Magic Quadrant for Endpoint Protection Platforms

Gartner RAS Core Research Note G00166218, Peter Firstbrook, Arabella Hallawell, John Girard, Neil MacDonald, 4 May 2009, RV2A2 08072009

The traditional blacklist antivirus capability is insufficient protection from today's more-professional malware threats. EPP vendors are competing on the strength of non-signature-based defenses, proactive management capabilities to reduce the attack surface, and data protection.

WHAT YOU NEED TO KNOW

Standard anti-malware signature engines are rapidly losing effectiveness against the surging volume of new threats, and have very little value against targeted threats. Non-signature-based solutions (such as a host-based intrusion prevention system — HIPS) and proficient operations procedures (such as asset discovery, configuration management, vulnerability assessment, software management and whitelisting) are needed to help inoculate PCs against unknown threats.

Endpoint protection platform (EPP) vendors continue to improve data protection. Several added or improved full-disk and removable media encryption, content-aware data loss prevention (DLP), and device and port controls. Data protection strategies must include consideration of the role of EPP vendors in providing some or all of this technology.

Pricing of EPP suites reflects the increased competition for basic signature-based defenses as suites continue to add functionality without significant price increases. Early competitive bidding is essential to get the best prices from incumbent vendors.

MAGIC QUADRANT

Market Overview

Threat Changes: There were no major changes in the threat landscape in 2009, but negative trends continue unabated.

Malware is increasingly Web-based (that is, it uses the Web as a distribution method and a command-and-control channel) and multistage — meaning there are multiple components that can be installed after the initial infection, depending on the motivation of the attacker and the victim's profile. In addition, the exploits of socially engineered trojans, which trick end users into downloading and executing malicious files, are on the rise and will continue to cause havoc in 2009 and beyond.

There continues to be a dramatic increase in the volume of unique malware, due to the maturity of the malware development industry and the increased use of automated "toolkits" (that is, Neosploit, MPack and CuteQQ) for malware development. The ability of signature-based systems to catch new and/or targeted malware is declining. Even heuristics and HIPS

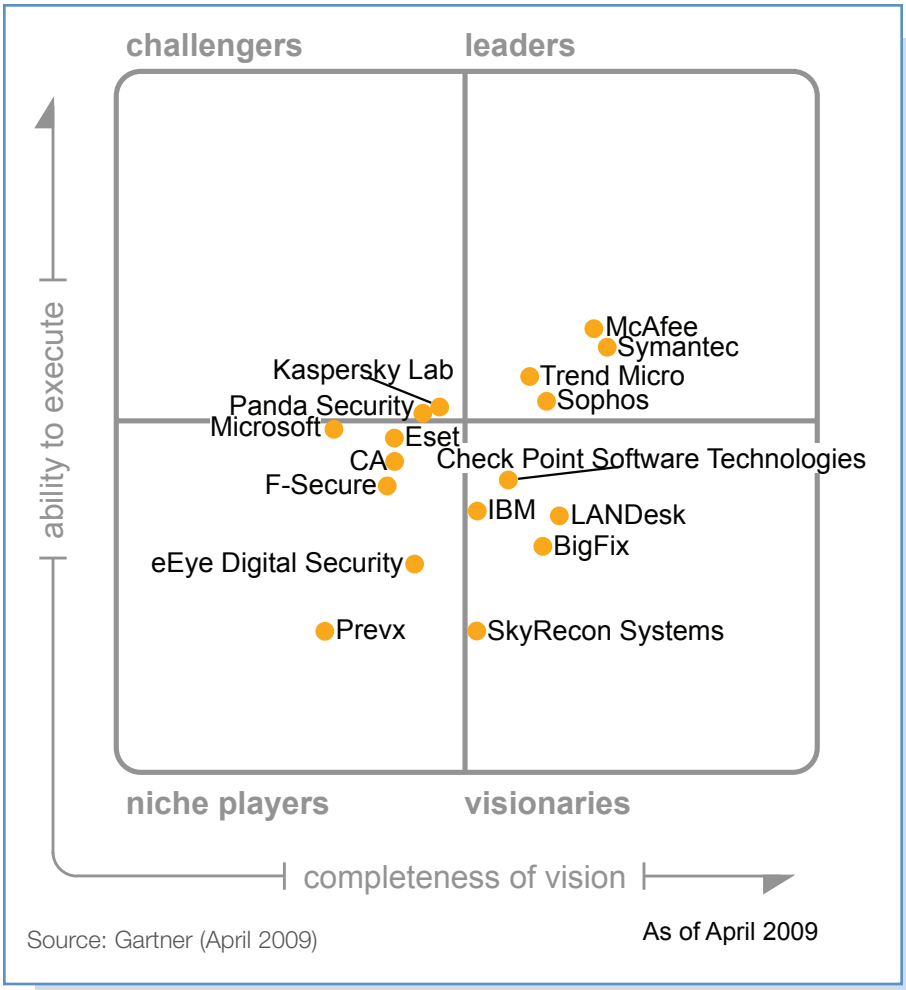
Gartner

techniques in signature engines are failing to bridge the gap. Despite the pressing need for proactive measures, IT organizations continue to be reluctant to enable full-featured HIPS for fear of increasing their administration.

Furthermore, as Web-based threats become the dominant vector for malware, companies and vendors will continue to invest and experiment with application control, alongside better and more-automated ways to detect which Web sites, applications (and versions of applications), and files can't be trusted. In addition, vulnerability assessment and patch management reporting will become important feedback loops to support application control strategies.

Product Changes: To address the increasing velocity of malware, some EPP vendors (notably Trend Micro, McAfee, F-Secure and Prevx) are adding some form of client queries directly to an "in the cloud" master-signature database for unknown, suspicious files. Other vendors are focusing on techniques to decrease the synchronization time between master-signature and local-signature databases. Given the accelerated distribution of unique threats, these efforts to speed up signature distribution are beneficial; however, it's becoming abundantly clear that the effectiveness of signatures in the face of swarming malware is declining. We note that Gartner clients suffered from rising infection rates in 2008 and early 2009.

Figure 1. Magic Quadrant for Endpoint Protection Platforms



Vendors are also addressing the shift in malware distribution with client-based techniques for detecting and blocking infected or suspicious Web pages and/or script-based attacks. In 2009, several vendors focused on improving "rootkit" scanning techniques, and this feature remains a differentiator.

Security vendors are gradually understanding the benefits of PC life cycle tools (such as asset discovery, configuration management, vulnerability assessment and software management) as a way to reduce the attack surface of endpoints. In essence, PC security requires better PC management. Meanwhile, operations vendors like BigFix and LANDesk, which already understand the utility of effective management, are improving their signature and HIPS defenses with security vendor partnerships and acquisitions.

Unfortunately, most vendors are perusing integration too cautiously. The security vendors (with the exception of Symantec) are fearful of stepping into unknown markets, while the operations vendors don't get enough security credibility in enterprises. Still, we're seeing signs of progress. McAfee is taking steps with the integration of Foundstone and Citadel Security Software into its management console, ePolicy Orchestrator (ePO) v.4; Trend Micro and IBM recently licensed BigFix technology; eEye Digital Security has an integrated vulnerability management solution; and Symantec is working on integrating Altiris into Symantec Endpoint Protection (SEP) management. EPP buyers must understand the benefits of this trend and consider PC life cycle configuration management (PCLCM) needs before investing in EPP solutions.

