Magic Quadrant for **Endpoint Protection Platforms**

Malware effectiveness continues to accelerate, while vendors are busy polishing increasingly ineffective solutions and doing little to fundamentally reduce the attack surface and protect users.

WHAT YOU NEED TO KNOW

- This year's analysis did not show considerable movement of vendors from last year's analysis.

- Malware detection accuracy has not improved significantly, while malware is improving in efficiency and volume.

- The inclusion of basic vulnerability and configuration management in endpoint protection platform (EPP) suites is still low as vendors continue to focus on signature-based defenses rather than addressing root causes.

- Application control (also referred to as "default deny" or "whitelisting") holds significant promise, but with a few exceptions, most of the vendors in this analysis do not provide flexible enough solutions for larger enterprises.

MAGIC QUADRANT

Market Overview

The threat environment continues to outpace improvements in malware detection effectiveness. High-profile attacks, such as Aurora and Stuxnet in 2010, illustrate the growing sophistication of malware attacks. While the volume and effectiveness of malware are growing rapidly, there have been few effective improvements in EPP vendors' defensive technologies. Gartner clients are increasingly frustrated with having to clean PCs from well-known consumer infections like "Fake AV" and are concerned about the potential impact of more stealthy, undetected, targeted attacks.

Signature-based malware detection has been limping along on life support for years, yet vendors seem unwilling to aggressively invest in more-effective solutions, preferring to "tweak" the existing paradigm. Dedicated host-based intrusion prevention system (HIPS) has failed to live up to its promise as a proactive protection method due to the management overhead required for marginal improvements in detection accuracy. The disillusionment with HIPS was illustrated by Cisco's retirement of its CSA product in 2010. Some effective HIPS techniques are making their way into the core anti-malware engines, and these solutions provide significant additional value in detecting new threats. However, they are not sufficient to keep pace with the changing threat landscape.

Gartner

We are starting to sound like a broken record. As far back as 2004, we have been saying that enterprise anti-malware vendors are falling behind in dealing with the current security threats. This year, they have fallen even further behind. Test after test has illustrated that current solutions are less than 50% effective at detecting new variations of existing threats and much worse at detecting targeted or low-volume threats, although testing methodologies have also not kept pace with changing EPP suite capabilities.

We believe that attention to better software management and maintenance is the key to reducing the attack surface and protecting users from social engineering attacks. "Default deny" methods of controlling what software is loaded onto machines (aka application control), configuration management, and vulnerability detection and remediation are the most effective proactive forms of malware defense. These methods reduce the overall attack surface and neuter the vast majority of threats.

However, we continue to see very slow progress toward integrating these solutions into current EPP suites. LANDesk, BigFix-IBM, Lumension Security, CA Technologies, Check Point Software Technologies and McAfee have begun to address application control needs, but fall short of point solutions that address this market. Symantec has invested in a unique file reputation system for its consumer products, but it is still unavailable in its enterprise engine. McAfee, Symantec, Lumension, BigFix, LANDesk and eEye Digital Security are similarly addressing vulnerability and/or configuration compliance checking. However, these tools need to be better integrated into the base EPP suite, and make it easier to acquire, understand and manage this information from the EPP management consoles. Because most malware is Web-borne, it is not surprising that a few vendors are starting to beef up protection from malicious websites. Check Point, Trend Micro, GFI Software, Kaspersky Lab, McAfee, Sophos and Symantec have integrated some level of Web protection, but there is significant room for improvement in protecting devices from the Web infection vector.

Port/device control is another topic that is rising to the top of RFP requirements. More and more organizations want to be able to control which USB peripheral devices are used and how.

Figure 1. Magic Quadrant for Endpoint Protection Platforms

Source: Gartner (December 2010)

As of December 2010
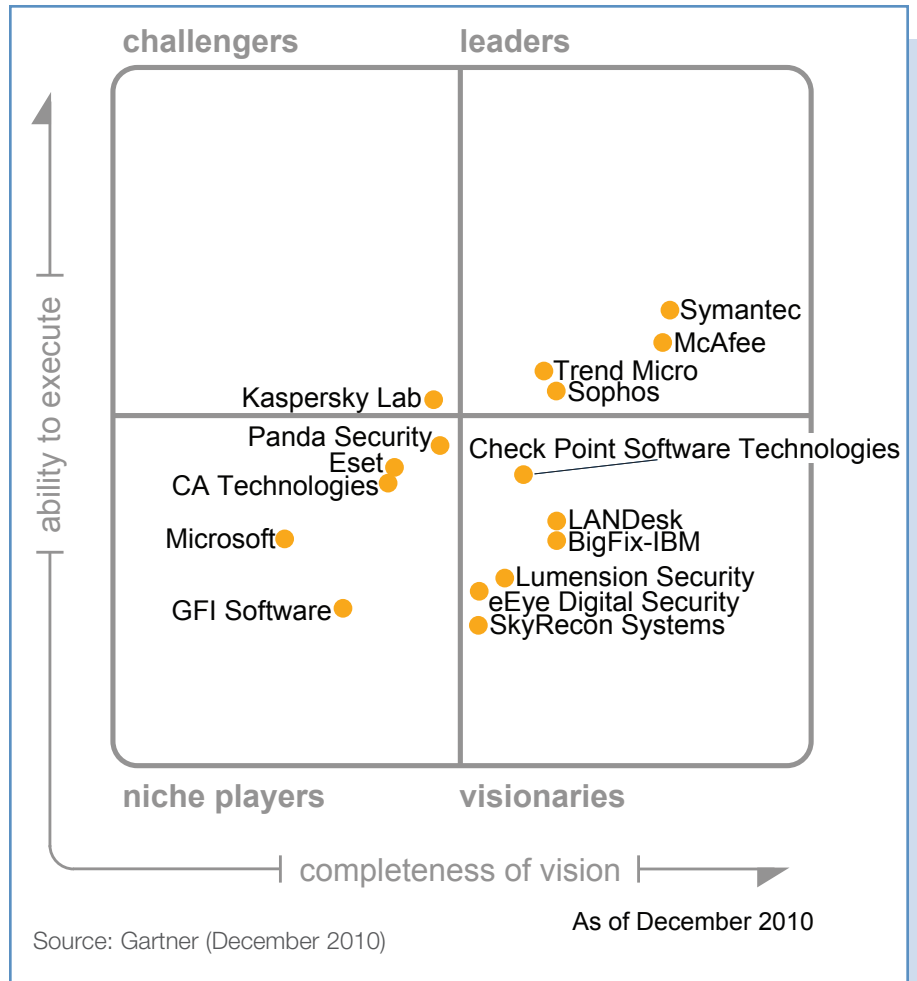
Lumension, SkyRecon Systems, Check Point, CA, LANDesk, McAfee, Sophos and Symantec all offer port/device solutions, but there is significant variation in the level of sophistication of these tools.

Data protection tools, such as full disk and file/folder encryption and data loss prevention (DLP), are becoming standard components of endpoint security toolkits, as companies attempt to address insider theft, government compliance and data protection. While it is not entirely necessary that the data protection capability be included with malware defense in an EPP suite, it can be significantly less expensive and easier to manage if it is. McAfee, Symantec, Trend Micro, Sophos and CA are providers that offer data protection tools, although the level of integration of these tools

is still a critical differentiator. Data protection that is well integrated with the EPP capabilities can offer correlated policy options that address complex business use cases and are more flexible.

Prompted by the rapid growth of employee-owned devices, such as laptops and iPads, and significantly more capable smartphones, such as iPhones, Windows Phone 7 and Androids, organizations are becoming increasingly concerned about the potential for data loss and malware introduction from these devices. So far, the threat environment remains very low on these platforms, so anti-malware is not yet an essential on these platforms. However, the abilities to manage these devices, enforce native security functions (for example, passwords, encryption and remote wipe), and simplify ActiveSync integration are moving up the requirements list. McAfee, LANDesk and Check Point are vendors that are beginning to directly address this issue. Mobile device management and security is another domain that sits at the intersection between PC life cycle management (PCLM) tools and EPP suites and is another benefit of these solutions becoming more tightly integrated.

Other improvements we detected in this year's analysis were focused around improvements in management consoles and reporting and improvements in the breadth of platform coverage (for example, 64-bit Windows 7, SharePoint and Macintosh). Only a few vendors (McAfee and Trend Micro) have addressed the specific needs of virtualization; however, we see this capability increasing in importance to buyers.

Market Definition/Description

The enterprise endpoint protection platform market is a composite market primarily made up of suites of products — which include anti-malware; anti-spyware; personal firewall; host-based intrusion prevention; port and device control; encryption of full disks, files and folders; and endpoint DLP.

Despite the introduction of new players, the displacement of incumbents is still a significant challenge in the large-enterprise market. The biggest impact of the Challengers and Visionaries is to push the dominant market players into investing in new features and functionality, and to keep pricing rational. This market continues to be very competitive in the sub-thousand-seat level. Current prices for comparable offerings are down from our last analysis; however, vendors are often substituting more-complete suite offerings with little or no increase in annual costs.

In 2009 (the last year for which we have full-year numbers), the enterprise market was still dominated by McAfee (24%), Symantec (27%) and Trend Micro (17%), which represent approximately 68% of the total enterprise market. However, the share of these dominant players is down considerably from 85% in 2007. These market leaders are losing market share to increased competition in the lower end of the market with less than 1,000 seats. Sophos (9%) and Kaspersky (4%) are the primary beneficiaries of this trend and are improving mind share and market share in the enterprise market.

The market size at the end of 2009 was around 2.7 billion, flat from 2008, due to increasingly competitive pricing, slow growth of enterprise PC inventory and cannibalization of point product revenue by suites. We anticipate growth rates of approximately 5% in 2010 and 2011.

