

# Magic Quadrant for Endpoint Protection Platforms, 2007

Gartner RAS Core Research Note G00153291, Peter Firstbrook, Arabella Hallawell, John Girard, Neil MacDonald, 21 December 2007 RA5 01052009

The stand-alone antivirus market has been replaced with a broader suite of defensive technologies supported by an extensible management platform that can subsume horizontal products, such as data protection and device management capabilities.

## WHAT YOU NEED TO KNOW

Point products for antivirus, anti-spyware, personal firewalls and host-based intrusion prevention (HIPS) are rapidly being replaced by suites with a centralized and extensible management framework. The management and reporting capability of endpoint protection platform (EPP) suites is a substantial differentiator, especially in large enterprises. A modular architecture that enables selective configuration based on security requirements and device location is also critical. EPP suites are being extended with new capabilities, such as encryption and data loss prevention (DLP). Management of end-node protection will increasingly duplicate operational management capability and eventually subsume these tools for small or midsize businesses (SMBs).

## Market Overview

The traditional point product antivirus, anti-spyware and personal firewall markets have been eclipsed by broader suites of related security technologies, which Gartner has labeled the EPP. Basic component technologies in EPP suites include antivirus, anti-spyware, HIPS and a personal firewall. Advanced EPP suites will include network access control (NAC) and data protection technologies, such as DLP and full-disk encryption. The requirements for holistic NAC solutions and the demanding management needs of large enterprise are also forcing EPP suites to replicate some PC configuration life cycle management tasks, such as security configuration management, asset discovery, patching and software management. By combining multiple co-related technologies into a single management framework, EPPs have the promise of increasing security while lowering complexity, cost and administrative overhead.

Spyware and virus threat databases and scan engines have largely merged into a single signature-based anti-malware agent. Although there are subtle differences in the speed and detection rates of anti-malware databases, this component is largely viewed as a commodity by buyers. Even the best signature databases can miss the wild threats 2% to 10% of the time, and most have less than a 50% chance of catching completely new threats. Signatures are extremely ineffective against targeted threats and zero day threats. HIPS and personal firewalls are increasingly critical to improve overall security. The convergence of these functions into a common management framework should increase the adoption of HIPS and desktop personal firewalls.

Enterprise interest in stand-alone personal firewalls has declined considerably as the capability of EPP suite firewalls has improved and given that Microsoft's entry-level personal firewalls are already included with Windows. Security-conscious enterprises want more-advanced firewall functionality at least for their mobile population.

Advanced features that define more-visionary firewalls include:

- ¥ Audit capabilities and protections to ensure that the firewall policy is active
- ¥ Detailed event logs
- ¥ Verified updates to firewall settings
- ¥ Coordinated use of firewall in conjunction with malware protection for the rapid defense of unpatched vulnerabilities
- ¥ Wireless firewall policies, such as enforcing one active network interface card (NIC) to avoid LAN-to-wireless-LAN bridges
- ¥ Firewall policies applied locally to application network traffic and rights management

Organizations should evaluate EPP firewalls and plan to phase out stand-alone personal firewall solutions.

**Figure 1. Magic Quadrant for Endpoint Protection Platforms, 2007**



HIPS technologies are critical to secure endpoints from more-evasive, targeted and zero-day threats. Advanced HIPS solutions use various protection styles to provide layers of defense at endpoints, including:

- ¥ Protocol anomaly detection
- ¥ Deep-packet inspection for known network attack signatures or vulnerability attack signatures
- ¥ Simulation of potentially malicious code before it executes by using static analysis, code simulation or virtual machines
- ¥ Genetic heuristics, which is the use of broad signatures to detect variants using common malware family characteristics

The Magic Quadrant is copyrighted December 2007 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.

© 2007 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.

- ¥ Comprehensive buffer overflow and program flow control protection
- ¥ Advanced application control to determine which applications are allowed to execute and to restrict system resource access
- ¥ Sandboxing and other virtualization techniques to inspect and isolate potentially malicious code from causing damage to the endpoint
- ¥ Behavior-based analysis of executing code to determine whether it is behaving maliciously and providing the capability to undo the damage and remove the malware

Visionary HIPS solutions must enable selection and configuration/tuning to balance the security level, transparency to end users and administration overhead. Solutions should provide preconfigured out-of-the-box templates for common application and system configurations, as well as a learning mode for custom applications.

The management capability of EPP suites is a substantial differentiator. Simply maintaining the security status for large PC fleets that are increasingly mobile for long periods of time is difficult. As NAC becomes an integrated feature of EPP suites, management capability has been forced to expand from simply maintaining the security posture of the EPP components to checking the security configuration, software inventory and patch levels. The new EPP management consoles are beginning to add PC configuration life cycle management capabilities to ensure the security and integrity of clients. Meanwhile, some PC life cycle operations vendors are starting to add defensive security tools to their offerings. These two markets will continue to slowly converge, although it will not be until after 2010 that a significant percentage of the market will buy completely integrated tools from a single vendor.

### Market Definition/Description

Enterprise antivirus, anti-spyware, personal firewall and desktop HIPS products make up the majority of endpoint security spending. The combined revenue of these segments was more than \$2.2 billion in 2005, and we anticipate that the EPP market will grow to nearly \$3.6 billion by 2010.

This market is still dominated by the market share of the big three traditional antivirus vendors (McAfee, Symantec and Trend Micro), which represent roughly 85% of the market share. However, many nimble vendors are beginning to challenging the status quo with innovative EPP solutions and a higher level of customer focus.

Microsoft's impact on the enterprise market is still nascent; however, we expect it to have a growing market share, starting primarily in Microsoft-centric SMBs.

Despite the introduction of new players, the displacement of incumbents is still a significant challenge. The biggest impact of the challengers and visionaries is to push the dominant players in the market to invest in new features and functionally and to keep pricing rational.