Using the whitelists of known-good/safe applications to accelerate scanning, or actually limiting the execution or network access of applications to a known set of good applications, is gaining ground. Vendors such as Bit9, CoreTrace and Lumension are augmenting, and, in some domains, replacing signature-based antivirus detection by locking PCs into a known good state and only allowing "good" applications to run. Gartner believes that, in 2010, leaders and visionaries should significantly develop this defensive technique.

EPP vendors continued to execute on another broad theme outlined in "Introducing the Endpoint Protection Platform": improving data protection. Several vendors have added or improved full-disk and removable media encryption, content-aware DLP, and device and port control (which is becoming a standard feature of EPP suites). The port and device policy is a simple, proactive configuration measure that can help with DLP and protect PCs from autorun worms in Universal Serial Bus (USB) storage (which resurged in 2008). With the exception of device control, we repeat our guidance from 2007 that, although these data protection strategies are convenient when they're part of the management console for EPP, there are numerous factors besides management ease that must be considered when acquiring DLP technology. DLP buyers should add their incumbent EPP vendors to shortlists, but must consult with other stakeholders to determine enterprise needs first.

Although many of the vendors in this Magic Quadrant include limited network access control (NAC) functionality, only four vendors (Check Point, McAfee, Sophos and Symantec) met the criteria for inclusion in the "Magic Quadrant for Network Access Control." Many EPP vendors in this Magic Quadrant have the ability to baseline an endpoint for NAC compliance, but most haven't focused heavily on solutions to enforce access for unmanaged or guest machines. NAC projects are driven primarily by network managers, most of whom prefer a network-based solution to enforce access control. This trend makes it difficult for EPP vendors to gain "mind share" with network managers.

Most of the other EPP suite improvements in 2009 can be grouped into manageability and client transparency. It was a big year for consolidating multiple EPP components into single expandable agents, thereby reducing the footprint of these agents. Other improvements focused on increasing the scanning speed, and other features aimed to decrease the impact of scheduled scans. Vendors also focused on increasing platform coverage for Vista (32-bit and 64-bit support), Mac, Linux and VMware platforms; however, broad platform coverage is still rare.

Market Definition/Description

Enterprise antivirus, anti-spyware, personal firewall and desktop HIPS products compose the majority of endpoint security spending. The combined revenue of these segments was more than $2.5 billion in 2008, and we anticipate that the EPP market will grow at a compound annual growth rate of 8%, driven by an increase in data products in the near term and PC expansion in the post-downturn era.

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

Microsoft's impact on the enterprise market is still extremely small, and mostly with companies looking to reduce costs. We still expect it to have a growing market share in 2010, but primarily in Microsoft-centric small and midsize businesses (SMBs).

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

Inclusion and Exclusion Criteria

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

- Products must provide malware (that is, virus, spyware, rootkit, trojan, worm) detection and cleaning, a personal firewall, and HIPS for servers and PCs.
- Centralized management, configuration and reporting capabilities for all products listed above, sufficient to support companies of at least 5,000 geographically dispersed endpoints.
- Global service and support organizations to support products.

Added

In 2009, we added Prevx, Eset and SkyRecon Systems to the list of EPP vendors.

Dropped

Bit9 and Webroot appeared in "Magic Quadrant for Endpoint Protection Platforms, 2007."

The 2009 inclusion criteria required vendors to offer signature-based anti-malware detection and removal capabilities. Although signature-based malware detection has numerous faults, it's still the anchor product in client buying decisions, and is a necessary (but insufficient) solution component for scanning/removal of known malware. Bit9's capability to lock endpoints and only allow known-good applications to be added is an excellent protection strategy. It's clearly viewed as a feature of a fuller EPP solution, or as a solution only for specific endpoint domains.

Although Webroot will continue to have a presence in the endpoint protection market with a stand-alone anti-malware solution, it won't pursue an EPP suite strategy. From now on, Webroot is mainly focused on pushing enterprise security (Web and e-mail) into the cloud.

Evaluation Criteria

Ability to Execute

The key ability-to-execute criteria used to evaluate vendors in 2009 were customer experience and market responsiveness and track record. The following criteria were evaluated to contribute to the vertical dimension:

- **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 evaluated product stability and performance, company experience with the vendor's support, and signature quality and response times. We evaluated comments from Gartner clients and reference customers, as well as from tests (such as AV-Test.org) and other sources of data on performance and signature response times.
- **Operations:** We evaluated companies' resources that were dedicated to malware research and product R&D.

Completeness of Vision

The most-important vision criteria in 2009 were market understanding and the sum of the weighted offering (product) strategy score:

- **Market Understanding:** Describes vendors that understand customer requirements for proactive and integrated defenses across all malware threat types, the need for better management and data security, and vendors that have an innovative and timely road map to provide these functionalities.
- **Offering (Product) Strategy:** When evaluating vendors' product offerings, we looked at the following product differentiators:
  - **Anti-malware Signature Capabilities:** Speed, accuracy, transparency and completeness of signature-based defenses.
  - **HIPS Capabilities:** The quality, quantity, accuracy and ease of administration of non-signature-based defenses.
  - **Personal Firewall Capabilities:** Advanced capabilities that exceed Microsoft's, such as location-based policy, specific virtual private network (VPN) and wireless rules, and USB and other port protection.
  - **Management and Reporting Capabilities:** Comprehensive centralized reporting that enhances the real-time visibility of end-node security state and administration capabilities, which ease the management burden of policy and configuration development. Vendors that have embarked on PCLCM-style operation integration showed considerable leadership and were given extra credit for this criterion.

Table 1. Ability to Execute Evaluation Criteria

Evaluation Criteria	Weighting
Product/Service	No Rating
Overall Viability (Business Unit, Financial, Strategy, Organization)	Standard
Sales Execution/Pricing	Standard
Market Responsiveness and Track Record	High
Marketing Execution	Standard
Customer Experience	High
Operations	Standard
Source: Gartner (April 2009)	

Table 2. Completeness of Vision Evaluation Criteria

Evaluation Criteria	Weighting
Market Understanding	High
Marketing Strategy	No Rating
Sales Strategy	Low
Offering (Product) Strategy	High
Business Model	No Rating
Vertical/Industry Strategy	No Rating
Innovation	Low
Geographic Strategy	Low
Source: Gartner (April 2009)	

- **Data and Information Protection:** In 2009, we increased the emphasis on 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.

Other criteria evaluated were:

- **Sales Strategy:** We evaluated each vendor's licensing and pricing programs and practices. Vendors that emphasized value to clients, that tended to incorporate new functionality without "up charges," and that were reasonable during renewal negotiations received high scores. We incorporated feedback from clients, reference customers, and channel partners on negotiation tactics and pricing strategies. We also evaluated the vendors' partnership strategies. We accounted for how vendors approached new channels and delivery models.

- **Innovation:** We evaluated vendors' responses to the changing nature of customer demands. We accounted for how vendors reacted to malicious code threats, such as spyware and targeted attacks, 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 actions in advanced malware protection, data protection and/or management capabilities 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 are warned not to assume that they should buy only from vendors in the Leaders quadrant. Some clients, however, may 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 have stronger sales, visibility and/or clout, which add up to higher execution than niche players. Challengers are good at competing on basic functions rather than advanced features. Challengers are efficient and expedient choices for narrowly defined problems.

Visionaries

Visionaries invest in the leading/"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, they may enjoy more personal attention.