Despite our previous optimistic predictions, Microsoft's impact on the enterprise market has been minimal as it has repeatedly delayed its next-generation offering until the end of 2010, and our expectations for future growth are tempered by Microsoft's glacially slow development pace.

Inclusion and Exclusion Criteria

Inclusion in this Magic Quadrant was limited to vendors that met the following minimum criteria:

- Detection and cleaning of malware (that is, malware, spyware, rootkits, trojans and worms), a personal firewall, and HIPS for servers and PCs.

- Centralized management, configuration and reporting capabilities for all products listed above, which are sufficient to support companies of at least 5,000 geographically dispersed endpoints.

- Global service and support organizations to support products.

Added

- We added GFI Software and Lumension Security to this year's analysis.

Dropped

- Prevx was recently acquired by Webroot. Webroot does not have a significant enterprise presence in the EPP market.

- F-Secure appeared in our last analysis but did not respond to our request for information for this year's analysis.

Evaluation Criteria

Ability to Execute

The key Ability to Execute criteria used to evaluate vendors in 2010 were overall viability and market responsiveness and track record. The following criteria were evaluated for their contribution to the vertical dimension of the Magic Quadrant:

- **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 strategic it is to the overall company.

- **Market Responsiveness and Track Record:** We evaluated each vendor's track record in bringing new, high-quality products and features to customers in a timely manner.

- **Sales Execution/Pricing:** We evaluated the vendor's market share and growth rate. We also looked at the strength of channel programs, geographic presence, and the track records of success with technology or business partnerships.

- **Marketing Execution:** We evaluated the frequency of vendors' appearances on shortlists and RFPs, according to Gartner client inquiries, as well as reference and channel checks. We also looked at brand presence and market visibility.

- **Customer Experience:** We primarily used reference customers' satisfaction scoring of the vendor in an online survey and data received from Gartner clients during our inquiry process to score vendors on customer satisfaction with the company and the product.

- **Operations:** We evaluated companies' resources that were dedicated to malware research and product R&D.

Completeness of Vision

The most important vision criteria in this analysis were market understanding and the sum of the weighted offering/product strategy score:

- **Market Understanding:** This describes vendors that understand customer requirements for proactive and integrated defenses across all malware threat types, consider the need for better management and data security, and have an innovative and timely road map to provide this functionality.

- **Offering (Product) Strategy:** When evaluating vendors' product offerings, we looked at the following product differentiators:

  - **Anti-malware detection and prevention capabilities:** This is the speed, accuracy, transparency and completeness of signature-based defenses, as well as the quality, quantity, accuracy and ease of administration of non-signature-based defenses and removal capabilities for installed malware. We looked at test results from various independent testing organizations and used Gartner inquiries as guides to the effectiveness of these techniques on modern malware.

  - **Personal firewall capabilities:** This is advanced personal firewall capabilities that exceed the built-in capabilities of Microsoft Windows. We looked at features such as dynamic policy enforcement (for example, location-based policy, specific virtual private network [VPN] policy and wireless policy capability), the breadth of firewall log capture information, anti-firewall-tampering capabilities and application-specific firewall policy.

  - **Management and reporting capabilities:** This is comprehensive centralized reporting that enhances the real-time visibility of end-node security state and administration capabilities, which eases the management burden of

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 (December 2010)	

Table 2. Completeness of Vision Evaluation Criteria

Evaluation Criteria	Weighting
Market Understanding	High
Marketing Strategy	No rating
Sales Strategy	No rating
Offering (Product) Strategy	High
Business Model	No rating
Vertical/Industry Strategy	No rating
Innovation	Standard
Geographic Strategy	Low
Source: Gartner (December 2010)	

policy and configuration development. Vendors that have embarked on PCLM-style operation integration showed considerable leadership and were given extra credit for showing up positive on this criterion.

- **Data and information protection:** This is the quantity and quality of integrated technology to protect data that resides on endpoints, such as full-disk encryption, data leak prevention, and port and device controls. Although we argued above that these technologies aren't mandatory requirements of every buyer, they do demonstrate vendor vision and leadership in this market.

- **Device and port control capabilities:** We explored the granularity and integration of policy-based controls for a broad range of ports and peripheral devices, such as USB and printer ports. We looked for granular control of a range of device types, interaction with encryption and DLP policy, and convenience elements, such as end-user self-authorization options.

- **Application control capability:** We looked for the ability to apply a flexible default deny-application policy that allows for trusted sources of change and can handle requirements ranging from full lockdown to allowing any trusted application to run. We focused on ease of administration and exception management.

- **Supported platforms:** Several vendors focused solely on Windows endpoints, but the leading vendors are able to support the broad range of endpoint and server platforms typically found in a large-enterprise environment. In particular, we looked for support for specialized servers, such as e-mail, collaboration portals (such as SharePoint, storage area networks and network-attached storage), the ability to optimize security for virtualized environments, and support for Mac and mobile devices.

The other criteria evaluated were:

- **Sales Strategy:** We evaluated each vendor's licensing and pricing programs and practices.

- **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, how they invested in R&D, or how they pursued a targeted acquisition strategy.

- **Geographic Strategy:** We evaluated each vendor's ability to support global customers, as well as the number of languages supported.

Leaders

Leaders demonstrate balanced progress and effort in all execution and vision categories. Their capabilities in advanced malware protection, data protection and/or management features raise the competitive bar for all products in the market, and they can change the course of the industry. A leading vendor isn't a default choice for every buyer, and clients should not assume that they must buy only from vendors in the Leaders quadrant. Some clients believe that Leaders are spreading their efforts too thinly and aren't pursuing clients' special needs.

Challengers

Challengers have solid anti-malware products that address the basic security needs of the mass market, and they have stronger sales, visibility and/or security lab clout, which add up to a higher execution than Niche Players offer. Challengers are good at competing on basic functions rather than on advanced features. Challengers are efficient and expedient choices for narrowly defined problems.

Visionaries

Visionaries invest in the leading-edge (aka "bleeding-edge") features — such as advanced malware protection, data protection and/or management capabilities — 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 haven't yet demonstrated execution. Clients pick Visionaries for best-of-breed features, and in the case of small vendors, clients may enjoy more personal attention.

Niche Players

Niche Players offer viable, uncomplicated anti-malware solutions that meet the basic needs of buyers. Niche Players are less likely to appear on shortlists, but fare well when given a chance. Niche Players may address the advanced security needs of highly attacked organizations or low-overhead, basic anti-malware for the broader market. Clients tend to pick Niche Players when the focus is on a few specific functions and features that are important to them.

Vendor Strengths and Cautions

CA Technologies

CA's EPP products have undergone a complete redesign since our last analysis. Release 12 of its Web-based management console for both anti-malware and HIPS capabilities improved role-based access control, unmanaged endpoint discovery and client installation, reporting, and auditing. It also converged its two clients into a single anti-malware and HIPS client. However, in 2010, CA has moved down in its ability to execute due to slow market responsiveness, stagnant market share and low visibility among non-CA customers. CA customers and global organizations seeking uncomplicated EPP capabilities should consider CA Threat Manager r12.

Strengths

- The new r12 console based on an Adobe Flex user interface offers significantly improved management and reporting, as compared with prior versions, and includes the capability to stream alerts about critical external events directly to the console from CA.

- With the converged anti-malware engine, CA Threat Manager Total Defense solution is on par in terms of the basic functional specifications for an EPP solution.

- The CA firewall can enforce policies by network context, and it provides excellent capabilities to set policies to defend or deny the operation of a new network interface, including restricting which ports and services are active.

- CA's HIPS capability includes numerous system checks, as well as vulnerability shielding, sandbox execution and behavioral anomaly detection. Its learning mode capability eases setup and policy creation.

- CA offers unified network control (UNC) in its r12 suite, which provides Microsoft Network Access Protection (NAP) capabilities, including inventory, patch, vulnerability and configuration assessment.

- CA has made significant investments in enterprise data protection and has strong endpoint data protection options. It is among a small number of ranked vendors with the ability to block certain data leakage operations on a per-application basis, such as using the clipboard.

- r12 provides port and device controls, including control over USB, Bluetooth, CD, infrared device, DVD and floppy disk drives.

- CA offers very broad platform support, including several varieties of Unix/Linux, Mac, Palm, Windows Mobile, VMware, Microsoft Hyper-V and Citrix presentation servers, as well as specialized servers, such as Microsoft Exchange, Lotus Notes/Domino, Novell NetWare, NetApp and EMC storage servers.

- CA offers solid application control capabilities, with one of the largest databases of applications grouped into categories (for example, games).

Cautions

- CA's long-awaited r12 console is much improved, but brings it only to parity with what other EPP leaders already offer and is not yet well field-tested. Some features are still lagging, such as extensive control over scheduled scans, flexible administrator role creation and custom dashboard widgets.

- CA's lack of participation in independent anti-malware testing makes it difficult to validate malware detection effectiveness. CA releases only two signature updates per day.

- CA's firewall technology is powerful, but policies can be complex to configure.

- CA lacks integrated full-disk/file encryption products, and CA lacks the ability to enforce encryption on data written to external storage devices.

- CA's DLP (acquired from Orchestria in 2008) is still a separate product managed from a separate division and has not yet been fully integrated.

- There is no integration between CA EPP and its PCLM offerings.

- Reference customers were lukewarm in their endorsement of CA.

Check Point Software Technologies

Well-known in the enterprise network firewall and VPN market, Check Point continues to improve its EPP product suite with an emphasis on addressing the increasing proliferation of unmanaged devices. Despite its laudable enterprise network presence, brand and channel, the company has failed to significantly improve its market share or mind share in this market. Organizations that value strong integration between remote-access solutions and the EPP suite, full-disk and media encryption, and application control solutions should include Check Point on their shortlists.