### Inclusion and Exclusion Criteria

Inclusion in this Magic Quadrant is limited to vendors that meet the following minimum criteria:

- ¥ Products must provide malware (virus, spyware, rootkits, trojans and worm) detection and cleaning, a personal firewall and/or some form of host intrusion prevention (such as application control, buffer overflow protection, behavioral monitoring and enforcement, and heuristics) capability for PCs.
- ¥ Vendors must have centralized management, configuration and reporting capabilities for the products listed above that can support companies that have, at a minimum, 5,000 geographically dispersed endpoints.
- ¥ Vendors must have global service and support organizations to support enterprise products.

### Added

Numerous vendors were added to the Magic Quadrant this year as a result of the evolution to endpoint protection platforms and the more liberal inclusion criteria. New entrants include BigFix, Bit9, Check Point Software Technologies, eEye Digital Security, IBM, Kaspersky Lab, LANDesk, Microsoft and Webroot Software.

### Dropped

No vendors were removed.

### Evaluation Criteria

#### Ability to Execute

Our key ability to execute criteria used to evaluate vendors were overall viability, and market responsiveness and track record.

- ¥ Overall viability: This included an assessment of financial resources, such as the ability to make necessary investments in new products or channels, and the experience and focus of the executive team. We also looked at the business strategy of each vendor's endpoint protection division and how significant that division is to the overall company.
- ¥ Market responsiveness and track record: We evaluated each vendor's track record in bringing new products and features to customers in a timely manner, as well as the market share of the vendors.
- ¥ Sales execution: We evaluated the vendor's licensing and pricing programs and practices. We incorporated feedback from clients and references on negotiation experiences. We also looked at the strength of channel programs, geographic

presence and the track record of success with technology or business partnerships.

- ¥ Marketing execution: We evaluated the frequency of vendors appearance on shortlists and RFPs, according to Gartner client inquiries, and reference and channel checks. We also looked at brand presence and visibility in the market.
- ¥ Customer experience: We primarily evaluated product stability and performance, company experience with the vendor's support, and signature quality and response times. We evaluated comments from Gartner clients and reference customers, as well as from tests, such as AV-Test.org, and other sources of data on performance and signature response times.

### Completeness of Vision

The most important vision criteria were market understanding and the product offering.

- ¥ Market understanding: In this category, vendors that understand customer requirements for proactive and integrated defenses across all malicious software (malware) threat types and have an innovative and timely road map to provide these functionalities scored best.
- ¥ Offering/product: When evaluating vendors' product offerings, we looked at the following product differentiators:
  - ¥ Anti-malware signature capabilities: speed, accuracy, transparency and completeness of signature-based defenses
  - ¥ HIPS capabilities: the quality, quantity, accuracy and ease of administration of non-signature-based defenses
  - ¥ Personal firewall capabilities: advanced capabilities that exceed Microsoft's, such as location-based policy, specific virtual private network (VPN) and wireless rules, and Universal Serial Bus (USB) and other port protection
- ¥ Management and reporting capabilities: comprehensive centralized reporting that enhances the real-time visibility of end-node security state and administration capabilities that ease the management burden of policy and configuration development
- ¥ Horizontal integration: the quantity and quality of integrated-related products or technology, such as NAC, full disk

encryption, data leak prevention, and e-mail and Web gateways. These related products enable vendors to become more-strategic suppliers to organizations and offer the promise of lower administration costs and better security through simpler policy administration and monitoring, and correlated threat information.

- ¥ Sales strategy: We evaluated each vendor's licensing and pricing programs and practices. Vendors that emphasized value to clients, tended to incorporate new functionality without upcharges and were reasonable during renewal negotiations received high scores. We incorporated feedback from clients, reference customers and channel partners on negotiation tactics and pricing strategies. We also evaluated the vendors' partnership strategies. We accounted for how vendors approached new channels and delivery models.
- ¥ Innovation: We evaluated vendors' responses to the changing nature of customer demands. We accounted for how vendors reacted to malicious code threats, such as spyware and targeted attacks, and how they invested in R&D or pursued a targeted acquisition strategy.

### 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 believe that leaders are spreading their efforts too thinly and not pursuing clients' special needs.

**Table 1. Ability to Execute Evaluation Criteria**

Evaluation Criteria	Weighting
Product/Service	no rating
Overall Viability (Business Unit, Financial, Strategy, Organization)	high
Sales Execution/Pricing	standard
Market Responsiveness and Track Record	high
Marketing Execution	standard
Customer Experience	standard
Operations	standard
Source: Gartner	

**Table 2. Completeness of Vision Evaluation Criteria**

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

## Challengers

Challengers have solid products that address the typical needs of the market, with stronger sales, visibility and clout, which add up to higher execution than niche players. Challengers are good at competing on basic functions rather than on advanced features. Challengers are efficient and expedient choices to narrowly defined access problems.

## 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 have not yet demonstrated execution. 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 specialized needs of specific buyers. Niche players are less likely to appear on shortlists but fare well when given a chance. 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 the focus is on a few important functions and features that are important to them.

## Vendor Strengths and Cautions

### BigFix

#### Strengths

- ¥ BigFix is one of two operations life cycle management vendors that is exploiting host intelligence and control to provide client security (BigFix AntiThreat). The integration of the security and operational tools provides a more concise view into the security status of the endpoint and enables more-concise reporting and rapid remediation.
- ¥ The AntiThreat offering includes antivirus, personal firewall and anti-spyware engines that are licensed from CA and integrated into the BigFix agent and management console. AntiThreat can also manage other EPP solutions, making it an excellent choice for large enterprises with multiple legacy antivirus solutions.
- ¥ BigFix gets high marks for management scalability and for control of off-LAN devices because of its intelligent agent architecture.
- ¥ AntiThreat includes the base device management platform, which includes payload/software distribution and command and control ability for about 800 variables of an endpoint, including configuration changes, registry changes and device control.
- ¥ Device control is very complete, including capabilities to disable and enforce policies for removable media, USB devices, CD-ROMs/DVDs, floppy drives, parallel ports, infra red ports, Bluetooth and PC Card devices.
- ¥ AntiThreat includes capabilities to conduct NAC assessments and self-quarantines at the endpoint.
- ¥ Client-based DLP was recently licensed from a third party and added to the security product portfolio.
- ¥ A recent IBM reseller agreement will increase brand awareness and channels.
- ¥ Recent pricing changes include the price of the platform, making BigFix cost-competitive with other EPP vendors.
- ¥ Organizations struggling with EPP management issues or those looking to consolidate the management of multiple EPP clients should strongly consider BigFix. Organizations looking for operations life cycle tools should consider BigFix's AntiThreat offering a valuable differentiator.