Niche Players

Niche players offer viable, dependable anti-malware solutions that meet the specialized needs of specific buyers. Niche players are less likely to appear on shortlists, but fare well when given a chance. Niche players may address 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 functions and features that are important to them.

Vendor Strengths and Cautions

BigFix

BigFix has a strong reputation for its software distribution and patch management capabilities, and is a visionary competitor in the PCLCM market. The company is growing rapidly, with approximately 20% of its revenue now derived from the sale of endpoint protection modules. In 2009, BigFix moved up in execution primarily on the value of strategic licensing deals that will increase its channels and enterprise profile. Its position also moved to the right due to better malware detection, given its move to the Trend Micro scan engine. BigFix also benefits from increased weight on management and PCLCM integration. BigFix is an excellent choice for organizations that are looking for very robust management of endpoints, integration of PCLCM capabilities, and the ability to manage endpoint security technologies from multiple vendors.

Strengths

- The BigFix agent-driven architecture for delivering content, managing configurations and real-time reporting receives high marks from customers on its ability to scale and its efficient use of bandwidth. The company is one of the few PCLCM vendors to leverage infrastructure for endpoint security.

- BigFix's optional EPP offering is robust and offers multiple components: Device Control; Asset Discovery; limited NAC and optional AntiVirus/AntiSpyware/firewall; rootkit detection; and Web Protection Module.

- As part of a broad cross-licensing agreement with Trend Micro, the company recently replaced CA as its anti-malware engine and now offers the Trend Micro scan engine. In addition, BigFix can manage a large number of third-party anti-malware solutions, including Symantec and McAfee, which is a valuable capability for mixed environments and migration.

- For a firewall, the BigFix Firewall (licensed from CA as a result of its acquisition of Tiny Software, and included in the EPP add-on) may be used; otherwise, BigFix may be used to manage a third-party firewall offering or Microsoft's integrated Windows XP and Vista firewall.

- Add-on security modules include data loss prevention, patch management, Security Configuration Management and application control (offered by Bit9 via integration with the BigFix platform).

- Device control is comprehensive and built into the BigFix EPP add-on, including encryption as well as capabilities to disable and enforce policies for removable media, USB devices, CD-ROMs/DVDs, floppy drives, parallel ports, infrared ports, Bluetooth and PC Card devices.

- For encryption capabilities, the BigFix unified management platform can deploy, manage and report on the state of multiple endpoint encryption technologies, including Pointsec Mobile Technologies, GuardianEdge Technologies, Mobile Armor and PGP.

- 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

- Although the BigFix security module is price-competitive with other EPP suites, there may be some reluctance to introduce another PCLCM infrastructure for organizations that already have a competitive operations tool.

- BigFix doesn't perform its own primary malware research, and instead relies on its OEM partnerships with CA and Trend Micro. BigFix is dependent on its malware partners to review suspicious code samples and prepare custom signatures for targeted viruses. Although we agree that signatures are becoming a replaceable commodity, business disruptions in this important partnership could impact customers.

- BigFix's primary installed base is in North America, where it derives 80% of its revenue. It isn't as well known in other parts of the world. The remaining 20% of its revenue is split between Europe, the Middle East and Africa (EMEA) and Asia/Pacific. Its customer base is dominated by a relatively small number of very large (more than 5,000 seats) clients. BigFix is planning an aggressive expansion into EMEA and Asia/Pacific to support its IBM and Trend Micro partnerships.

- BigFix Endpoint Protection Suite is targeted at Windows endpoints and doesn't protect Unix, Linux, and Mac platforms, or specialized servers such as Exchange, SharePoint, or network-attached storage or storage area networks.

- The BigFix agent provides no support for any mobile device platforms — EPP or otherwise — although management of these devices (but not EPP) is planned for 2009.

- BigFix provides no native file, folder or full-disk encryption capabilities, although these are planned for 2009.

- BigFix lacks significant HIPS capabilities beyond those found in the CA firewall. Application control capabilities from Bit9 come at an additional cost.

- BigFix doesn't provide an agentless version of its technology. The BigFix agent requires administrative privileges to install; however, some customers have deployed BigFix as a lightweight agent with automatic cleanup as a way to remediate noncompliant machines.

- Customers report that the BigFix console is weak on security-specific reporting capabilities, and that it's difficult for them to get the reporting and statistics they need. A security-specific dashboard and console view to address this difficulty is expected by 2H09 in Decision Support System (DSS), which is BigFix's Web services reporting framework.

CA

CA is a long-term player in the enterprise IT management market with large global support operations that provide follow-the-sun support. In this analysis, CA moved down in its ability to execute due to slow market responsiveness, declining market share, low visibility and tepid customer enthusiasm in 2008. However, we see tentative signs of improvement for 2010 due to CA's renewed focus and aggressive feature road map, as well as the rate of product improvements that are being delivered by the HCL Technologies partnership. CA customers and global organizations seeking uncomplicated, inexpensive EPP capabilities should consider CA Threat Manager.

Strengths

- In 2008, CA partnered with HCL Technologies to take over product development, engineering, support and threat research. This has paid off by delivering much-faster and more-ambitious product features than CA was able to deliver natively, and the next version of the product, r8, which is expected in 1Q10, promises continuing improvements.

- CA Threat Manager Total Defense solution is on par in terms of the basic functional specifications for the EPP (anti-malware, HIPS and a personal firewall).

- CA consolidated its two virus detection engines into a single engine in 2008.

- Servers and clients are certified to run in VMware and Citrix client sessions.

- The CA firewall can enforce policies by network context, and 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 behavior anomaly detection. Its learning mode capability eases setup and policy creation. CA also maintains a very comprehensive "known good" application database for broad, industrywide whitelisting.

- CA 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.
- Very broad platform support, including several varieties of Unix/Linux, Mac, Palm, Windows Mobile, VMware, Citrix presentation servers, and specialized servers such as Exchange, Notes/Domino, NetWare, and NetApp and EMC storage.
- CA offers very attractive subscription prices.
- CA is finally recognizing the value of its IT client manager, and fulfilling its promise to deliver operations and security integration. CA plans to begin integrating PCLCM functionality into the EPP suite in late 2009.
- CA acquired an enterprise DLP solution in 2008.

Cautions

- Despite rapid improvements by HCL, CA still lacks the advanced management capabilities of leaders. Management interfaces are very detailed, but they have a ponderous look and feel that could diminish administrator productivity. Threat Manager and HIPS aren't under a single console with a common policy engine, or even a common look and feel. Reporting is distinct across both, so it's difficult to get a unified view on the security status. The reports are text/table-based, lacking easy-to-read graphs, and there's no custom reporting or scheduling capabilities. Reports are static, and there are no hot links to drill down into more detail. Role-based administration isn't granular (read or read/write only) for a large enterprise. Improvements in reporting are expected in r12, which is due out in 1Q10.
- Policy is difficult to audit once it's created. There's no summary view, and policy reviewing requires administrators to repeat the policy development process.
- The client interface isn't integrated. There's a different one for the firewall and for antivirus/anti-spyware, and options for delegating control to users is very binary.
- Firewall policy improvements are needed to control VPN tunnel sessions, and to limit the mixing of network interfaces — particularly wireless LAN.
- CA lacks the ability to enforce encryption on data written to external storage devices.
- The intrusion prevention system (IPS) is generally good, but lacks rootkit detection (which is due in 3Q09).
- NAC is limited. CA isn't a strategic NAC vendor.
- Orchestria DLP is still a separate product. It was acquired to be integrated with CA's IAM offerings in the short term, with integration planned for CA's governance products along with its security information and event management offering next.
- CA lacks integrated full-disk/file encryption products.