Strengths

- Check Point Endpoint Security suite includes personal firewall, anti-malware/anti-spyware (licensed from Kaspersky Lab), full-disk encryption, network access control (NAC) and integrated VPN in a single client deployment.

- Check Point's management console was recently improved and integrates malware protection and data encryption suite offerings. It offers a clean interface with easy navigation and quick access to summary data (overview/dashboard, organization, policies, reports and deployment) that is very similar to a network firewall interface. Reporting is significantly improved. The dashboard can be customized for each administrator. It provides good hierarchical and object-oriented policy and can exploit network firewall policy objects, such as network zones, in client firewall policy and can leverage installed gateway appliances as relays for client updates. Check Point offers a unique user-based management capability that allows administrators to develop and view user-specific policies across multiple devices.

- The personal firewall is comprehensive and includes extensive prepopulated program profiles, excellent location-based policies and very good VPN client integration.

- Check Point has some basic HIPS techniques in its firewall and as part of the Kaspersky engine.

- Check Point's Program Advisor service allows administrators to enable application control of acceptable applications based on an existing inventory of applications, certificates and/or Check Point's database of known good applications.

- Check Point has very strong full-disk and file/media encryption, as well as extensive port control, including very granular device and file identification.

- NAC is extensive for remote access via Check Point's VPN and Secure Sockets Layer (SSL) VPN products, and it includes an on-demand scanner for unmanaged machines. LAN NAC is limited to personal or network firewall enforcement, or participation in an infrastructure NAC solution (that is, 802.1X).

- Check Point added browser protection technology from ZoneAlarm, which helps clients avoid malicious Web-based malware.

Cautions

- Check Point is challenged in sufficiently differentiating itself from its core malware detection engine partner, Kaspersky, for clients seeking basic protection, or from market leaders for clients seeking data protection solutions.

- Although the management console provides a good summary view of the EPP agent status, it does not include any vulnerability or configuration assessments, nor does it have any integration with operations tools.

- Check Point is dependent on Kaspersky for anti-malware signatures to review suspicious code samples and to prepare custom signatures for targeted malware. Although signatures are becoming a replaceable commodity, business disruptions in Kaspersky could impact Check Point customers.

- The Check Point management console is a Windows client/server application rather than browser-based. Check Point is dependent on software distribution tools to install the initial client, and lacks the ability to remove other anti-malware products. The solution doesn't include many options to minimize the impact of scheduled scans, such as the impact on CPU use, or to avoid conflicts with critical programs.

- Check Point's program control solution can't prevent programs from installing. It only blocks network access via firewall permissions and terminates the process. Program control doesn't clearly pinpoint machines with particular rogue applications, thereby making remediation more difficult than necessary. Program control is not flexible enough for larger enterprises. It doesn't have a good centralized way of allowing trusted sources of change.

- The SmartDefense HIPS policy isn't tunable and doesn't allow administrators to whitelist applications that incur false positives.

- The NAC solution doesn't support guest NAC enforcement.

- Port control device management is included in the media encryption solution rather than in the firewall.

- Check Point's data protection strategy is still missing client-based content-aware DLP.

- Check Point protection is limited to Windows endpoint PCs. It doesn't offer protection for Macs or specialized servers, such as Microsoft Exchange, Lotus Notes or Microsoft SharePoint.

eEye Digital Security

eEye's historical strength has been in vulnerability analysis. As the EPP market has evolved to broader platform capabilities, eEye has remained focused on its traditional strength of malware and intrusion prevention capabilities, backed by its own malware research labs and augmented by a licensed signature database. Since our last review, eEye has redesigned and unified the management consoles of its various offerings, including vulnerability analysis, providing a much more holistic security state assessment. This improvement moved eEye over the line into the Visionaries quadrant. Existing eEye Retina customers should shortlist Blink. Other buyers, such as enterprises seeking a tactical HIPS solution to supplement signature-based protection and native firewalls on Windows clients and servers, and enterprises that value integrated vulnerability analysis, should consider eEye Blink.

Strengths

- The Retina CS management console has been redesigned with a modern, Flash-based user interface and has been unified across the various eEye offerings.

- Blink uses an embedded version of eEye's Retina Network Security Scanner to perform local vulnerability assessments and report the findings to the Retina CS console. eEye has launched the Retina Protection Agent (RPA), which is a subset of Blink (minus antivirus and firewall), designed to work alongside other EPP and antivirus solutions, and to provide agent-based vulnerability assessment and intrusion prevention services.

- All functions are packaged in a single agent, including the Norman signature engine. Layers of function are easily enabled or disabled by the administrator without making changes to the installed image or drivers. Security policies can be monitored and updated from outside the firewall without requiring a VPN. Change management details are held in XML files for revision monitoring and control. The actual installed footprint stored and in RAM is relatively small.

- Since our last analysis, eEye has added a new generic heap-spraying detection and vulnerable ActiveX protection for Internet Explorer. It has also added an on-access scanning throttle to allow deeper scanning for user-accessed files and improved buffer overflow protection.

- eEye is the only company in this analysis to offer a service-level agreement (within 48 hours) on new critical exploits, meaning that it will protect against these exploits within 48 hours even if the system is unpatched.

- eEye uniquely offers physical management appliances for rapid deployment and management, and offers a software as a service (SaaS) product for vulnerability assessment.

- Anti-malware performance is enhanced by not rescanning files that were previously marked "good" if the file hash hasn't changed.

- eEye has a small but very skilled team of malware experts that provides excellent technical support and malware information.

Cautions

- eEye is one of the smallest companies in this market, and it has a limited presence outside North America and in organizations with more than 500 employees. Its total staff size, including research and engineering groups, is small compared with the EPP industry average.

- The management console is improving but still may be limiting for larger enterprises. Policy is based on physical hosts, not directory groups. Although directory information can be imported, it is a one-time association. Some client configuration options must be done on an endpoint, using the registry, and exported to the management console and applied to other groups. The addition of vulnerability information in the management console is a significant benefit of eEye; however, the solution lacks actionable guidance. There is a reporting linkage between vulnerabilities and HIPS-based vulnerability shields, but it is not in the dashboard. It does not offer an ad hoc reporting capability or custom dashboards. The solution has the capability to blacklist applications, but it is a manual process with no trusted sources of change. It offers limited NAC integration.

- Although eEye develops its own spyware signature database and cleanup routines, the solution relies on Norman for anti-malware signatures. Although signature feeds from reputable labs are becoming a replaceable commodity, business disruptions in Norman could impact eEye customers. Although the Norman anti-malware engine is tested regularly, eEye does not participate in many industry tests to demonstrate the effectiveness of its collection of technologies. It offers only one signature update per day, while other vendors have gone to real-time cloud-based signature updates. Automated malware damage cleanup capabilities are limited.

- eEye has limited application and device control capabilities, but no encryption or DLP capabilities. It lacks the ability to enforce encryption on data that's written to external storage devices, but it does have a number of policies to limit access and writing to external devices.

- It supports only Windows OS platforms (including 64-bit Windows, which has been added), so companies with other devices and servers will need to buy other or additional EPPs.

- Although the storage and RAM footprints look relatively low, eEye's real-time evaluations and quarantine IPS techniques consume a significant amount of resources and can be an issue on older systems.

- There's no enhanced protection for wireless interfaces or direct support for wireless LAN (WLAN) security supplicants.

Eset

Eset has built a substantial installed base in EMEA, particularly in Eastern Europe, and it has a rapidly growing small or midsize business (SMB) presence in North America. Its Completeness of Vision score benefits from good malware effectiveness in a lightweight client, but it still suffers from weak enterprise management capabilities and lack of investments in market-leading features, such as data protection or more-holistic security state assessments. Eset is a good shortlist option for organizations seeking effective, lightweight anti-malware scan engines and personal firewalls that do not have extensive management requirements.

Strengths

- The flagship enterprise product, Eset Smart Security, includes integrated anti-malware, anti-spam and personal firewall in a single-agent footprint. The low performance impact of the Eset product has been noted by many customers. Recently, Eset introduced a new core engine with improved performance and client self-defense, as well as new HTTPS and POP3S scanning, firewall profiles, and support for Cisco NAC.

- The management console is a native Windows application with a spreadsheet-style interface. It has the look and feel of a Microsoft Management Console. We like its capability to highlight machines in the log table and then, with a left-click, to install the EPP agent or perform other remediation activities.

- The Eset anti-malware engine is a consistently respectable performer in test results (that is, VB100 and AV-Comparatives tests) and performs very well in tests of heuristic detection techniques. The Eset engine has a strong reliance on heuristics and generic signatures, including sandbox heuristics, which run all executable files in a virtual emulator and provide client-based malicious URL filtering.

- Eset supports a broad range of Windows clients and servers, including Exchange, Lotus Notes/Domino, Linux Solaris, and Novell NetWare and Dell storage servers. The company recently added endpoint products for mobile devices (Windows Mobile and Symbian), as well as an anti-malware solution for Mac OS X and Linux desktop platforms.

- To further reduce the performance impact of scanning, Eset recently introduced more control over scanning of archives and a feature that automatically determines which files need deeper scanning.

Cautions

- Eset is lacking in management features for larger, more-complex organizations. The management console is long overdue for an update; it's very complex and lacks a clear, actionable dashboard view to enable more-rapid or automated problem identification and remediation. It also lacks many common enterprise capabilities, such as role-based administration, information and policy elements that can be

delegated (or restricted) to end users, automatic location-based policies — especially enforcing and monitoring policies for off-LAN clients — and automatic rogue machine detection.