#### Cautions

- ¥ BigFix is one of the smaller companies in this Magic Quadrant, although it is well-capitalized. The company has a minimal customer presence outside North America. Its customer base is dominated by a relatively small number of very large (more than 5,000 seats) clients.
- ¥ Operations tools, such as software distribution, patch, vulnerability and configuration management, are not included with the AntiThreat solution pack.

- ¥ It lacks a proven track record in the anti-malware protection side of the business. BigFix's anti-malware capabilities are immature and dependent on CA and other partners. It lacks HIPS capabilities in the current release (due the first half of 2008).
- ¥ Visionary extended products, such as DLP and encryption, are lacking.

## Bit9

### Strengths

- ¥ Bit9 takes a different approach from the other vendors in this Magic Quadrant, with a heavy focus on application control.
- ¥ Bit9 Parity blocks software execution on devices that are not on a corporate preapproved list from running and maintains the integrity of installed applications by cross-checking multiple file hashes before they execute.
- ¥ Bit9 has developed a huge source of information on applications and files with Knowledgebase, its file and application identification system, which Bit9 has licensed to vendors such as Kaspersky and Norman to enable their whitelisting capabilities.
- ¥ To reduce the overhead of maintaining whitelists, Bit9 ParityCenter, which is driven by the Knowledgebase data, is a software-as-a-service (SaaS) offering that integrates with Bit9 Parity and provides context on more than 9 million applications and 4 billion individual files to help customers identify and assess the software applications they find in their environments.
- ¥ Bit9 has focused on limiting the management and usability challenges associated with application control. Bit9 Parity is transparent to users and the only graphical user interface (GUI) is the pop-up box that appears when software is blocked. Exceptions are handled by automatically whitelisting software if it comes from trusted sources (directories, virtual LANs and software distribution tools), trusted software vendors or trusted people (users authorized to add applications).
- ¥ The vendor offers Device and Application Reporting Tool, which is an agentless software and device audit tool.
- ¥ Bit9 is appropriate for organizations that have the political clout to enforce an authorized-only software image on PCs or subsets of PCs with a high security requirement. We view it primarily as a good adjunct to an EPP solution because almost all Bit9 customers continue to use some form of signature-based malware scanning.

### Cautions

- ¥ Bit9 is a small vendor with a limited user base that is primarily in North America.

- ¥ It does not have a personal firewall, antivirus or HIPS capability beyond application and device control.
- ¥ If a malware manages to evade detection, then Bit9 cannot clean it up.
- ¥ Bit9 has limited operating system platform support. Current versions only work on Windows.
- ¥ It has limited resources to integrate wider EPP capabilities, such as NAC, DLP or encryption.

## CA

### Strengths

- ¥ CA's biggest strengths are its global support capabilities, mature malware research labs, and broad portfolio of operational and security products.
- ¥ CA EPP solutions include the basic components of anti-malware, HIPS and a personal firewall. CA also offers software-based e-mail and HTTP gateway solutions.
- ¥ The personal firewall has many advanced features, such as support for one active NIC, VPN detection, and good event logging and device control.
- ¥ CA's HIPS capability includes numerous system checks, as well as vulnerability shielding, sandbox execution and behavior anomaly detection. Its learning mode capability eases set up and policy creation. CA also maintains a known application database for broad industrywide whitelisting.
- ¥ Reference customers and resellers often noted the low cost as a major benefit of the CA product.
- ¥ CA customers and those looking for inexpensive EPP capabilities should consider CA's eTrust solutions.

### Cautions

- ¥ Despite the significant resources CA could bring to the EPP suite, it appears that a solid commitment to market in the form of innovation or market leadership is still missing. CA recently announced that it is going to outsource eTrust antivirus product development, engineering, support and threat research to HCL Technologies, while CA will continue to perform sales, marketing and product management tasks. Although this arrangement may be suitable for product maintenance, it is fraught with operational risk and it is difficult to see how it would accelerate innovation.
- ¥ It took several years to integrate the PestPatrol anti-spyware capability. The HIPS solution is not yet integrated in the eTrust Management console. Correlation between different components is shallow.
- ¥ Rootkit detection is weak. There is no capability to discover an installed rootkit in the corporate version.

- ¥ NAC capabilities are limited to participation in Cisco NAC and Microsoft Network Access Protection infrastructure.
- ¥ Although CAs pricing is very reasonable, it is also a somewhat complicated a la carte price structure.
- ¥ CA does not have an aggressive road map for new features or related EPP capabilities, such as NAC, DLP, encryption and even PC life cycle operations integration, which could be a CA strength given that its data center experience is minimal.

## Check Point Software Technologies

### Strengths

- ¥ Check Point Software Technologies is expanding its network firewall reputation to include endpoint security through a combination of acquisitions and partnerships.
- ¥ The cornerstone component of Check Point's EPP (Integrity) is its Zone Labs personal firewall technology and the installed base of millions of consumers of ZoneAlarm, which provides a major source of data for malware research.
- ¥ Check Point's firewall capabilities are much improved since 2006 and are very complete.
- ¥ Integrity licenses Kaspersky's malware engine, and signatures are augmented with Check Point's own threat research spyware signatures.
- ¥ HIPS techniques include vulnerability shielding, Kaspersky's heuristics engine and application control, which includes a database of known good programs with recommended network access rules that are licensed from Bit9.
- ¥ Check Point recently acquired Pointsec Mobile Technologies, a provider of endpoint full-disk and file encryption products.
- ¥ Integrity clientless security creates an encrypted work space where only programs specified by the administrator may run and have access to data used during the session. The administrator can choose to prevent data from being copied or saved outside the secure work space.
- ¥ Check Point is also a significant provider of VPN clients.
- ¥ Integrity includes an 802.1X supplicant and also supports self-enforcement native NAC solutions. An on-demand agent is available for unmanaged machines.
- ¥ Existing Zone personal firewall, Pointsec encryption and Check Point VPN users should include Check Point on their shortlists. Others may want to wait for better integration and a more mature management capability.