Check Point Software Technologies

Well-known in the enterprise network firewall and VPN market, Check Point is slowly accumulating the component pieces of an EPP suite, and is gradually building on its acquired installed base. In 2009, Check Point moved slightly down in execution due to slow growth, despite its laudable enterprise presence, brand and channel. The company moved slightly right in vision due to better integration of data protection measures. Visionary movement was tempered slightly as a result of the lack of native malware detection engines and still-maturing management capabilities. Organizations that value strong integration among remote access and the EPP suite, full-disk and media encryption, and application whitelisting solutions should include Check Point on their shortlists.

Strengths

- Check Point Endpoint Security suite includes personal firewall, antivirus/anti-spyware (licensed from Kaspersky), full-disk encryption, NAC and integrated VPN in a single client deployment.
- The management console is Web-browser-based and offers basic status reporting on endpoint status, including compliance status based on custom parameters such as third-party anti-malware engines.
- The personal firewall is very complete and includes extensive prepopulation program profiles, excellent location-based policies, and the best VPN client integration.
- Check Point has some basic HIPS techniques in the firewall and as part of the Kaspersky engine.
- Program Advisor service is a valuable asset for administrators to enable whitelisting 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 VPN products, and 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).

- Successful OEM with SanDisk Cruzer Enterprise shows the valuable ability of Check Point's endpoint security to adapt to portable usage scenarios.

- Check Point will soon be adding browser virtualization technology to protect against malware that targets browsers. The technology was developed internally for the consumer product ZoneAlarm ForceField, and will soon be part of the single enterprise client.

Cautions

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

- Check Point conducts its own spyware analysis and publishes its own anti-spyware, but it's dependent on Kaspersky for antivirus signatures, to review suspicious code samples and to prepare custom signatures for targeted viruses. Although we agree that signatures are becoming a replaceable commodity, business disruptions in Kaspersky could impact Check Point customers.

- Centralized management is still maturing and not all products are fully integrated yet — for example, full-disk encryption and Media Encryption and port protection each have their own management console, and agents are still separate.

- The Check Point management console is weak for enterprise needs. It only supports manual standby for management server clusters. There's no native discovery of rogue endpoints. Although the product has a multisourcing service integrator (MSI) file builder, it depends on software distribution tools to push clients to endpoints, and lacks the ability to remove other antivirus products. The solution doesn't include many options to minimize the impact of scheduled scans, such as CPU use, or to avoid conflicts with critical programs.

- Native reporting capability is weak. There are no scheduled or custom reports available in the management console. Administrators looking for this function will have to use the Check Point Eventia Reporter, which is a global event reporter for all Check Point products and comes at a substantial additional cost (for example, $2,000 to $5,000).

- 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.

- A "smart defense" 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 the firewall.

- Check Point's data protection strategy is still missing content-aware data leak prevention.

- Check Point is limited to Windows endpoint PCs. It's been slow to deliver Vista and 64-bit support in the enterprise product, and doesn't offer protection for specialized servers, such as Exchange or SharePoint.

eEye Digital Security

eEye focuses on ease of administration, advanced malware research and innovation in malware/intrusion prevention. eEye moved up to reflect a market share growth relative to its peers. The company also moved right to reflect good malware detection and malware research, as well as improvements in price, which are now more reflective of market conditions. Consider eEye Blink if you're an SMB seeking a tactical HIPS solution to supplement signature-based protection and native firewalls on Windows clients and servers.

Strengths

- The management and development teams represent a diverse set of talents and include some key personnel from other companies in the EPP market.

- All functions are packaged in a single agent. Layers of function are easily enabled or disabled by the administrator without making changes to the installed image or drivers.

- The graphical user interface (GUI) console greatly simplifies the process of associating tasks, functions and datasets so that working with large numbers of managed systems is relatively easy for a novice administrator.

- Security policies can be monitored and updated from outside the firewall, and these actions don't require a VPN. Change management details are held in XML files for revision monitoring and control. The actual installed footprint that's stored and in RAM is relatively small.

- eEye is the only company in this Magic Quadrant to offer a service-level agreement (48 hours) on critical issues.

- eEye has a well-organized, third-party management integration document and process.

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

- Antivirus performance is enhanced by never rescanning files that were previously marked "good."

- eEye also offers an excellent vulnerability management solution called Retina Network Security Scanner, which can aggregate results for regulatory compliance to a central management console (REM Security Management Console).

Cautions

- Despite rapid growth, eEye is still one of the smallest companies in this market, and has a limited presence outside North America or in organizations with more than 500 employees. Its total staff size, including research and engineering groups, is small compared with the EPP industry average. eEye seems adept at doing more with less, but this could be a limiting factor if it tries to compete on a global scale.

- Although eEye develops its own spyware signature database and cleanup routines, the solution relies on Norman ASA for antivirus signatures. Although we agree that signatures are becoming a replaceable commodity, business disruptions in Norman could impact eEye customers.

- eEye has limited application and device control capabilities, but no encryption or DLP capabilities.

- eEye lacks the capability to detect installed rootkits, although it has techniques to prevent rootkit installation.

- Only Windows OS platforms are supported, so companies with other devices need to buy other or additional EPP platforms.

- Client protection is limited to new-generation Windows endpoints only, with plenty of resources to run real-time evaluations and quarantine IPS techniques. References commented that the product can be resource-intensive on legacy endpoint systems, although the storage and RAM footprints look relatively low — probably because they rely on pre-execution in quarantine.

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

- eEye doesn't offer an on-demand scan engine.

- Blink 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.

Eset

From its Slovakia headquarters, Eset has built a substantial installed base in EMEA, and also has an emerging presence in North America and Asia/Pacific. Eset is new to the Niche Players quadrant and has good overall execution, as illustrated by its market share, rapid growth and enterprise interest. Its vision score benefited from good HIPS and signature accuracy, but lost ground due to ineffective management capabilities and lack of investments in market-leading features. Eset is a good shortlist option for SMBs seeking very effective, uncomplicated anti-malware scan engines and personal firewalls.

Strengths

- The flagship enterprise product, Eset Smart Security, includes integrated antivirus, anti-spyware, anti-spam and personal firewall in a single-agent footprint. The low performance impact of the Eset product has been noted by many customers.

- 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 left-click to push agent or other remediation activities.

- The Eset anti-malware engine is a consistently respectable performer in test results (that is, VB100 and antivirus comparatives) 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.

- In 2008, Eset expanded rootkit detection, reduced the update footprint, improved active directory integration and considerably improved cleaning capabilities.

- More recently, Eset launched rudimentary device control, which enables blocking and/or immediate scanning of removable media.

- Eset supports a broad range of Windows clients and servers, including Exchange and Windows Mobile, as well as Lotus/Domino, Linux Direct Stream Digital and Solaris servers, and Novell NetWare and Dell storage servers.

- To reduce the impact of scanning, Eset recently introduced more control over the depth, size, and time of scanning archives as well as Eset Smart Security, which automatically determines which files need deeper scanning.

Cautions

- Eset is lacking in management features for larger, more-complex organizations.