- It has very poor reporting. A lot of information is captured, but it is hard to get at, and there is no ad hoc reporting, just filtered log views. Real-time updates are impossible.

- The management server never pushes updates to clients — clients have to pull jobs at configurable intervals.

- There is no significant security state assessment beyond EPP agents (that is, application vulnerability and configuration assessments) and no significant integration with operations tools.

- Clients can be distributed by the management console; however, deinstallation of competitive solutions is an additional service cost that isn't included in the solution.

- The HIPS capability can only be activated or deactivated; it can't be selectively deactivated to allow specific false-positive files to execute.

- Eset doesn't yet offer many of the additional EPP components, such as application control, advanced port/device control, encryption, and DLP or VPN integration.

- Eset offers only rudimentary device control, which enables blocking and/or immediate scanning of removable media.

GFI Software

GFI Software is a new entrant in this year's analysis. U.S.-based Sunbelt Software was recently acquired by GFI Software, which offers a wide range of security solutions (notably, secure e-mail Web gateways, archiving and backup) primarily aimed at SMB organizations. GFI is a reasonable shortlist candidate for small to midsize organizations looking for a simple and lightweight anti-malware engine.

Strengths

- GFI's Vipre management interface is very efficient and clean. It provides a large range of preinstalled movable dashboard widgets and provides good ability to view and drill into log data and assign policy to groups and users.

- Malware detection is augmented with MX-Virtualization, which analyzes malware in real time in a virtual environment on the PC, and offers client-based malicious URL blocking, rootkit scanning and automatic scanning of USB drives.

- The client is relatively lightweight and efficient, providing fast scanning.

- GFI offers Windows and Mac client support, as well as Exchange server versions.

- Vipre's net per-year list pricing is one of the lowest in this analysis.

Cautions

- GFI is a relative newcomer to the enterprise market. We do not have a lot of reference customers in the Gartner installed base, and GFI is not evaluated in most of the malware effectiveness testing, so performance in the wild is not well-documented. Reference clients were unenthusiastic and commented that signature data would benefit from improved quality control.

- The Vipre management capability will be limiting for larger enterprises. It relies on Windows network browser or Active Directory information to find unmanaged machines. It does not have any ad hoc reporting capability, only filtered views of historical data. Role-based administration is limited to read or write options only. HIPS policy control is limited to creating exceptions for specific programs by name.

- The firewall does not offer extensive policy options, such as Wi-Fi or location-based policy.

- The solution does not offer any advanced capabilities, such as port/device control, application control capability, encryption or DLP. There is no significant security state assessment beyond EPP agent status (that is, application vulnerability and configuration assessments) and no significant integration with operations tools.

- The solution does not offer Linux, Unix or Lotus Domino support.

BigFix-IBM

When we last evaluated IBM's offering, it had two separate offerings — Proventia Desktop with BitDefender anti-malware and Proventia Endpoint Secure Control offering, which was a combined offering with BigFix, Proventia for HIPS and firewall, and Trend Micro for anti-malware. In 2010, IBM implemented several changes to better align its overall security and endpoint product businesses. Ownership of IBM Internet Security Systems (ISS) Proventia technology moved from the IBM Global Services division to the IBM Tivoli software division, and IBM will now go to market with a cross-IBM security brand — IBM Security Solutions.

The Tivoli division acquired BigFix to bolster its PCLM capability and serve as a platform for its EPP offering. The relationship with BitDefender has been phased out. A new, more rationalized, combined offering will be based on BigFix, with Trend Micro for antivirus signatures, and Proventia for HIPS and firewall. While potentially positive in the long run, these extensive changes reflect negatively on IBM's Ability to Execute score in this analysis. Large organizations that have a close relationship with BigFix-IBM or Trend Micro should include IBM on their shortlists, once this offering becomes available and the organization settles.

Strengths

- IBM's acquisition of BigFix into its Tivoli organization will provide a strong anti-malware (from Trend Micro and supported by the IBM X-Force research team) and PCLM combined offering, with a unified console and a single agent for system life cycle management, endpoint protection, and security configuration and vulnerability management.

- A future release will offer the choice of the Trend Micro basic firewall or the more advanced ISS Proventia firewall.

- Proventia Server and Server Sensor are expected to continue providing deep packet inspection and HIPS capabilities, sharing the same under the Protocol Analysis Module of ISS network-based appliances, and backed by the reputation and capabilities of X-Force labs.

- The ISS SiteProtector management console used to manage Proventia Server can be used to manage multiple ISS products and consolidate high-level security information.

- The IBM Global Services group offers managed security services and provides mature managed security services centralized around the ISS Proventia platform.

- Proventia server boasts very broad server support with Windows, Linux, HP-UX, Solaris and AIX, including 64-bit support for Windows and Linux, new AIX 6.1 support, and planned HP-UX Itanium support.

- For mobile laptop users, the BigFix Relay provides real-time visibility and control for endpoints, regardless of network location, and allows for updating malware definitions, engines and EPP.

Cautions

- IBM's current plans are promising, but the company has not executed well in the EPP market in the past. It remains to be seen if the current level of commitment is sustainable, and if IBM is agile enough to compete in this market.

- IBM has indicated its intent to deliver a single solution with Proventia Desktop and Trend Micro built on BigFix for clients in 2011. However, similar integration of those technologies on the server side may not occur until after 2011.

- Proventia Desktop as a stand-alone offering will likely be phased out, although IBM has indicated that existing customers will be entitled to an updated solution.

- Proventia Server is expected to continue as a separate offering controlled with the SiteProtector management console. However, Trend Micro antivirus signatures to server platforms will be delivered via the BigFix platform.

- Version 8.0 of BigFix introduced an overhauled user interface with domain-specific views to enable functional administrators to easily focus on their specific tasks, but BigFix's console is more complex than others in this market and more oriented to the operations domain.

- Security state assessments are still disjointed, lack prioritization and are missing from the dashboard.

- No support beyond Windows and Macintosh clients is offered, and there is even no ISS firewall planned for Macs. Also, no support is offered for Microsoft Exchange, Lotus Notes, SharePoint and other specialized servers, or for mobile devices.

- IBM has no encryption solution of its own, and its previous partner, PGP, was acquired by its competitor Symantec. IBM has no DLP solution of its own and relies on a relationship with Verdasys to provide this capability on endpoints (and Fidelis Security Systems for network-based DLP).

- Although IBM has its X-Force security analysis team, it has no signature-based anti-malware capabilities of its own and is dependent on Trend Micro. Disruptions in these critical partners could have an impact on customers.

- IBM provides limited device control capabilities, and the application control capabilities of Proventia are expected to be phased out.

Kaspersky Lab

Kaspersky continues to increase its brand awareness for its anti-malware labs and enterprise offerings outside of its large Eastern European installed base. Since our last analysis, Kaspersky has launched a new anti-malware engine with increased scanning speed, lower system resources impact and a redesigned administrative console. Kaspersky remains focused almost exclusively on malware protection, affecting its Completeness of Vision score, which reflects the increasing weight in our analysis on a data security strategy and/or a PCLM integration story that Gartner clients are requesting. Organizations that prefer to focus on core malware defenses only should evaluate Kaspersky. Moreover, Kaspersky should be considered a strong anti-malware engine when offered in other vendors' e-mail and Web gateways.

Strengths

- The malware research team has a well-earned reputation for rapid and comprehensive malware detection, as well as small, frequent signature updates.

- The redesigned Kaspersky console is comprehensive and offers very granular control of its agent, improving manageability for large enterprises. It also offers improved support for Active Directory, a security status dashboard, improved reporting capabilities and native client distribution capabilities.

- Kaspersky historically has a small disk and memory footprint for a comprehensive suite platform and has further improved this in its latest release.

- Kaspersky offers advanced HIPS features, including an isolated virtual environment for behavior detection, application and Windows registry integrity control, and integrated malicious URL filtering.

- The company has a strong OEM business with EPP, e-mail and secure Web gateway vendors.

- For on-demand malware scanning, Kaspersky offers the Anti-Virus Second Opinion Solution, which can be used along with competitive EPP clients.

- Kaspersky offers broad endpoint platform support, including Windows Server 2008, Citrix, Linux, Novell NetWare, Microsoft Exchange, Lotus Notes/Domino, Windows Mobile, BlackBerry and Symbian, as well as Microsoft Forefront Threat Management Gateway and EMC Celerra.

Cautions

- The redesigned Win32 console, while comprehensive, may be viewed as overly complex for SMB usage, as compared with competitors' offerings. In addition, it surfaces only malware-related events and not other types of security state information beyond its own EPP agent, such as application vulnerability and configuration assessments. It does not have any significant integration with PCLM or other operational tools.

- The dashboard is not highly customizable by the user, nor is a browser-based console available.

- The policy management paradigm is flat and lacks the object-oriented inheritance of competitive offerings, increasing the amount of work necessary to fully program policies.

- With its anti-malware focus, Kaspersky doesn't yet offer any endpoint encryption capability or DLP.

- The firewall offers no Wi-Fi-specific protection or policy support, and it has limited VPN policy options. Kaspersky's location-based policy is limited to three manually selected zones.

- Basic device control capability is coarse and is limited to device groups. It can only block or allow certain ports without providing for exceptions.

- It offers only limited application control capabilities that are not flexible enough for a large enterprise.

- Native NAC capability is missing.

- There is no SharePoint support, nor an offering uniquely targeted to address hosted virtual desktops.