### Cautions

- ¥ Although Check Point has an excellent reputation in the enterprise network space, it has not yet established this

reputation with the desktop security buying center. Horizontal product integration is lacking. There is little buying or management synergy between the traditional network firewall and client security.

- ¥ An advanced management capability is lacking. It will take time for the vendor to integrate its various acquisitions into a common code base, client and management framework.
- ¥ Although Check Point has a small research lab, it is primarily dependent on antivirus partners (Kaspersky) for malware research.
- ¥ Rootkit detection is limited to spotting traffic patterns.
- ¥ Device control is in the Pointsec product, which is still being integrated.

## eEye Digital Security

### Strengths

- ¥ eEye Digital Security's Blink EPP product is more of an HIPS solution than a traditional antivirus product. Its primary strength is in multiple styles of proactive HIPS-based protection, including strong host-based, deep-packet inspection supplemented with heuristics-based application pre-scanning, registry protection (rules for controlling access to the registry) and some vulnerability shielding.
- ¥ The included firewall is complete with good advanced features, such as a dynamic location-based policy, as well as a USB and firewire storage device policy.
- ¥ Blink does not depend on signature-based mechanisms as the primary mechanism for malware detection, but it does offer integrated signature-based antivirus, sandboxing and buffer overflow protection, which is licensed from Norman.
- ¥ Blink includes a host vulnerability scanner that is similar to eEye's Retina product, which provides agentless vulnerability and patch assessment capabilities.
- ¥ The company has strong malware research capabilities. It is profitable and growing slightly faster than the market in general (although off a small base).
- ¥ Clients are mostly midsize enterprises. It has 35,000 Blink personal users.
- ¥ Consider eEye Blink if you are an SMB looking for a tactical HIPS solution to supplement signature-based protection and native firewalls on Windows clients and servers.

### Cautions

- ¥ Despite rapid growth, eEye is still one of the smallest companies in this market, with only 74 employees, limited direct sales capabilities and limited presence outside North America or in organizations with more than 500 employees.
- ¥ Management features for large enterprises, such as role-based administration, are lacking or immature.

- ¥ It has limited application and device control capabilities.
- ¥ The vendor doesn't have NAC capabilities.
- ¥ eEye lacks the capability to detect installed rootkits.
- ¥ Platform support is limited to Windows. Windows Vista and 64-bit Windows are not supported.
- ¥ It has expensive list pricing.

## F-Secure

### Strengths

- ¥ F-Secure's malware research lab is well-established and provides fast response times to outbreaks because of automated threat analysis and multiple sources of threat samples.
- ¥ The vendor has the largest share of ISP customers, including a SaaS multitenant platform, F-Secure Protection Service for Business, which enables ISPs to offer SMBs a fully managed security solution.
- ¥ Host-based intrusion prevention capability includes sandboxing, which enables applications to run but stops it if they exhibit suspicious behavior. Suspicious application behavior can be subjected to user query, and the decision is enforced as a rule for further decisions for that application every time it runs.
- ¥ Customers comment on the outstanding support from F-Secure.
- ¥ F-Secure backlight provides a good rootkit scanning capability.
- ¥ The personal firewall component, Internet Shield in F-Secure Client Security, uses Vista's Windows Filtering Platform.
- ¥ F-Secure supports 20 languages.
- ¥ It is a good alternative for SMBs, especially those in their direct service area of northern Europe and those looking for SaaS-type services.

### Cautions

- ¥ F-Secure has limited direct presence in the enterprise market, resulting in less-advanced enterprise management features (distributed management console, role-based administration and automated network scanning for agentless machines), which makes the use of this product in large environments challenging.
- ¥ The HIPS solution is missing some basic capabilities, such as buffer overflow, vulnerability shielding or application whitelisting.
- ¥ F-Secure only offers a Web-based, on-demand scanner. It does not have an enterprise version suitable for scanning unmanaged machines.
- ¥ The personal firewall is basic and lacks features such as device control and expansive logs, and it has limited attack prevention to shield it from being disabled.

- ¥ Advanced data protection, such as DLP and encryption, are not on F-Secure's road map. The vendor exited the encryption market.
- ¥ NAC is limited to agent self-enforcement for signature file freshness.
- ¥ Market presence is mostly in Europe, the Middle East and Africa, with limited presence in North America and Asia/Pacific.
- ¥ F-Secure needs to enhance its quality control and alpha testing on new product version releases.

## IBM

### Strengths

- ¥ IBM acquired EPP vendor ISS in 2006, putting it back into the EPP market after a long absence.
- ¥ IBM Proventia's main strength is in a variety of styles of HIPS protection, including a seven-layer stateful analysis of Internet protocols, proactive executable scanning for malicious intent and buffer overflow protection.
- ¥ The personal firewall is full-featured and mature, including location-based policies, and device and application control capabilities.
- ¥ Proventia offers an optional integrated antivirus signature engine from BitDefender, which includes heuristics technology for nonsignature malware detection.
- ¥ IBM/ISS has the broadest platform coverage of any HIPS vendor. For less-common operating systems, such as AIX, HP-UX and others, IBM/ISS offers a subset of the Proventia capabilities.
- ¥ IBM's X-Force R&D labs have a strong reputation.
- ¥ Potential exists for future integration with the IBM Tivoli operations management agent for shared inventory and configuration management information.
- ¥ IBM's reputation and channel presence in large enterprises enable it to attract capable partners, such as BigFix and Sophos. We fully anticipate that several partners will become acquisition candidates in the near term.
- ¥ IBM's Global Technology Services offers managed security services and provides mature managed security services centralized around the ISS Proventia platform.
- ¥ IBM has announced strategic plans for a significant program to move into the data security market around the three pillars of data protection, system protection and an extensible management framework.
- ¥ Organizations with a close relationship with IBM and those looking for a managed security service should certainly include IBM on their shortlists. Other organizations may want to wait for IBM's aggressive road map and development plans to be

finalized and for development to be nearer to completion to avoid future disruptions.