- The management console is due for a refresh; it's very complex and lacks a clear, actionable dashboard view to enable more rapid/automated problem identification and remediation. It also lacks many common enterprise capabilities, such as role-based administration, custom reports (although the 18 default reports can be modified), report hyperlinks to detailed log information,

policy elements that can be delegated (or restricted) to end users, automatic location-based policies — especially enforcing and monitoring policies for off-LAN clients, automatic rogue machine detection and advanced NAC features.

- Clients can be distributed by the management console; however, installation will fail if there's a competitive solution. 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 fine-tuned to accommodate false positives.
- Some customers with numerous custom applications cautioned that Eset can have a high false-positive rate, and is tardy in delivering full compatibility with the latest versions of Microsoft Office file formats.
- Some customers cautioned that Eset support was difficult to reach.
- Eset doesn't yet offer many of the additional EPP components, such as application control/whitelisting, advanced port/device control, and encryption, DLP or VPN integration.
- Eset doesn't have an anti-malware engine for Mac.

F-Secure

F-Secure is a longtime player in the European Union's (EU's) EPP market, and has a number of product innovations. F-Secure's position in this Magic Quadrant moved to the Niche Players quadrant as a result of the lack of emphasis on advanced management features and data protection. However, it's a good, alternative anti-malware tool for SMBs, especially those in F-Secure's direct service area of Northern Europe, and those looking for SaaS-type services.

Strengths

- F-Secure's malware research lab is well-established and provides fast response times to outbreaks because of automated threat analysis and multiple sources of threat samples.
- The vendor has the largest share of Internet service provider customers, including a SaaS multitenant platform, F-Secure Protection Service for Business, which enables resellers and partners to offer SMBs a fully managed security solution.
- F-Secure added two new capabilities to reduce the lag between threat detection and signature distribution. The first is a network query capability called DeepGuard 2.0, which allows clients to request file reputation information from a network database with the most-recent signature information. The second is a peer-to-peer signature database with update capabilities.
- The vendor's HIPS capabilities include sandboxing, which enables applications to run, but stops this if they exhibit suspicious behavior. Suspicious application behavior can be subjected to user query, and the decision is enforced as a rule for a given application every time it runs. Applications that are classified as clean (that is, whitelisted) can avoid this step by reducing latency.
- F-Secure has a dynamic client update mechanism that allows for frequent (that is, 60-day) protection capability updates.
- Customers comment on the outstanding support from F-Secure.
- F-Secure BackLight provides a good rootkit scanning capability.
- The personal firewall component, F-Secure Client Security — Internet Shield, uses Vista's Windows Filtering Platform.
- Client Security supports Windows, Linux, Windows Mobile, Symbian and Citrix servers.
- F-Secure supports 20 languages.

Cautions

- F-Secure has limited direct presence in the enterprise market, resulting in less-advanced enterprise management features (such as distributed management console, role-based administration and automated network scanning for agentless machines), which makes it challenging to use this product in large environments.
- Market presence is mostly in EMEA, with limited presence in North America and Asia/Pacific.
- The HIPS solution is missing some basic capabilities, such as buffer overflow, vulnerability shielding or malicious Web site blocking, but these are in the consumer product and on the road map for the enterprise version in 2Q10.
- F-Secure only offers a Web-based, on-demand scanner. It doesn't have an enterprise version that's suitable for scanning unmanaged machines.
- The vendor's personal firewall lacks some of the advanced features of its rivals, such as device control and expansive logs.
- Advanced data protection, such as DLP and encryption, aren't on F-Secure's road map. Its exit from the encryption market several years ago didn't demonstrate good vision.
- NAC is limited to agent self-enforcement for signature file freshness and client presence.

- F-Secure needs to enhance its quality control and alpha testing on new product version releases.
- F-Secure scan engine is notably slow on recent AV-Comparatives.org tests.
- There are no Mac, Unix, Notes or SharePoint solutions.

IBM

In 2009, the strength of the IBM brand and channel helped expand the Internet Security Systems (ISS) customer base, mostly with smaller customers. Although the Proventia client base is still skewed slightly toward the North American market, a healthy percentage of its customers are in Asia/Pacific and EMEA. In 2009, IBM declined in execution due to minimal product feature development, and improvements in market share were disproportionately low given the strength of the IBM brand and channel. Organizations that have a close relationship with IBM, and those seeking advanced HIPS capabilities or a managed security service, should include IBM on their shortlists.

Strengths

- IBM's X-Force malware research labs have a strong reputation and are a valuable differentiator for Proventia, which is essentially a delivery vehicle for X-Force analysis and advice.
- Proventia's main strengths are its strong HIPS protection and its full-featured personal firewall capabilities. Proventia Desktop's signature-based antivirus and anti-spyware engine is licensed from BitDefender.
- The underlying detection and blocking engine in the HIPS solution identifies and analyzes more than 198 network and application layer protocols and associated data formats. The X-Force security team produces vulnerability shielding signatures. It also uses pre-execution malicious behavior detection and shellcode detection.
- In 1Q09, IBM announced IBM Proventia Endpoint Secure Control (ESC), which combines the Proventia HIPS and firewall with BigFix management capabilities and PCLCM tools, such as Patch Management, vulnerability and configuration management, and also resells the Trend Micro anti-malware engine.
- In 2008, IBM licensed PGP for desktop encryption and port/device control, and Verdasys for endpoint data leak prevention, and these products will be integrated into ESC.
- The ISS SiteProtector management console can be used to manage multiple ISS products and consolidate high-level security information.
- IBM's Global Technology 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.

Cautions

- With ESC, IBM is taking a framework approach to build the EPP suite. IBM only owns the Proventia desktop HIPS and firewall; all other components will be licensed and added via integration with the BigFix management console. Although this has the advantage of more agility in selecting components, it's unlikely to offer the tight integration and price of single vendor suites.
- IBM won't sell or support BigFix's Software Asset Management and License Management, OS Deployment/Software Distribution or Remote Control Modules, and will instead direct customers to Tivoli for these capabilities.
- As a result of the BigFix license agreement, IBM's Global Technology Services group will effectively be competing against components of Tivoli for PC and server patch, configuration, and vulnerability management. IBM must better articulate how it will resolve this tension, and provide a clear road map for integrating these two operations platforms in organizations that end up with both.
- Although it's growing, the Proventia installed base is tiny compared with the market leaders' installed bases. Even in its installed base, Proventia isn't always exclusive, and is often just deployed tactically in high-security domains.
- Proventia management (without ESC/BigFix) is still lacking advanced enterprise features, such as the ability to distribute signatures, and advanced reporting and monitoring.
- So far, integration with PGP and Verdasys is limited to reselling and to first-tier and second-tier support.
- IBM's signature-based anti-malware capabilities are dependent on BitDefender and, now, Trend Micro.
- HIPS technologies are generally harder to tune due to potential false-positives, and Proventia can require more administration overhead when setting up.
- SiteProtector is used to manage endpoint and network-based IBM/ISS offerings; however, in most organizations, these are two separate groups, which minimizes much of the value of a converged console.

- IBM NAC functionality is very limited and isn't a strategic NAC solution.

- There is no support for Exchange, Notes, SharePoint or other specialized servers, or for mobile devices.

