are in antivirus and anti-spyware products. The PFW component of its suite ranks as niche for vision, which means it is good enough to protect against common port attacks and integrates to a single console. Gartner clients do not cite the PFW component as a critical purchasing factor; therefore, integration with antivirus and anti-spyware products do not contribute strongly to execution. To improve execution, Trend should expand its PFW vision functionality to compete with the breadth of Symantec and Senforce. Although Trend does not currently possess a suite of on-demand security tools that compete in the remote access market, its HouseCall Web page tools could be transformed into future on-demand security products.

Note 1

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.