### Cautions

- ¥ IBM has not had a significant presence in the enterprise endpoint security business for a long time. It sold its IBM AV business unit to Symantec in 1998. Adapting to the constantly changing threat environment will be a cultural shift for IBM, which typically concentrates on less-dynamic markets. Despite announcing a significant budget for a new push into security, IBM's expansion plans for PC and data security are in the early stages and may change significantly.
- ¥ Organizationally, ISS falls into the IBM Global Technology Services Group, which is somewhat an unnatural fit for a software product.
- ¥ High administration, careful tuning and exception handling are essential to the successful deployment of Proventia desktop.
- ¥ Some HIPS techniques may have an impact on endpoint CPU, and memory use is relatively high.
- ¥ There is slow support for Windows Vista for 64-bit Windows.
- ¥ IBM's signature-based anti-malware capabilities are dependent on a smaller vendor, BitDefender, which might pose risks that limit appeal to larger clients.
- ¥ SiteProtector is used to manage endpoint and network-based IBM/ISS security offerings; however, in most organizations, this is two separate groups, which negates most of the value of a converged console.
- ¥ Minimal NAC support exists, and IBM doesn't have any encryption or DLP plans yet.

### Kaspersky Lab Strengths

- ¥ Kaspersky Lab is a smaller, but technically astute, organization with a strong reputation for fast signature response and high-malware detection rates.
- ¥ Its primary client base has been in Europe, but it is rapidly expanding into North America and emerging markets, such as China.
- ¥ The Kaspersky client has a relatively small disk and memory footprint for a comprehensive suite platform.
- ¥ Starting with v.6.0, Kaspersky introduced advanced HIPS features that were previously only available in the consumer product. HIPS features include an isolated virtual environment for behavior detection, and application and Windows registry integrity control.
- ¥ The vendor has a strong OEM business with e-mail and Web

gateway vendors.

- ¥ SMBs that prefer to focus on signature-based defenses and HIPS should evaluate Kaspersky. Larger organizations should consider Kaspersky as a strong antivirus engine when offered in other vendors' e-mail and Web gateways.

### Cautions

- ¥ Despite expansion, Kaspersky is still a small company relative to the market leaders, and its minor global enterprise market share is mostly in SMBs.
- ¥ Kaspersky needs to develop a better understanding of business value issues, the convergence of operations and the EPP market.
- ¥ Its current solution lacks some visionary capabilities, including self-contained NAC, firewall controls for VPN enforcement, prevention of Wi-Fi bridging and device management, DLP, encryption and network gateways.
- ¥ Rapid growth and global expansion will be difficult to manage and could have a negative impact on product quality.

### LANDesk Strengths

- ¥ LANDesk is a leading PC configuration life cycle management vendor (see Magic Quadrant for PC Configuration Life Cycle Management, 2006) that started branching out into the EPP market in 2003. The integration of the security and operational tools provides a more concise view into the security status of the endpoint and enables more-concise reporting and rapid remediation.
- ¥ The security suite includes several operations management capabilities, such as vulnerability, patch, NAC, discovery and inventory, software license monitoring, security configuration management and traditional EPP technologies, such as firewall, virus, spyware and HIPS.
- ¥ Some advanced firewall capabilities, such as device control, location policy and NIC management, can be provided via configuration control. Device control for USB and numerous other ports, including encryption for removable media, is extensive.
- ¥ Malware detection is provided by partners Lavasoft and Kaspersky. The management of other antivirus engines is provided by McAfee, Sophos, Trend Micro and Symantec.
- ¥ LANDesk's HIPS technology, acquired from ViGuard in January 2007, includes application whitelisting/blacklisting, application control/whitelisting and buffer-overflow protection. Whitelist administration is eased by learning mode policy development

and the use of trusted software and trusted users that can self-authorize additions to the whitelist.

- ¥ One of LANDesk's main advantages is the ease of which it can find, assess and update any aspect of a PC, even when it is off a LAN.
- ¥ The vendor has a strong international presence, with 50% of its revenue coming from outside North America, in countries such as France, Germany, the U.K., Japan and China. It has product localization in 18 languages.
- ¥ LANDesk offers NAC (802.1X, DHCP, Cisco NAC and IPsec) to automate security assessments and remediation.
- ¥ LANDesk customers should carefully evaluate their security offerings to augment and eventually replace incumbent EPP solutions, especially organizations with multiple incumbent/legacy EPP vendors. Organizations looking for PC life cycle management tools should consider the security offerings of LANDesk to be a valuable differentiator.

#### Cautions

- ¥ The biggest drawback to LANDesk EPP is that the initial investment in infrastructure needs to be shared with operations administrators and their budgets, which can have some internal political ramifications. Few enterprises will want to deploy multiple operations management infrastructures. However, once the base product is in place, the security offerings are reasonably priced.
- ¥ The extensive management interface can be overwhelming at first; however, after training, it becomes intuitive.
- ¥ LANDesk does not resell a firewall but can manage Windows XP and Vista firewalls.
- ¥ It lacks a proven track record in the protection side of the business. Although it has 50 engineers to research current trends, security issues and vulnerability assessment/remediation content, LANDesk's anti-malware capabilities are primarily dependent on partners Lavasoft and Kaspersky, which may pose risks that limit its appeal to large organizations.
- ¥ Visionary extended products, such as DLP and encryption, are lacking.

#### McAfee Strengths

- ¥ McAfee is a consistent leader in the antivirus market, with a high desktop penetration rate and a solid international threat research capability.
- ¥ It was the first traditional antivirus vendor to incorporate HIPS

capabilities into its base anti-malware product. Its advanced HIPS solution (acquired from Entercept) is comprehensive. Native rootkit detection and removal are also very good.