Kaspersky Lab

Kaspersky is rapidly leveraging its Eastern European base and increasing brand awareness in enterprise opportunities in North America and Asia/Pacific. In 2009, Kaspersky moved up in execution to reflect its expanding channel and increased enterprise interest, which have resulted in very healthy sales growth in 2008, tempered by delays in the release of version 8. The vision score was impacted by the increasing weight in our analysis on a data security strategy and/or a PCLCM integration story. SMBs that prefer to focus on core anti-malware defenses should evaluate Kaspersky. Larger organizations should consider Kaspersky as a strong antivirus 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.

- Kaspersky has a relatively small disk and memory footprint for a comprehensive suite platform.

- Kaspersky offers advanced HIPS features, including an isolated virtual environment for behavior detection, as well as application and Windows registry integrity control.

- 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.

- The company also offers a new vulnerability scanner based on Secunia, which helps users identify vulnerable applications and find solutions.

- Kaspersky offers broad platform support, including Windows Server 2008, Citrix, Linux, Novell NetWare, Exchange, Notes, Windows Mobile and Symbian.

Cautions

- Kaspersky is undergoing significant growth in the enterprise market and is aggressively expanding into new geographies, and it must invest in support and enterprise-class features well ahead of demand.

- The latest v.8 products boast a number of new features, but have been delayed due to quality issues and are now targeted for a 3Q09 general release. Also, Kaspersky recently scrambled to fix a bug in the latest update of v.6.0, which caused some concerns about Kaspersky's code quality process.

- Kaspersky still needs to improve its manageability for large enterprises — for example, providing more task-based workflow, supporting multiple application development trees, providing a unified view of endpoint security status, improving reporting functionality, increasing support for more-flexible group-level policies, and improving native client distribution capabilities. Some of these issues are expected to be addressed in the delayed v.8.

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

- Device control capability isn't very granular, is limited to device groups and can only block or allow certain ports.

- Kaspersky doesn't offer any endpoint encryption capability or DLP. A Kaspersky sister company is developing a DLP and encryption solutions; however, integration and functionality road maps are still undefined.

- Native NAC capability is missing.

- There is no Mac or SharePoint support.

LANDesk

LANDesk, an Avocent company, is an established leader in the PCLCM market. LANDesk benefited in this Magic Quadrant from our increased weight on management and PCLCM integration, thus moving it to the right. The company's movement in execution was weighted down by its higher pricing in a tighter economic cycle. LANDesk is an excellent choice for organizations seeking very robust management of endpoints, integration of PCLCM capabilities, and the ability to manage endpoint security technologies from multiple vendors.

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 reporting framework. Likewise, the LANDesk agent has a single, modular architecture so that security functionality (like antivirus) may be activated as needed. Customer feedback on the LANDesk console says that it's a very powerful

tool for administrators that have operational and security responsibilities. Customers like the ease with which it can find, assess and update any aspect of a PC, even when it's off a LAN.

- The base LANDesk Security Suite includes an anti-spyware signature engine (Lavasoft), patch management, vulnerability management, HIPS, device control compliance, standard scanning and remediation, USB encryption, application blacklisting/whitelisting, and limited NAC capabilities. Customers may use LANDesk to manage McAfee, Symantec, Sophos, CA and Trend Micro, or they may choose to pay for LANDesk AV, which is built around the Kaspersky virus scan engine.

- LANDesk HIPS technology (acquired from ViGuard in January 2007) is one of the most-comprehensive of all EPP vendors evaluated, and is now included as part of the Security Suite. Capabilities including buffer overflow protection, application whitelisting/blacklisting, as well as 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 control over USB and other removable media, including its own 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, and allows for updating malware definitions, engines and EPP.

- LANDesk offers very broad endpoint platform support, including Windows 98, Windows NT, Windows 2000, Windows XP, Windows Vista, Windows Server 2003, Windows Server 2008, Mac OS X, Red Hat Linux, SUSE Linux, HP-UX, AIX and Sun Solaris.

Cautions

- LANDesk's list pricing is expensive. Buyers should always leverage the competitive bidding process to get the best price.

- LANDesk Security Suite includes patch management, which can have internal political ramifications between operations and security groups.

- 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 viruses. Although we agree that signatures are becoming a replaceable commodity, business disruptions to this important partner could have an impact on customers. However, this is offset by LANDesk's ability to readily manage other solutions.

- LANDesk doesn't yet provide a firewall of its own, and instead manages the Windows XP and Vista firewalls. It's planning on adding its own, more-capable firewall with location-aware policies in late 2009.

- Not all LANDesk Security Suite features are available on all platforms it supports for PC management. For example, LANDesk HIPS and the LANDesk AV add-on only support the Windows platform, and aren't supported for Linux or Mac endpoints, although the Mac solution should be available by 2010. There's no malware support for SharePoint, Notes or Mobile clients. Exchange support will be available in 4Q09.

- LANDesk should expand its application control capabilities for whitelist automation and exception management to close the gap with competitive application control.

- In addition to its own offering, LANDesk should integrate with Microsoft Network Access Protection (NAP).

- LANDesk doesn't offer DLP or full drive encryption, and won't release a file/folder encryption solution until 2H09.

- Customer feedback indicates that the LANDesk console is designed from an operational perspective, and that dedicated security professionals may have difficultly getting the security-specific views and reports they want.

McAfee

McAfee has the second-largest market share in the traditional antivirus market. The company has significant marketing resources, a solid operations capability, and a strong malware research and management team. McAfee continues to be a leader based primarily on long-term leadership in cross-product management functionality, as well as an early focus on data protection. McAfee is a strong strategic vendor that's suitable for any enterprise.

Strengths

- The company's vision is to become a more-strategic vendor by building out a suite of security products under common management that can provide correlated protection as well as better visibility into the enterprise's security posture.

- The recently revised ePO, which is the top-level manager for most of McAfee's products, is a Web-based management console and includes many advanced options, such as configurable dashboards, actionable reports and fully active directory integration. ePO also has new application

programming interfaces to accelerate the integration of acquired products and partners. McAfee also offers a SaaS-based management console for SMBs that eliminates the need for an ePO server on-premises.

- The antivirus and anti-spyware database has been combined into a single anti-malware database. In 2008, McAfee launched "Artemis," a cloud-based service that enables clients to check the latest signature data to identify brand-new threats.
- McAfee recently launched a product that supports offline virtual image scanning for VMware partitions and other virtualization platforms.
- HIPS is a strong feature of the McAfee suite and has an expanding assortment of techniques to detect unknown malware.
- McAfee offers significant data protection tools, including full-disk and file/folder encryption, encrypted USB storage devices, device control, and endpoint and enterprise DLP solutions.
- The NAC solution is improved with McAfee network IPS appliance enforcement, which allows NAC for unmanaged devices to be managed by ePO.
- Policy Auditor, Vulnerability Manager and Remediation Manager are finally adding integrated value in ePO v.4 by providing more-complete information on the security status of PCs.
- McAfee offers a very broad range of supported platforms, including EMC file servers, Windows Mobile, Linux, Solaris and Mac platforms.