LANDesk

LANDesk, established leader in the PCLM market, was recently acquired by venture investment company Thoma Bravo. The departure from Avocent will reinvigorate the company's commitment to managing and protecting diverse endpoints, including virtual and non-Windows client devices. LANDesk continues to benefit from our increased weight on more-holistic security state assessment and whitelisting, which is countered by a continued lack of a security management orientation in the product set. The company's movement in its Ability to Execute was weighted down by a restrictive pricing policy that appeals only to existing PCLM customers and a lack of market or mind share growth. LANDesk is an excellent choice for existing PCLM customers or those seeking integrated solutions for security and operations.

Strengths

- LANDesk has been a pioneer in the integration of operations and security, targeting organizations that want to leverage endpoint management infrastructures and extend this to managing desktop security capabilities.

- The LANDesk console is comprehensive and includes all security management capabilities within the same console, alerting and a new reporting framework. Likewise, the LANDesk agent has a single, modular architecture so that security functionality (like anti-malware) may be activated as needed. Policy is very object-oriented, and reuse is common. We particularly like the concept of pilot groups that get advanced copies of changes, with a set delay for subsequent rolling updates, and the ease with which it can find, assess and update any aspect of a PC, even when it's off LAN.

- LANDesk recently introduced mobile device management and security into its integrated suite to enable management of security functions of new platforms, such as iPads and mobile device platforms.

- The base LANDesk Security Suite includes an anti-spyware signature engine (Lavasoft), personal firewall, HIPS, device control and file/folder encryption, vulnerability and configuration management, patch management, and limited NAC capabilities. Customers may use LANDesk to manage McAfee, Symantec, Sophos, CA and Trend Micro, or they may choose to pay extra for LANDesk Antivirus, which is built around the Kaspersky malware scan engine.

- LANDesk HIPS and firewall technology capabilities include location-aware policies, buffer overflow protection, application whitelisting and blacklisting, and more-granular control of applications once they're executing. Whitelist administration is eased by a learning mode for the development of policies.

- LANDesk Configuration Manager provides extensive port and device control, including encryption capabilities for removable media.

- LANDesk provides NAC (LANDesk Trusted Access), which leverages four different technologies based on 802.1X, Dynamic Host Configuration Protocol (DHCP) and IP security, which is included in the base Security Suite. LANDesk also has its own DHCP server capability to enforce quarantines on noncompliant machines.

- For mobile users, the LANDesk Management Gateway provides real-time visibility and control for endpoints, regardless of network location, improving visibility and control over mobile devices.

- LANDesk offers endpoint protection for Windows endpoints, and anti-malware for Microsoft Exchange.

Cautions

- LANDesk's list pricing is expensive, because it charges for the basic management capability as a prerequisite to the Security Suite. This makes it almost impossible for security practitioners to acquire this technology without operations groups' approval and budget for the base PCLM patch components.

- LANDesk doesn't perform its own malware research, although it does have 30 engineers validating content from its partners. Still, the solution relies on LANDesk's OEM partners to review suspicious code samples and prepare custom signatures for targeted malware samples. Although signatures are becoming a replaceable commodity, business disruptions to important partners could have an impact on customers. However, this is offset by LANDesk's ability to readily manage other solutions. Encryption capabilities are also provided by partners.

- Not all LANDesk Security Suite features are available on all managed platforms. LANDesk HIPS and the LANDesk Antivirus add-on support only the Windows platform and aren't supported for Linux. There's no malware support for Microsoft SharePoint, Lotus Notes or Windows Mobile clients. Macintosh platforms benefit from PCLM tools, but antivirus is supplied by a Kaspersky-branded solution. Some mobile devices (iPhone and iPad) can be remotely restored to factory defaults, but LANDesk can't enforce native security functions.

- LANDesk should expand its application control capabilities to close the gap with dedicated application control solutions.

- In addition to its own offering, LANDesk should integrate with Microsoft NAP.

- LANDesk doesn't offer DLP or full-drive encryption.

- Customer feedback indicates that the LANDesk console is designed from an operational perspective, and that dedicated security professionals may have difficulty getting the security-specific views and reports they want. For example, security state assessment is still disjointed, unprioritized and missing from the primary dashboard. It is also not very task-oriented, and the learning curve for security operations administrators who are used to working with competitive solutions will be steep.

Lumension Security

Lumension is a new entrant in this year's analysis, after it added a licensed anti-malware engine (Norman) to its PCLM suite. The Lumension Endpoint Management and Security Suite includes anti-malware, application control, patch and remediation, power management (with wake on LAN), scan, and security configuration management modules. Lumension also offers an IT governance, risk and compliance management (GRCM) capability. Existing Lumension customers or those seeking integrated solutions for security, operations and compliance should add Lumension to their shortlist.

Strengths

- The Web-based management interface includes all PCLM products, with similar task-based orientation and consistent navigation. Dashboards can be changed for a number of widgets, allowing administrators to have their own somewhat customizable dashboards. The step-through policy workflow is similar for PCLM and anti-malware policy. The solution offers a single unified client agent for antivirus, application control, patch and remediation for a broad range of client platforms. Lumension recently added new encryption capabilities and power management. The management interface provides rich role-based restrictions, including the ability to restrict log visibility to managed groups only.

- Lumension Application Control module provides good software restriction capabilities for this class of solutions, with flexible trusted sources of change and application inventory discovery. It also offers a quick lockdown capability, which instantly authorizes all installed applications, but blocks all new applications unless they are from predefined trusted sources.

- Lumension Device Control provides a simple-to-use port and device control capability, which can limit the types of removable devices and media that may be used, the type of files that users are allowed to read/write, and specific device types. It can capture files that are written to or read from those devices and media, can limit the volume of data uploaded and downloaded, and can force encryption using a native encryption module.

- Malware prevention includes sandbox capability that intercepts and prevents changes to host files, registry settings and so on that are typically made by malware.

- A separate Risk Manager GRC tool provides security state information gathered from Lumension, and third-party tools illustrate compliance with corporate or regulatory standards over time.

Cautions

- While there is still market opportunity, Lumension has limited resources to assemble such an extensive suite. It needs to accelerate execution and raise its profile quickly to gain market and mind share before the Leaders execute on their PCLM integration strategies and eliminate Lumension's differentiation.

- Lumension still feels like a collection of technologies rather than a cohesive EPP suite. The Device Control agent is not in the Lumension Endpoint Management and Security Suite agent. GRCM is in a different interface. Lumension is reliant on its anti-malware partner Norman to review suspicious code samples and prepare custom signatures for targeted malware r samples. There is no personal firewall component; Lumension relies on the Windows firewall. Full-disk encryption is provided via partners (PGP and Symantec). Business disruptions to this important partner could have an impact on customers.

- The company does not offer DLP.

- The management interface could be improved with continuous discovery scanning to discover new rogue clients on the network, user-defined dashboard widgets, improved ad hoc and hyperlinked drill-down reporting, and more actionable and prioritized vulnerability and compliance information, as well as improved workflow between problem discovery and resolution.

- The Application Control function does not include a library of known good applications.

- Endpoint protection does not extend beyond Windows endpoints and servers. It does not provide protection for Macintoshes or specialized servers, such as Microsoft Exchange, and signatures are updated only a maximum of twice daily.

McAfee

McAfee offers a powerful, mature, complete and attractive suite of features in its Total Protection for Endpoint — Enterprise Edition Suite. It holds the second-largest market share in the endpoint protection market. The company has a broad portfolio of products, including network security components, data protection, risk and compliance, significant marketing resources, a solid operations capability, and a strong malware research and management team. In 2010, its well-executed early investment in SafeBoot firmly established McAfee as a leader in mobile data protection (encryption). It also acquired Trust Digital to extend its mobile device management and encryption capabilities into the mainstream of smartphones. The pending acquisition of McAfee by Intel brings financial resources as well as future tight integration with Intel platforms, but it also increases execution risk. McAfee continues to be a Leader, based primarily on long-term leadership in cross-product management functionality, and it should be considered a strong vendor that's suitable for any enterprise.

Strengths

- McAfee's ePolicy Orchestrator remains one of the better management capabilities in this market. Architectural benefits include a multitier architecture (agent handlers), workflow improvements (filtering by tags), support for user-based policy development (virtual groups), improved user interface design (drag and drop, search functions, customizable shortcuts, and so on), and IPv6 support. It includes trouble-ticketing system integration, such as integration with HP PC Helpdesk and BMC Remedy. Microsoft integration improvements have been made to Active Directory and System Center Configuration Manager (SCCM), especially for asset reconciliation, software deployment and root cause event visibility.

- McAfee's integration of mobile data protection (MDP) solutions was well executed in terms of time to maturity, bundling options and pricing.

- McAfee's ePolicy Orchestrator policies are customizable for each user, and all reporting requirements can be viewed and edited in a single interface. Users can select from queries and custom elements like McAfee feeds. Data that is shown in a dashboard is specific to the administrator rights or subgroup managed.

- Technology acquired from Solidcore provides a solid application control mechanism, with some trusted sources of change.

- McAfee Global Threat Intelligence (formerly referred to as Artemis), a cloud-based signature look-up system, provides a real-time look-up for the latest signature information, using lightweight queries (using the DNS protocol) to a McAfee data center.

- McAfee SiteAdvisor, along with the McAfee host Web filtering add-on module, provides decorated search results to educate end users about risky sites. It also provides host-based URL and content filtering that features integrated gateway-aware capability to enforce the appropriate policy, whether the user is on the corporate network, behind the Web gateway or outside the network. Endpoint protection is available with a SaaS-based management console.

- A new product, McAfee Management for Optimized Virtual Environments (MOVE) is one of the few solutions to centrally manage anti-malware security controls for virtual environments.

- The combination of McAfee Risk Advisor, Vulnerability Manager, remediation module, and integration with Microsoft System Center and McAfee Security Innovation Alliance partners provides improved capabilities for security state reporting.