- ¥ McAfee has demonstrated excellent vision, leading the market with the acquisition of DLP capabilities (Onigma) and full-disk encryption (Safeboot) to protect enterprise data. The vendor also offers a managed service (SaaS) for SMBs.
- ¥ It is slowly acquiring some operations life cycle tools, such as those from Citadel (policy auditing and patch) and Foundstone (vulnerability detection), and integrating them into ePolicy Orchestrator (EPO), the McAfee management console.
- ¥ McAfee's Total Protection for Enterprise offers a single agent and single management console for anti-malware, personal firewall and HIPS.
- ¥ Total Protection for Enterprise includes a unique product site advisor, which overlays search results with URL threat information.
- ¥ McAfee's spyware detection rates are very good for a traditional antivirus vendor.
- ¥ EPO has historically been the standard for centralized administration consoles, and the latest version (v.4) has significant improvements, most notably a new Web interface to replace the Microsoft Management Console.
- ¥ McAfee demonstrated market leadership with recent acquisitions of client-based DLP prevention capabilities (Onigma) and full-disk encryption (Safeboot), which will help customers address data protection and some aspects of compliance. These moves will help elevate McAfee's strategic importance with large enterprises.

#### Cautions

- ¥ McAfee needs to continue to invest in its personal firewall capabilities and integrate its acquired technologies into a more cohesive solution.
- ¥ Although EPO is a strong management solution, it is designed to support all McAfee's products, and users report that it can be difficult to navigate and use. Integration of new products (for example, Foundstone, Citadel and IntruShield) into the console is often very slow. Also, we continue to get reports that EPO status reports are not always accurate. In large distributed organizations, the number of management servers can be excessive.
- ¥ Longtime EPO users report some frustration navigating the new Web version.
- ¥ HIPS policy setting can be administration-intensive.
- ¥ The McAfee agent can have an impact on PC startup and streaming media.

- ¥ NAC capability is limited to self-enforced NAC or McAfee NAC 2.5 integrated with IntruShield Network IPS, and is lacking granular policy capability.
- ¥ Foundstone is primarily used for manual vulnerability detection by security groups, and Citadel has a low penetration rate and is only for specific functions.
- ¥ McAfee's Total Protection for Enterprise products suite has a high list price and includes gateway products (Web and e-mail) that enterprises should source separately. McAfee can be aggressive in negotiating renewals. It must be cautious of pricing itself out of its valuable incumbent status on the desktop.

## Microsoft

### Strengths

- ¥ Microsoft finally entered the enterprise EPP market in 2007 with Forefront Client Security (FCS), which is built around its consumer OneCare anti-malware engine.
- ¥ Microsoft's historical strengths in ease of use and manageability are extended to FCS, especially for enterprises used to Microsoft System Center's look and feel.
- ¥ The FCS management console provides excellent drill-down reporting of the security status of managed clients, including configuration, patch levels and vulnerabilities. Signatures and engine updates are distributed using Microsoft Windows Server Update Services, leveraging infrastructure already in use by many enterprises.
- ¥ Microsoft has a good array of broad high-level signature types, including generic, behavior and event signatures to detect new malware variants. It also has capabilities to decrypt obfuscated malware and rootkit detection by checking operating system inconsistencies.
- ¥ It has solid operating system knowledge and integration, which minimize the risk of operating system conflicts and destabilization.
- ¥ Pricing is attractive, especially for enterprises that purchase Microsoft's Enterprise Client Access License.
- ¥ Microsoft NAC support is embedded.
- ¥ In the long term, Microsoft will better integrate Forefront Client Security with Active Directory and System Center for automated remediation, shared inventory and configuration management information.
- ¥ Consider Microsoft's FCS if you are an SMB looking for basic protection for Windows desktops and servers. Larger organizations under Microsoft's Enterprise Client Access License program should compare FCS with their incumbent EPP provider in terms of scalability and HIPS capabilities and use that as competitive bargaining leverage.

### Cautions

- ¥ FCS only offers Microsoft Windows client and platform support. Partnerships or plans for non-Windows platform support, including Windows Mobile, are still in their infancy.
- ¥ Large enterprises are wary of Microsoft as an operating system platform vendor selling threat protection because of the potential for a conflict of interest.
- ¥ Microsoft is continuously challenged to choose between embedding security into Windows, which benefits all customers, or providing competitive security products. Ownership of security technologies is split between the Microsoft Windows business unit, which owns the firewall and the majority of HIPS techniques, and the Security Products unit, which owns FCS. These groups are managed separately with independent goals and revenue targets.
- ¥ FCS does not manage all Windows built-in security capabilities, such as the firewall, Windows device control capabilities and built-in NAC capabilities. The next major release of FCS (Sterling), which is due in 2009, promises to include better integration of the operating system security elements and the FCS management console, and to offer advanced HIPS techniques.
- ¥ The FCS Security Management Console is not yet integrated into the other Forefront security products (for example, Forefront Security for Exchange Server, ISA Server and Intelligent Application Gateway).
- ¥ Initial Microsoft malware lab weakness in early evaluations of OneCare (same core engine and labs as FCS) is improving rapidly, but a consistent long-term track record is lacking.
- ¥ FCS is optimized for Active Directory Group Policy for configuring agents and Windows Server Update Services for distributing signatures. Companies with other directories and software distribution tools will get less out-of-the-box functionality. Also, acting on alerts may require operators to switch to other consoles, and exception handling is weak.
- ¥ Microsoft is missing visionary features, such as DLP, and encryption is only available in Windows Vista.

## Panda Security

### Strengths

- ¥ Panda Security has a mature malware lab and was early to embrace the EPP concept. It has a good understanding of the business value of EPP.
- ¥ Extensive financial reorganization in the form of new ownership has resulted in new management and a better ability to fund international expansion. Panda recently acquired many of the regional franchises to provide more-consistent global service levels.