Cautions

- McAfee has accelerated the integration rate of its various acquired products with ePO v.4; however, there are still variations in the level and stages of integration. Buyers need to understand the level of integration and press McAfee for details on integration milestones.
- Some acquired features aren't rationalized into more-appropriate technologies. For example, port and device control are features of the DLP solution, not the firewall.
- Without HIPS, McAfee's malware detection effectiveness hasn't been as good as some of its peers and some of the smaller vendors in this market. However, recent tests show improvement with the implementation of Artemis.
- HIPS is still difficult to granularly disable rules (that is, per application) to address false positives, and can be noisy — partly due to uncorrelated alarms.
- McAfee's list prices are generally higher, relative to its peers, for similar functionality, and sales are often very aggressive. Effective negotiations with McAfee must involve early competitive bidding.
- NAC for unmanaged endpoints requires the NAC appliance or NAC add-on module to the Network Security Platform (IPS). NAC for managed endpoints requires the McAfee NAC endpoint agent, which can be purchased separately (and it's included in the Total Protection for Endpoint advanced suite). The IPS appliances are very expensive for shops with fewer than 5,000 users, and there are no out-of-band or software options.
- With the new Web-based ePO 4.0, it's sometimes harder to see complete lists of log or report events, due to limitations in the number of rows per Web page.
- Policy Auditor, Vulnerability Manager and Remediation Manager aren't included in all EPP suites, and they aren't integrated with any software distribution or patch management tools to ease remediation.
- McAfee's acquisition of Secure Competing will likely cause some management distraction, product development challenges, and channel confusion as it attempts to become the first security vendor to compete effectively in the endpoint and network security markets.

Microsoft

Microsoft is a relative newcomer to endpoint security, given that Forefront Client Security (FCS) was only introduced in 2007, but the company has used its significant resources to establish a credible lab presence to gain wide visibility into malware from FCS, Windows Live OneCare, Windows Defender, the Microsoft Malicious Software Removal Tool, as well as malware submitted by the opt-in SpyNet community.

In 2009, Microsoft moved down in execution because it hasn't had much success penetrating the enterprise market outside very budget-conscious organizations. The company lost some vision points because it has yet to improve management or add advanced features, and the malware detection accuracy is lagging behind its peers. FCS should be considered only by Microsoft-centric organizations that are seeking basic, signature-based anti-malware capabilities, primarily for desktop PCs and Windows servers at a competitive price. For organizations that subscribe to Microsoft's Enterprise Client Access License (ECAL) program and are renewing antivirus contracts in 2009, FCS offers an immediate opportunity to reduce costs. Forefront for Exchange and SharePoint remains an excellent choice due to its signature engine diversity and compatibility with these platforms.

Strengths

- Microsoft's FCS console is a native Windows application built on top of an embedded Microsoft System Center Operations Manager, which provides alerting and logging capabilities, and management of FCS endpoints. Clients have favorably rated its ease of use and reporting capabilities. Signatures and engine updates are distributed using Microsoft Software Update Services, leveraging infrastructure and knowledge that many enterprises are already using.

- Most organizations already have infrastructural Microsoft software components installed (for example, Active Directory and System Center). Microsoft will use integration to upsell its security products.

- 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 way to reduce costs in 2009 and 2010.

- FCS is part of a Forefront family that includes products addressing endpoint security, server platforms (such as Exchange and SharePoint) and the network edge (for example, Intelligent Application Gateway and a future unified threat management software solution). Management consoles across these three lines will be integrated in the next major release, which is due around 1Q10.

- 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 FCS anti-malware engine to generically decrypt malware that has tried to scramble the engine's contents. Test results (that is, AV-Comparatives.org) show low false-positives.

- Rather than duplicate functionality provided in the Windows OS and other platforms, FCS focuses on the anti-malware engine, and, in the longer term, will manage OS features like the Windows firewall and DLP capabilities that are currently licensed from RSA.

- Forefront for Exchange and for SharePoint benefits from tight integration with these platforms and with multiple scan engines.

- FCS doesn't include a 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 FCS and non-FCS settings (like the Windows Firewall).

Cautions

- 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.

- Despite significant improvements to Microsoft's signature detection engine, it still suffers from inconsistent detection scores and slow scanning speeds in AV-Comparatives.org tests.

- Microsoft first released FCS in 2007, and there have been only minor updates since then. We believe the next major release won't be delivered until 1H10. 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, data execution prevention options, User Account Control options or BitLocker encryption.

- FCS lacks HIPS capabilities. However, these are planned for delivery in the next major release of FCS.

- Microsoft has no agentless version of FCS for scanning unmanaged machines.

- 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), but lacks advanced firewall features, such as a location sensing policy. The firewall is owned and managed by the Windows OS team.

- Removable device control comes from Microsoft's Windows OS group and is only available with Windows Vista (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 console, although this is planned for the next major release of FCS.

- Although the FCS console uses an integrated Microsoft Operations Manager (MOM) console, there's no current synergy for organizations using Windows System Center. There's a significant, longer-term opportunity for integration with System Center. However, this isn't planned for the next major release of FCS. In this market, as with other management and security areas, Microsoft puts buyers in the position of managing multiple point solutions.

- Scalability beyond 10K nodes 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 threat protection, because of the potential for a conflict of interest.

- Microsoft is continuously challenged to choose between embedding security into Windows, which benefits all customers, or providing competitive security products. Ownership of security technologies is split between the Microsoft Windows business unit, which owns the firewall and the majority of HIPS techniques, and the Identity and Security Division, which owns FCS. These groups are managed separately and have independent goals and revenue targets.

Panda Security

Panda Security is gradually expanding from its EMEA presence, radiating outward from its Spanish base. Panda's vision score was impacted by the increasing weight in our analysis on a data security strategy and/or PCLCM integration story. However, Panda rose in execution to reflect continuing strength in its EU installed base, which moved it into the Challengers quadrant. SMBs seeking a more customer-intimate alternative should consider Panda as a good shortlist entry. In particular, we like the malware radar as a technique to audit incumbent performance and test Panda's effectiveness.

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 PDF format.

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

- Panda offers very good rootkit inspection that reads raw data from the hard drive to look for hidden processes.

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

- 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 can modify rules or create their own rules to override Panda's rules.

- 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.

- Malware Radar is Panda's free, agentless, network crawling malware and vulnerability audit tool, which uses a cloud database look-up to detect new threats. It can be a good utility for double-checking incumbent antivirus accuracy. Malware Radar is managed in its own management dashboard, and uses a different scanning engine with more-advanced detection techniques than the regular Panda product.

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

- Panda offers a SaaS-hosted management server called Panda Managed Office Protection (PMOP) with a Web-based management console.

Cautions

- Despite Panda's globalization plans, the installed base is still mostly EMEA SMBs. Panda lacks brand recognition in North America or Asia/Pacific.

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

- Panda's HIPS policy doesn't provide a monitor-only mode to enable testing and tuning before deployment. TruPrevent only identifies files 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 (CPU load limitation) to minimize the impact of scheduled scanning, although end users can delay scanning if they're authorized.

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

- The only NAC option is limited to self-contained NAC, and Panda doesn't offer guest NAC.

- Malware Radar is a separate tool that isn't managed from the Panda management interface. Output is a very short executive summary or a very long technical report. It isn't really designed to run continuously and can take too much time to complete on a large production network (and PCs must remain "on" to be scanned). Malware Radar is primarily used as a sales tool.

- Panda doesn't support Mac clients or any mobile clients, and some clients have complained about stability on Windows servers. Panda doesn't support SharePoint.