- McAfee offers a very broad range of supported platforms, including EMC and NetApp file servers and Macintoshes.

- McAfee has a very strong endpoint DLP solution that can integrate with its more comprehensive enterprise DLP solution.

Cautions

- While Intel can help McAfee improve in the core enterprise and consumer EPP markets in the near term (that is, 12 to 24 months), longer-term investments in Intel priorities may distract McAfee from customer priorities, especially in the network security market. McAfee customers should evaluate the progress of the acquisition by monitoring McAfee's achievements in its core markets very closely.

- McAfee Risk Advisor could be better at prioritizing alerts and resulting activities to reduce the attack surface of PCs. McAfee has minimal current integration with PCLM tools, and its partnership approach will not result in tight integration. McAfee ePO is a leading solution for management, but its architecture is being tested by the demands of both network and endpoint security requirements. Integration of solutions into ePO is at various levels. ePO is not as robust and reliable as most PCLM tools, and critical reports should be validated periodically by alternative tools.

- Clients have expressed dissatisfaction with service and support overall. In 2010, McAfee experienced a significant false-positive signature, which caused significant global interruptions. While the company responded appropriately, and it has since improved its quality control considerably, it was disappointing that it was in a state that enabled such an easily avoidable event.

- Device control and DLP are not integrated in the McAfee firewall, nor with EPP policies, which may require companies to create duplicate policies for different subsystems.

- Solidcore does not have flexible trusted sources of change; it doesn't allow end users to self-authorize, request software or use a whitelist catalog. Despite integration with ePO, it is a separate product, with a distinct look and feel and separate policy development.

- The firewall's defense against dual homing (that is, two active network connections) needs to be improved. Today, the protocol stacks are not fully protected.

- The McAfee client agent is not as efficient as peers, according to industry test results (that is, PassMark Software and AV-Comparatives), and clients complain about agent footprint and scan performance.

- McAfee continues to lag other leaders and other vendors on anti-malware test results (that is, AV-Comparatives, NSS Labs and AV-Test).

- McAfee's HIPS solution is not gaining wide acceptance due to administrative overhead. It is still difficult to granularly disable rules (that is, per application) to address false positives and can be noisy partly due to uncorrelated alarms.

Microsoft

Very little has changed in Forefront Client Security (FCS) since it was originally introduced in 2007. In 2H09, based on feedback about performance and reliability during the beta testing of its Beta 1 release, Microsoft made the decision to halt the beta and perform an architectural overhaul to shift Forefront to the SCCM architecture from the embedded version of the Microsoft Operations Manager console. This shift delayed the release of Forefront Endpoint Protection (FEP) to year-end 2010, so Microsoft has once again moved down in execution, because FEP has remained frozen in time, while the rest of the EPP market has moved on. On the positive side, Microsoft is adding heuristics-based malware detection and HIPS capabilities and the ability to manage the Windows firewall in the FEP release (due at the time of this writing).

Forefront has gained only single-digit market penetration, and it is primarily adopted among budget-constrained organizations that subscribe to Microsoft's Enterprise Client Access License (ECAL) program. Forefront Protection 2010 for Exchange Server and Forefront Protection 2010 for SharePoint (under the same brand name but now in a different business unit — Microsoft Business Systems Division) remain excellent choices due to Microsoft's signature engine diversity and compatibility with these platforms. Despite difficulties with the management and console framework around its engine, the engine itself performs well, and Microsoft's labs are steadily improving in independent tests, because of the wide visibility into malware from FCS, Microsoft Security Essentials, Windows Defender and the Microsoft Malicious Software Removal Tool, as well as malware submitted by its opt-in SpyNet community.

Strengths

- In the current version, signatures and engine updates are distributed using Microsoft Software Update Services, leveraging infrastructure and knowledge that many enterprises are already using. In the year-end 2010 FEP release, this shifts to SCCM, which most organizations are also using. For these organizations, deployment of the new release of FEP will require only the purchase and deployment of the agent. No additional management servers or consoles should be required for SCCM organizations.

- Organizations that are licensed under Microsoft's Volume Licensing programs receive FCS at a discount. Organizations that are licensed under Microsoft's ECAL program receive FCS at no perceived additional cost, leading many organizations to consider Microsoft's FCS as a "good enough" way to reduce costs.

- FCS is part of a broader Forefront-branded family that includes products addressing endpoint security, server platforms (such as Exchange and SharePoint) and the network edge (for example, Unified Access Gateway and Threat Management Gateway). Plans to integrate these management consoles were scrapped, and the Forefront Protection 2010 for Exchange and Forefront Protection 2010 for SharePoint offerings were moved back into the platform teams they protect.

- Microsoft's anti-malware engine creates generic signatures that can be applied to malware families. It also creates P-code-based signatures that enable the engine to target specific behaviors, or specific event sequences for known malware, regardless of file variations. Dynamic translation capabilities enable the FEP anti-malware engine to generically decrypt malware that has tried to scramble the engine's contents. Test results such as AV-Comparatives show low false positives. The year-end 2010 release will provide additional heuristics and protocol malformation protection capabilities.

- Rather than duplicate functionality provided in the Windows OS and other platforms, FCS focuses on the anti-malware engine and, in the year-end 2010 release, will manage the Microsoft firewall.

- Forefront Protection 2010 for Exchange Server and Forefront Protection 2010 for SharePoint benefit from tight integration with these platforms and with multiple scan engines.

- FCS doesn't include a NAC/NAP product (this is handled by the Windows OS). However, FCS does include a security state assessment engine that can report on the client's current security status, vulnerabilities and relative risk levels, including FEP and non-FCS settings (like the Windows firewall).

Cautions

- Microsoft's FEP is in the middle of an architectural overhaul. Deployment of the current version is not recommended until the new version based on SCCM is available and field-tested (by the second quarter of 2011).

- If an organization is not using SCCM, the year-end 2010 release will require organizations to install SCCM to support the centralized deployment and management of the next-generation FEP agent. It is not a good fit for organizations using Altiris, LANDesk or other PCLM frameworks.

- Microsoft's FCS addresses endpoint security needs only for Windows client and server OS platforms. Non-Windows platforms aren't addressed, nor is Windows Mobile. Microsoft has announced its intent to provide Macintosh or Linux support, but no partners have been announced.

- Microsoft first released FCS in 2007, and there have been only minor updates since then. The next major release is targeted at year-end 2010. FCS's glacially slow releases aren't competitive with those provided by dedicated security vendors.

- FCS doesn't manage other built-in Microsoft client security capabilities, such as the OS firewall, User Account Control options, BitLocker encryption or AppLocker policies. The year-end 2010 release will manage only the Windows firewall.

- The current version of FCS lacks HIPS capabilities; these are planned for delivery in the year-end 2010 release.

- The current agent is relatively heavy on memory usage, compared with peers.

- FCS includes a system health agent (SHA) that integrates with Microsoft's NAP framework. However, the FCS agent doesn't provide self-enforcement, and access control enforcement requires other components of the NAP framework.

- The Windows firewall provides only basic firewall services (for example, inbound only on Windows XP), and the location-sensing policy was added in Windows 7. The firewall is owned and managed by the Windows OS team.

- Removable-device control comes from Microsoft's Windows OS group and is available only with Windows Vista and Windows 7 (which provides administrators with the ability to centrally restrict devices from being installed). Administrators can create policy settings to control access to devices, such as USB drives, CD-RW drives, DVD-RW drives and other removable media. These capabilities aren't managed by the FCS, nor are they planned for the year-end 2010 release.

- Scalability beyond 10,000 nodes with the current architecture requires the use of FCS Enterprise Manager — a tool that enables customers with more than 10,000 seats to provide centralized management and reporting across multiple logging and reporting servers and, potentially, multiple distributed FCS deployments in a large enterprise.

- Large enterprises are wary of Microsoft as an OS platform vendor selling EPP 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 various Microsoft business units — for example, the Windows division owns the firewall and the majority of HIPS techniques; the SCCM team owns Forefront Client Security; and the Business Systems Division owns the Exchange and SharePoint offerings. These groups are managed separately and have independent goals and revenue targets.

Panda Security

Panda Security is slowly expanding from its EMEA presence, radiating outward from its Spanish headquarters. However, Panda's desire to expand its installed base in North America has not materialized, and it has lost mind share. We have reflected this in its Ability to Execute score, lowering it into the Niche Players quadrant. Panda's overall Completeness of Vision score remains impacted by the increasing weight in our analysis on a data security strategy and/or PCLM integration story, but it has shown innovation in its Cloud Office Protection solution. SMBs seeking a comprehensive, more-customer-intimate alternative should consider Panda as a good shortlist entry in the geographies it supports.

Strengths

- The Windows-based management interface provides very granular role-based management and group-level configurations. The dashboard provides a quick view to see PCs that don't have agents installed and to push new agents via .msi files. The solution provides an easy-to-use report scheduler that delivers reports in a PDF format.

- Panda malware detection includes integrated anti-malware and anti-spyware, as well as several proactive HIPS detection techniques.

- Panda offers very good rootkit inspection that bypasses a potentially rootkitted OS to read raw data directly from the hard drive to look for hidden processes.

- The product also enables the blocking of known-malicious URLs.

- Panda's HIPS capability includes policy-based rules, vulnerability shielding and behavior-based detections, and administrators have very granular control to modify policies or add exclusions.

- The application control module, TruPrevent Technologies, uses application profiles to enforce runtime behavior and permissions for well-known applications. Administrators can opt in or opt out of TruPrevent, and they can modify rules or create their own rules to override Panda's rules.