- ¥ The biggest differentiator and contributor to vision for Panda is its broad array of HIPS techniques that enable it to catch malware prior to execution without relying on threat signatures. The vendor also has some interesting plans for software identification in the cloud, which could improve malware signature speed and accuracy.
- ¥ Panda Security for Small Business is a hosted management anti-malware solution for Windows endpoints. Management is performed via a Web-based management console hosted in a Panda network operation center. A light client is distributed and installed locally in the endpoints.
- ¥ Panda has good platform support for handheld platforms.
- ¥ Companies looking for a second opinion on the security state of their clients can use Panda's Malware Radar assessment tool, which is included with the EPP suite but can also be purchased separately. Malware radar performs a network-based scan for client infections.
- ¥ Panda also offers Web and anti-spam gateways that are suitable for small businesses and managed with a common console.
- ¥ SMBs that are looking for a more customer intimate alternative to the incumbent giants in the antivirus market should consider the EPP suite from Panda. In particular, we like the malware radar as a technique to audit incumbent performance and test Panda's effectiveness.

### Cautions

- ¥ Overall, Panda is still a small regional vendor and needs to break out of its niche market in Spain. Its international growth plans may stretch corporate resources.
- ¥ It lacks several visionary capabilities regarding its firewall, such as external media controls, VPN enforcement and the prevention of Wi-Fi bridging.
- ¥ Future road maps for DLP and encryption are lacking.
- ¥ The NAC platform is incomplete, although frequent compliance re-checks are a plus.
- ¥ Some customers reported poor Office 2007 compatibility.

### Sophos Strengths

- ¥ Sophos is a privately held EPP vendor that specializes in the enterprise market. It has its roots in Europe, although it has been growing rapidly in North America in recent years.
- ¥ The company has a strong financial position, which new management is leveraging to become more agile and aggressive in adding new features and products. The company recently announced its intention to file for a public offering.

- ¥ Current product management has a better understanding of business needs, particularly the need to provide return on investment for the buyer and to balance advanced features with low administration.
- ¥ The acquisition of Endforce provided excellent integrated NAC capability, including easy-to-deploy Dynamic Host Configuration Protocol (DHCP) enforcement or more complex 802.1X, CNAC and MNAP, as well as DHCP/MAC.
- ¥ The management is significantly improved with its simple to manage and support SmartView filter that shows, for example, only those computers that are out of date or only those that have an outstanding alert. The view can be of the whole fleet or just those in a selected group. This is a real-time view from which actions can be immediately taken (for example, force an update on all those computers). Reporting is also greatly expanded to include PC configuration and software status indicators.
- ¥ The management console is able to monitor, assess and remediate some competitive EPP clients.
- ¥ The Sophos EPP suite offers a good balance of malware, personal firewall and HIPS defenses that are deterministic and easy to deploy and manage. Buyers who prefer a broad and comprehensive EPP suite with impressive management capability, especially NAC — and who are willing to consider smaller, more-intimate providers — will do well to consider Sophos.

### Cautions

- ¥ Lack of consumer products and a small North American presence have resulted in low brand recognition. Brand perception is trailing recent aggressive feature development.
- ¥ The majority of Sophos' client base is small enterprises with fewer than 500 seats. Work is needed to expand its reach into medium to large enterprises, although recent very large (100,000 seats) customer wins have demonstrated scalability and appeal to large enterprises.
- ¥ Sophos lacks several visionary capabilities, including agentless scanning, advanced firewall controls (to prevent Wi-Fi bridging), device control, DLP and encryption, although road map commitments for data encryption with basic media port controls are in place.
- ¥ The EPP management console is not yet integrated with advanced NAC and e-mail and Web gateway products.
- ¥ Ad hoc and scheduled reporting could be improved.

## Symantec

### Strengths

- ¥ Symantec has been a significant competitor in the antivirus market, and it is a large, multinational organization with worldwide presence and malware research lab capabilities.
- ¥ It recently released a thoroughly revised EPP product called Symantec Endpoint Protection (SEP) 11.0. This new version integrates Symantec's antivirus, anti-spyware and personal firewall capabilities with the personal firewall and HIPS capabilities of Sygate and WholeSecurity.
- ¥ Long-suffering Symantec Antivirus (SAV) 9 and 10 users will appreciate less-intrusive scheduled malware scanning with SEP 11.0, a task that formerly had a significant impact on system performance.
- ¥ The new management architecture, based on Sygate technology with a new Web GUI has significant improvements, notably improved directory integration and reporting.
- ¥ Symantec's multiple styles of protection in a modular, plug-in agent architecture can be extended to support future EPP needs, such as DLP, content monitoring and filtering.
- ¥ Its system lockdown capability can provide a snapshot of a system and restrict further execution to a resulting whitelist, effectively hardening the system to unwanted change.
- ¥ Location-based policy awareness subjects clients located in a higher-risk situation (for example, an unsecured Wi-Fi connection) to tighter controls.
- ¥ Symantec On-Demand Agent is a solid (but optional) offering for scanning unmanaged machines with a light downloaded agent.
- ¥ Symantec recently acquired Altiris, which will enable it to provide integrated client life cycle management and better integrated NAC remediation capabilities in 2H08.
- ¥ Symantec recently acquired DLP vendor Vontu, which should enhance its future DLP capabilities.
- ¥ The new SEP 11.0 solution is a free-of-charge upgrade for current Symantec, Sygate and WholeSecurity clients under maintenance, although Symantec will charge a small (11%) increase during the next maintenance renewal.
- ¥ Global organizations should consider Symantec Endpoint Protection if they use Symantec Antivirus, Symantec Client Security, Sygate or WholeSecurity, or if they use a basic antivirus/anti-spyware solution and are looking for a more complete protection platform that supports the selection of multiple styles of protection from an extensible agent framework and managed from a single console.

### Cautions

- ¥ Symantec Endpoint Protection 11.0 is relatively new (general

availability was September 2007) and has spent a long time in development. For SAV 9 and 10 customers, it has been a painful wait at times.