- Panda Security for Desktops and Panda Security for File Servers use a cloud database look-up to detect new threats.

- Malware Radar is Panda's network-crawling malware and vulnerability audit tool. It can be a good utility for double-checking incumbent anti-malware accuracy. Malware Radar uses a different scanning engine, with more-advanced detection techniques activated (which takes longer to scan and potentially produces more false positives) than the base Panda product.

- Panda pricing is very competitive, and there are no upfront license costs, only an annual subscription.

- Panda offers a SaaS-based management solution for endpoint protection, which is fully hosted by Panda, called Panda Cloud Office Protection. References cite it as being extremely valuable for managing remote installations.

Cautions

- Despite Panda's globalization plans, the installed base is still mostly EMEA SMBs. Panda lacks brand recognition in North America or Asia/Pacific, and its efforts to grow its North American installed base have stalled.

- The server-based management console (not Panda Cloud Office Protection) is still a Windows fat client, rather than a more-flexible, browser-based management console. It also lacks advanced features, such as adaptable dashboards, consolidated compliance status indicators, hyperlink drill-downs to log data and custom reporting.

- Panda distributes only one signature update per day for clients not using the cloud look-up mechanism.

- Panda's HIPS capabilities are powerful. However, in many cases, they are ahead of the market demand for these capabilities and, in other cases, lack features to make HIPS more manageable — for example, Panda's HIPS policy doesn't provide a monitor-only mode to enable testing and tuning before deployment. Moreover, TruPrevent identifies files only by name and can be thwarted by changing file names.

- Panda still lacks advanced firewall features, such as location-based policies, wireless-specific firewall options and VPN integration options.

- There's only one option to minimize the impact of scheduled scanning (CPU load limitation), although end users can delay scanning if they're authorized.

- The end-user GUI is minimal, and end-user controls are limited to performing on-demand scanning, as well as to changing the signature update mechanism and proxy settings.

- Cloud Office Protection is not feature-rich for large enterprises.

- The agent managed by Cloud Office Protection is a subset of the full Panda client — for example, it lacks HIPS capabilities and provides no application control capabilities.

- Malware Radar uses a separate console for reporting its information (for example, critical vulnerability information surfaced by Malware Radar isn't visible in the main console).

- Panda is focused on traditional Windows and Linux support and doesn't support any mobile clients. Panda is offering a stand-alone Antivirus for Mac product, and a corporate version is expected to be launched by the end of 2010. Panda doesn't support Microsoft SharePoint, nor does it offer a solution that addresses the needs of terminal services or hosted virtual desktop environments.

- Panda doesn't yet offer many additional EPP components, such as port and device control, encryption, or DLP.

- Panda provides no significant state assessments beyond the EPP agent (that is, application vulnerability and configuration assessments) and outside of its separate Malware Radar tool. Panda also provides no significant integration with PCLM and operational tools.

SkyRecon Systems

In November 2009, Arkoon Network Security, a European unified threat management vendor, announced the acquisition of SkyRecon. Although this acquisition will provide SkyRecon with greater technical resources and investment capabilities, linking network security and endpoint security has not been a successful strategy in the past. SkyRecon's Ability to Execute score is hampered by its relatively small market share and limited geographic presence, lack of a native malware detection engine, and its still-maturing management capabilities. SkyRecon is a reasonable shortlist vendor for organizations that are in supported geographies seeking data protection solutions and willing to invest extra effort to bolster the administration.

Strengths

- The company's flagship product, StormShield Security Suite, is designed to address system and data protection via an extensible EPP capability that integrates multiple layers of security. These include HIPS; a personal firewall; Device Control System (DCS); encryption; and an optional, signature-based, anti-malware engine licensed from Panda Security, Avira or Microsoft.

- We particularly like the company's primary focus on techniques to block unknown threats, using a combination of configuration policies, such as application control, very fine-grained device control and a flexible firewall policy, as well as proactive HIPS capabilities, such as features for blocking keyloggers and targeted attacks. SkyRecon effectively uses policy-based restrictions to minimize the attack surface with object-oriented policies and configurations that are easy to set up. Policy-based application control is improved by a "challenge response" mechanism, which allows users to add software if they type in the justification for the installation in a pop-up window.

- Other defenses include rootkit detection, honey pots, privilege escalation and reboot protection.

- The firewall provides good Wi-Fi policy options, as well as options to force VPN connections.

- The company recently added Flexible Data Encryption (FDE) for files and folders on fixed hard drives and removable devices. FDE is integrated with the DCS service to provide device encryption and to audit device file activities.

- SkyRecon has a single management interface and a single lightweight agent (10MB) to support its multiple functions.

- Full-disk encryption has been added in the latest version.

- The product features granular device control policies, including controlling access to optical drives and blocking print-screen printing for a specific application.

- Increased compliance auditing and reporting capabilities have been added.

Cautions

- Although it continues to grow rapidly, SkyRecon is still one of the smaller vendors in this analysis. It has a limited enterprise client base and lacks significant brand recognition outside of France. Arkoon also does not have a significant business presence outside of French markets.

- It supports only 32-bit Windows clients (64-bit is due in the first quarter of 2011) and provides no Mac, Linux, Unix, mobile or e-mail server support.

- The company has a very small malware research team and is dependent on Panda Security, Avira or Microsoft for signature-based protections.

- The management interface was very complete, but it looks like it requires a steep learning curve, and it lacks context-sensitive help. Help file documentation is available only in a PDF format.

- Ad hoc reporting is not supported. Reports can be filtered but not changed, and it is not possible to drill down into details. No dashboard function is present.

- There is no significant native security state assessment beyond the EPP agent, and no significant integration with operations tools.

- It does not yet offer any DLP solution.

Sophos

Sophos is a veteran anti-malware company that is dedicated to the enterprise market. More-ambitious management has resulted in excellent growth and geographic expansion from its European base to the North American and global enterprise markets. Sophos' Completeness of Vision score continues to benefit from its data and port protection. The Sophos EPP suite offers a good balance of integrated malware, personal firewall, HIPS defenses and data protection capabilities that are deterministic and easy to deploy and manage. Organizations that prefer a broad EPP suite with simplified management capabilities should consider Sophos.

Strengths

- Sophos continues to have a strong reputation for support and service from customers and its channel.

- The management interface was upgraded with improved ease of use and better role-based administration and reporting since our last analysis. The dashboard is complete with actionable information and offers right-click remediation options via integration with third-party patch management tools. Windows, Mac, Linux and Unix clients are all supported in the management console.

- Microsoft vulnerability and patch assessment information is available with Sophos NAC Advanced (available at extra cost), which provides excellent client security status information.

- Malware detection improved in 2010 with the introduction of Sophos Live Protection, a cloud-based real-time protection update mechanism and improved client tamper protection.

- Sophos also provides integrated client-based malicious website blocking and URL reputation, as well as a JavaScript emulation to identify and block potentially malicious Web code.

- Sophos offers full disk and file encryption, encryption key management, endpoint DLP, and very granular device control in its suite.

- Sophos provides basic application control capabilities that enable administrators to define and update a whitelist of authorized applications, and enable the blocking of potentially unwanted applications, such as instant messaging products or media players, by name or category.

- Sophos offers a limited NAC enforcement capability embedded in the EPP agent and an advanced NAC solution at extra cost.

Cautions

- Sophos is continuously challenged in differentiating itself from the "big three" players in the Leaders quadrant. Lack of consumer products has resulted in low brand recognition. The company must continue to focus on expanding its international channel to overcome its limited presence in Asia/Pacific, the Middle East and South America.

- Although it does have a growing number of very large enterprise customers, and the management console is designed for ease of use, it lacks the depth found in the large-enterprise features of other Leaders. Policy development is eased with pop-up windows, check boxes or prepopulated menu lists, which can be limiting for more-experienced administrators.

- The application control list of categorized applications is limited to what Sophos sees as potentially malicious. In addition, there is no way to lock down to a specific set of applications, nor is there an ability to allow trusted sources of change.

- It offers only binary configuration of two HIPS rules — suspicious behavior and buffer overflows — although it can exempt specific applications from HIPS policies.

- Security state detection is done via Sophos NAC Advanced and Sophos Compliance Manager, which have a different look and feel, and state information is limited to Microsoft applications.

- Sophos Enterprise Console does not yet manage encryption deployment, policy management or reporting (which is due in the second half of 2011), and it does not offer centralized management for its gateway and EPP solutions.

- Endpoint DLP (other than encryption) is weaker than vendors that specialize in this market. Sophos is not a major vendor in the more comprehensive enterprise DLP market.

- Sophos' support for mobile clients is limited to Microsoft, and it does not yet address the specific needs of virtualized clients or servers.

Symantec

Symantec continues to have the largest EPP market share, but its lead is gradually eroding. With the acquisitions of GuardianEdge and PGP, Symantec will be able to offer a more complete suite, including data protection. Symantec provides a very comprehensive and effective malware protection solution and is an excellent and safe shortlist candidate for any large global enterprise, particularly those that appreciate PCLM and EPP integration.

Strengths

- Symantec continues to perform well in numerous tests of malware effectiveness (for example, AV-Comparatives, AV-Test, NSS Labs and PassMark) compared with peers. The enterprise version will benefit from file reputation and prevalence technology, now called Ubiquity, in its enterprise solution in 2010, which should improve detection rates.

- Symantec recently launched the Symantec Protection Center (SPC), which provides a central management point and dashboard viewer for a number of Symantec protection products (Web Gateway, Critical System Protection and Endpoint Protection). SPC also provides consolidated dashboard and reporting and a unique process manager to automate repetitive IT processes. Reports are composed via Microsoft Report Builder, which makes it easy to transparently add reports as new dashboard elements with Microsoft management tools. This makes it easy to create performance indicators, which display as gauges and graphs. A workflow process designer includes predefined templates and the ability to create custom templates.

- Many helpful common tasks are automated, including finding unmanaged PCs, installing Symantec Endpoint Protection (SEP), implementing endpoint recovery and ensuring configuration compliance.

- Symantec provides good port and device controls, mobile device synchronization, and the best firewall of any ranked vendor. A Snort format may be used to create HIPS rules for firewalls capable of deep packet inspection.

- The client has a large disk footprint but is very fast and light on memory usage in several tests (that is, PassMark and AV-Comparatives). Administrators can delegate most controls to the end-user GUI very simply. The client also boasts the most policy controls to limit the performance impact of the scheduled scan.

- Symantec also offers data backup and remote-access technology and imaging technology in the Symantec Protection Suite Enterprise Edition, but these technologies haven't yet made their way into the EPP management console.

- Symantec's acquisition of Altiris, a leader in the PCLM market, will be a significant asset as the PCLM integration trend continues. Symantec will be able to leverage PCLM functionalities, such as asset discovery and inventory, configuration management, vulnerability assessment, and software management and distribution capabilities.

- Symantec has also made significant investments in DLP, and it offers a client DLP agent as a component of the Vontu DLP suite.

- Symantec covers a broad range of endpoints, including Windows Mobile, Symbian, Palm, Linux and Mac.

- Symantec can monitor other anti-malware engines (but it can't manage them).

Cautions

- Symantec has made a number of visionary investments for its EPP solution; however, it is continuously challenged with ensuring fast integration of its various acquisitions. SPC is a good start but still operates more like a portal and log consolidation and reporting engine than a true integration of disparate products. Despite significant improvements and product management focus since Symantec AntiVirus 10, the company still gets low marks on overall customer satisfaction from reference customers.

- Altiris is a significant asset for Symantec as these two disciplines integrate, but it is notably absent from SPC, and SEP cannot exploit any Altiris functions. However, presently, the Symantec Protection Suite Enterprise Edition for Endpoints includes Altiris Inventory, and Altiris IT Analytics can merge SEP and Altiris data in the SPC console. More work is needed to deliver detailed state assessments, beyond the basic information reported by the SEP agent so that reports are prioritized, correlated and actionable. For example, there is currently no relationship between severity indicators and the list of active prevention measures.

- Symantec has limited capability on smartphones and essentially is starting over with an investment in Mocana, as its distribution arrangement with Trust Digital is terminated.

- Symantec does not offer optimization or deployment architectures for virtual machines. However, existing SEP features, such as randomization and lightweight clients, make it reasonably efficient in these deployments.

- List pricing is expensive, on average, compared with other EPP vendors, but negotiated pricing is typically on par with its closest competitors.

- Symantec's Ubiquity solution will need to be more flexible and implement the concept of trusted sources to work effectively in the enterprise market. Ideally, it should exploit the Altiris application catalog to provide an application control capability rather than a simple file reputation score.

- HIPS rules in the anti-malware engine do not allow for rule-based exceptions.

- Port Control capability is spread over multiple products (SEP, Encryption and DLP), which may create enforcement gaps and complicate management.

- Symantec's HIPS solution for servers, Symantec Critical System Protection, is a separate product from SEP 11, with a different agent and management console (although it can be managed from SPC).

Trend Micro

Trend Micro is the third-largest anti-malware vendor, with a significant market presence in Asia/Pacific and EMEA, and one of the larger worldwide networks of labs and monitoring capabilities. Trend Micro slipped slightly again this year in its Ability to Execute and Completeness of Vision due to its continued narrow focus on signature-based malware prevention versus other Leaders. Trend Micro should be considered by organizations seeking a solid, signature-based anti-malware solution.

Strengths

- OfficeScan provides anti-malware, anti-spyware, and basic firewall and Web threat protection in a single product. It also offers an optional advanced deep-packet-inspection-based HIPS firewall (Intrusion Defense Firewall) in a single agent and management interface. It also provides DLP for endpoint capabilities in a separate management console and agent.

- Trend Micro recently acquired Mobile Armor to provide full disk, file and folder encryption and will begin integrating this solution into the native management console.

- Trend Micro was the first vendor to introduce a cloud-based signature capability called the Smart Protection Network. This network of cloud-based data centers allows clients to perform a real-time query of global signature and Web reputation databases to get the very latest reputation information. This lightens the client footprint and eliminates the signature distribution time lag. Larger clients can benefit from a local Smart Protection Network server.

- With the release of OfficeScan 10.5, Trend Micro delivered a virtual desktop infrastructure (VDI)-aware solution (Citrix and VMware). This improves performance and security by preventing resource contention, and by leveraging base image prescanning to avoid duplicate scanning among multiple virtual desktop images, which has a significant impact on VDI density. It also offers a deep security platform and agentless virtual machine solution that provides agentless security for multiple virtual machine environments.

- OfficeScan protection is bolstered by the capability to block malicious URLs at the client level, critical system resources and process protection, which blocks malicious changes and behavioral monitoring.

- Client performance in version 10.5 is improved.

- Trend Micro offers a SaaS-based management console.

- Trend Micro offers a unique threat management service, which combines out-of-band VMware servers that monitor networks for malicious traffic with a service-assisted remediation and incident management service, to its premium support customers. It also offers it as a stand-alone solution to monitor incumbent EPP solution effectiveness.

- Trend Micro offers broad platform coverage for endpoints and servers, including native Mac support, mobile device protection, Microsoft SharePoint, Microsoft Exchange and network-attached storage, in a single management console.

- The company has made investments in endpoint DLP.

Cautions

- Trend Micro's tendency to rely on in-house development, combined with very conservative development investments and an over-reliance on partnerships versus acquisitions, has resulted in slight declines in both Completeness of Vision and Ability to Execute scores in this analysis. Recent acquisitions (Provilla, Third Brigade and Mobile Armor) are welcome changes, but most came well after the competition had made similar moves.

- The BigFix partnership improves manageability in environments with distributed management servers connected over low-bandwidth connections. However, it failed to gain significant installed-base traction, and the recent acquisition of BigFix by IBM has clouded the future of this partnership.

- Trend Micro product management has not embraced PCLM integration, nor appreciated the value of more-holistic security state assessments or application control.

- Control Manager doesn't yet have the richness of reporting or dashboards that other solutions do. Rogue client detection is a manual process.

- OfficeScan provides few application control capabilities. However, the Intrusion Defense Firewall plug-in (available at an additional charge) can control applications at the network level, but can't block specific controls from running in a browser. However, execution and firewall behavior rules are in different policy settings, complicating management.

- Trend Micro port and device control capabilities are very limited, granting just read-only or executing control on storage devices.

- Its endpoint DLP is weaker than vendors that specialize in this market. Trend Micro is not a major vendor in the more comprehensive enterprise DLP market.

- 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.

Vendors Added or Dropped

We review and adjust our inclusion criteria for Magic Quadrants and MarketScopes as markets change. As a result of these adjustments, the mix of vendors in any Magic Quadrant or MarketScope may change over time. A vendor appearing in a Magic Quadrant or MarketScope one year and not the next does not necessarily indicate that we have changed our opinion of that vendor. This may be a reflection of a change in the market and, therefore, changed evaluation criteria, or a change of focus by a vendor.

Evaluation Criteria Definitions

Ability to Execute

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

Overall Viability (Business Unit, Financial, Strategy, Organization): Viability includes an assessment of the overall organization's financial health, the financial and practical success of the business unit, and the likelihood that the individual business unit will continue investing in the product, will continue offering the product and will advance the state of the art within the organization's portfolio of products.

Sales Execution/Pricing: The vendor's capabilities in all 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 to influence the market, promote the brand and business, increase awareness of the products, and establish a positive identification with the product/brand and organization in the minds of buyers. This "mind share" can be driven by a combination of publicity, promotional initiatives, thought leadership, word-of-mouth and sales activities.

Customer Experience: Relationships, products and services/programs that enable clients to be successful with the products evaluated. Specifically, this includes the ways customers receive technical support or account support. This can also include ancillary tools, customer support programs (and the quality thereof), availability of user groups, service-level agreements and so on.

Operations: The ability of the organization to meet its goals and commitments. Factors include the quality of the organizational structure, including skills, experiences, programs, systems and other vehicles that enable the organization to operate effectively and efficiently on an ongoing basis.

Completeness of Vision

Market Understanding: Ability of the vendor to understand buyers' wants and needs and to translate those into products and services. Vendors that show the highest degree of vision listen to and understand buyers' wants and needs, and can shape or enhance those with their added vision.

Marketing Strategy: A clear, differentiated set of messages consistently communicated throughout the organization and externalized through the website, advertising, customer programs and positioning statements.

Sales Strategy: The strategy for selling products that uses the appropriate network of direct and indirect sales, marketing, service and communication affiliates that extend the scope and depth of market reach, skills, expertise, technologies, services and the customer base.

Offering (Product) Strategy: The vendor's approach to product development and delivery that emphasizes differentiation, functionality, methodology and feature sets as they map to current and future requirements.

Business Model: The soundness and logic of the vendor's underlying business proposition.

Vertical/Industry Strategy: The vendor's strategy to direct resources, skills and offerings to meet the specific needs of individual market segments, including vertical markets.

Innovation: Direct, related, complementary and synergistic layouts of resources, expertise or capital for investment, consolidation, defensive or pre-emptive purposes.

Geographic Strategy: The vendor's strategy to direct resources, skills and offerings to meet the specific needs of geographies outside the "home" or native geography, either directly or through partners, channels and subsidiaries as appropriate for that geography and market.