- ¥ SEP 11.0 completely replaces the previous SAV management servers and agents, so migration is not trivial and must be planned more carefully than a typical version upgrade. Symantec offers migration tools and services to ease the migration, and some early adopters have found the migration to be reasonable.
- ¥ The converged SEP 11.0 client functionality and management console does not extend to Macintosh or Linux clients or to its e-mail and Web gateways.
- ¥ Overlap with Symantec Critical System Protection and Symantec Compliance Manager, which uses a separate management and reporting console, needs to be rationalized.
- ¥ The SEP management console is completely new and slightly immature. It still has some legacy tabs, which clients report can be sluggish, and fast drill-down reporting on device history is poor. Administrators must get trained on the new interface before it is rolled out.
- ¥ Buffer overflow technology from Sygate was not integrated. Most EPP competitors offer buffer overflow protection.
- ¥ Client dissatisfaction with Symantec support continues to be an issue, especially with account executive turnover and the contract negotiation process; however, Symantec recently increased the size of its internal support teams in anticipation of SEP 11.0 rollouts.
- ¥ Add-ons to the SEP 11.0 foundation can become expensive. Although SEP 11.0 is NAC-ready, even minimal policy enforcement capabilities require NAC starter edition at roughly \$10 per endpoint, and some clients reported wireless NAC synchronization issues.

## Trend Micro

### Strengths

- ¥ Trend Micro is an established leader in the enterprise antivirus market, with excellent international malware research capabilities.
- ¥ It gets high marks from its clients for service and support.
- ¥ The vendor has recently expanded its reputation system to include an in-the-cloud Web URL reputation database that enables a real-time look up of the security status of a Web site and then blocks clients from going to recently infected Web sites.
- ¥ Trend Micro OfficeScan provides basic HIPS functionality, including code emulation and Trend Micro's proactive Outbreak Prevention Services.

- ¥ NAC capability is good, and Cisco CNAC integration is strong because of its partnership with Cisco and OfficeScan's inclusion of the Cisco Trust Agent.
- ¥ Trend Micro recently acquired Provilla for client DLP.
- ¥ A managed EPP security service in Japan is expected to be expanding to other markets in 2008 and will join a new e-mail and Web security SaaS offering.
- ¥ Trend Micro recently developed a plug-in architecture that enables more rapid integration of new technologies acquired by Trend Micro or offered by smaller innovative companies that do not have the management capability for enterprises. This new architecture also improves the ability for administrators to select which plug-ins to deploy. With its HIPS and personal firewall technology, Third Brigade is the first third party to take advantage of this new plug-in architecture, and Trend Micro expects others.
- ¥ Trend Micro's NeatSuite packaging/pricing is attractive. In some regions, Trend Micro resellers provide free protection software for employees' home PCs.
- ¥ Enterprises looking for a reliable and conservative alternative to other leaders would do well to include Trend Micro on their shortlists.

#### Cautions

- ¥ Trend Micro's execution score is affected by the company's slow response to changing market conditions and its strategy of organic growth over significant acquisitions. However, recent moves, such as its acquisition of Provilla and licensing of Third Brigade, are encouraging.
- ¥ OfficeScan's lack of advanced HIPS and personal firewall features had a significant impact on its vision score. Although the strategy of application programming interface integration of third-party software is a good direction, independent HIPS and personal firewall vendors are rapidly disappearing, and the competition more tightly controls these base technologies.
- ¥ Trend Micro's global market share distribution is somewhat skewed to the Asia/Pacific region, and the North American enterprise business is skewed to the gateway market.
- ¥ The company has no operations life cycle tool components, such as vulnerability scanning patch or security configuration management, nor does it have any integration with partners for this type of capability.
- ¥ OfficeScan Client is relatively heavy, and scheduled scans can affect PC performance.

- ¥ The product portfolio has only limited agentless scanning capabilities.
- ¥ Native NAC capability is appliance-based, making it expensive and complex for large organizations.
- ¥ Control Manager does not yet have the richness of reporting like some competitive solutions, and central management can be difficult.

### Webroot Software

#### Strengths

- ¥ Webroot Software's primary strength is its spyware and adware threat detection and filtering capabilities. The Phileas URL search engine is distinguished in the industry as an excellent site-oriented spyware detection system.
- ¥ Its malware engine uses 17 real-time shields that identify and block malware from loading.
- ¥ The vendor has leveraged its spyware niche into a profitable business with no debt, but larger incumbents are catching up in spyware detection rates. Webroot is challenged to leverage its spyware expertise to create an EPP solution. It has licensed Sophos for antivirus signatures, including Sophos' Behavioral Genotype Protection.
- ¥ Webroot will continue to fill the niche need of buyers who primarily seek to augment spyware defense until it can provide HIPS and personal firewall functionality.

#### Cautions

- ¥ Webroot is a relatively small company in this market, and it has experienced some management turnover. It will be difficult for it to compete in the broader EPP market with such small engineering and support capabilities.
- ¥ The relative breadth of Webroot's EPP features is limited compared with the market average. For example, its platform lacks a firewall and HIPS features.

### Acronym Key and Glossary Terms

<b>DHCP</b>	Dynamic Host Configuration Protocol
<b>DLP</b>	data loss prevention
<b>EPO</b>	ePolicy Orchestrator
<b>EPP</b>	endpoint protection platform
<b>FCS</b>	Forefront Client Security
<b>GUI</b>	graphical user interface
<b>HIPS</b>	host-based intrusion prevention
<b>NAC</b>	network access control
<b>NIC</b>	network interface card
<b>SAV</b>	Symantec Antivirus
<b>SEP</b>	Symantec Endpoint Protection
<b>SMB</b>	small or midsize business
<b>SaaS</b>	software-as-a-service
<b>USB</b>	Universal Serial Bus
<b>VPN</b>	virtual private network

- ¥ The Webroot enterprise client base is primarily U.S.-based SMBs (fewer than 500 seats).
- ¥ Despite a relatively lightweight client, scheduled scans can have a noticeable performance impact on PCs.
- ¥ Webroot lacks several visionary capabilities, including on-demand protection, NAC, device controls and DLP capabilities.

### 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.