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

Prevx

Prevx is an innovative provider of anti-malware solutions. Based in the U.K., Prevx has pioneered the use of community visibility — what it refers to as "herd intelligence" — of software as a factor in determining whether a given program is malicious. Prevx is new to the Magic Quadrant and falls into the Niche Players quadrant, primarily due to its small corporate size and small market share of customers, most of which have limited deployments in specific domains alongside (as opposed to replacing) traditional signature-based malware detection. Management features for large enterprise are maturing. Organizations should consider Prevx if they're seeking an additional and unorthodox layer in their defense-in-depth strategies for protecting sensitive endpoints. Organizations conducting business with Internet-based consumers, and seeking innovative, lightweight and downloadable protection, should consider Prevx eCommerce Secure Access Checker (eSAC).

Strengths

- The core of Prevx technology is signature-based (whitelist and blacklist), but with a unique approach. In addition to conventional application signatures, Prevx also uses signatures of what an application does as it executes to determine whether the software is malicious.

- The herd approach is effective at pinpointing targeted attacks by recognizing new or low-frequency usage applications. Prevx Edge enables customers to set policies that query or block applications that are less than x minutes old, or have been seen by fewer than x users in the customer environment or the Prevx customer community.

- Prevx provides a number of malware detection, remediation and real-time protection solutions, all of which share a common protection engine and download structure. All Prevx EPP products can be managed using the Web-based console, or the Prevx CSI Enterprise dedicated management console.

- The lightweight Prevx 3.0 Banking and eCommerce Security enables any banking, brokerage or e-commerce Web site to protect its customers by checking a client PC for active malware and rootkit infections prior to logon, and before their credentials are exposed, thereby preventing fraud and identity theft.

- Prevx 2.0 provides a number of HIPS capabilities, including a facility to upload suspect code to be tested in a centralized sandbox environment and verified before execution. In addition, Prevx 2.0 incorporates generic heap-and-stack buffer overflow detection; however, this isn't yet available in Prevx CSI and Edge-based products.

- Prevx endpoint protection products provide application control. Applications can be blocked or allowed based on signature, metadata, digital certificate, name, source path, reference image, vendor, registry entry, behavior or any combination thereof.

- Although Prevx could replace antivirus, it positions its offerings to operate alongside other leading security products to improve malware defense by leveraging two malware detection capabilities in tandem.

Cautions

- Prevx is privately funded and is one of the smallest vendors in this analysis. It has very limited brand-name recognition. Most Prevx revenue comes from U.S. and U.K. enterprise customers, with the majority of its enterprise business concentrated in smaller organizations with fewer than 500 seats.

- Prevx's advanced management capability for large enterprises is still maturing.

- Prevx provides limited signature-based detection of malware. We find that many organizations are unwilling to give up antivirus and want the sense of comfort provided by a traditional antivirus scanning solution. Adding more vendors complicates administration and increases costs.

- The large family of Prevx solutions is confusing and Windows-client-centric. None of the Prevx offerings provide support for Linux, Unix or Mac, or mobile clients. Only Prevx CSI, Edge and eSAC support 32-bit and 64-bit versions of Windows.

- None of the Prevx family of solutions provide a traditional host firewall, although the Prevx console will report on the status of the Windows XP and Vista firewall.

- Prevx provides no DLP or encryption solutions.

- Prevx doesn't provide a NAC client or NAC integration.

- Customers report issues with the Prevx technology because it often flags legitimate applications as potentially malicious.

SkyRecon Systems

A new vendor on this Magic Quadrant, SkyRecon Systems was started in 2003 and is based in France. In its rookie year, the company just made it into the Visionaries quadrant due to its focus on an extensible platform that encompasses malware and data protection. SkyRecon's execution score is hampered by its relatively small market share and geographic presence, lack of a native malware detection engine, and its still-maturing management capabilities. SkyRecon is a reasonable shortlist vendor for organizations in supported geographies seeking more-aggressive malware detection solutions and willing to invest in administration.

Strengths

- The company's flagship product, StormShield Security Suite, is designed to address system and data protection via an extensible EPP that integrates multiple layers of security.
- StormShield provides HIPS, a personal firewall, Device Control System (DCS), encryption and an optional, signature-based, anti-malware engine licensed from Panda Security.
- 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.
- The firewall provides good Wi-Fi policy options, as well as options to forced 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.
- StormShield provides client-side NAC.

Cautions

- Although it's growing rapidly, SkyRecon is still one of the smaller vendors in this analysis. It has a limited enterprise client base and lacks brand recognition outside France.
- SkyRecon has a very small malware research team and is dependent on Panda Security for signature-based protections. The Panda malware engine is a separate agent. SkyRecon is still maturing its management capabilities, and customers have commented on a higher-than-necessary level of complexity, reporting various challenges, lack of policy inheritance options, high false-positives and tuning challenges.
- The FDE capability is brand new and not widely field-tested.
- DCS file encryption can be challenging to manage due to reported application conflicts and immature integration.
- StormShield is limited to only Windows 2000, XP and Vista endpoints. It doesn't have solutions for servers such as Exchange and SharePoint.

Sophos

Sophos is a veteran anti-malware company that's dedicated to the enterprise market. More-ambitious management has resulted in excellent growth and geographic expansion from its European base to the North American market. Sophos' vision score benefited slightly due to the acquisition of Utimaco Safeware's data and port protection. The Sophos EPP suite offers a good balance of malware, personal firewall, HIPS defenses, and integrated data protection capabilities that are deterministic and easy to deploy and manage. Buyers that prefer a broad, comprehensive EPP suite with simplified management capabilities — and are willing to consider smaller, more-intimate providers — should consider Sophos.

Strengths

- Sophos continues to have a strong reputation for support and service from customers and the channel.
- The management interface achieves a good balance of simplicity without sacrificing depth of control. In particular, the dashboard is complete with actionable information upfront, with right-click remediation options via integration with third-party patch management tools. Sophos provides single-console management of Windows, Mac, and Linux and Unix clients, including Itanium.
- Vulnerability and patch assessment information is available with Sophos NAC Advanced, which provides excellent client security status information.
- Malware detection improved in 2009 with the addition of rootkit protection for Windows endpoints, and with Web-based malicious attack detection, which blocks malicious script in Internet Explorer.
- The company improved its data protection capability in 2008 by acquiring Utimaco and its SafeGuard Enterprise Encryption product, which adds disk and file encryption, rudimentary data leakage prevention, and device control to the suite. Sophos is busy integrating this capability into the management console and deployment packages.
- Sophos provides application control that enables administrators to define and update a whitelist of authorized applications, and enables 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.

Cautions

- Sophos' market share in large enterprises remains small relative to other leaders in the quadrant, and it's experiencing increasing competition in the SMB market. Sophos is continuously challenged to differentiate itself from the "big three" players in the Leaders quadrant. Lack of consumer products has resulted in low brand recognition. The majority of Sophos' client base is small enterprises with fewer than 500 seats. Work is needed to expand its reach into midsize and large enterprises, although recently, very large (that is, 100,000 seats) customer wins have demonstrated Sophos' scalability and appeal to large enterprises.
- 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.
- Large enterprise management features (such as advanced role-based administration, audit controls and compliance reporting) are lacking in the current product, but are planned for 2009.
- The integration of Utimaco is incomplete and will continue to consume a large amount of corporate and development resources in 2009.
- Advanced firewall policies, such as location awareness and VPN, and the Wi-Fi policy could be improved. Sophos is planning on adding a simple, location-aware policy based on automatic detection of location for v.9, which is expected for general availability in 2H09.
- The Utimaco DLP solution is still immature and not widely field-tested. Advanced capabilities (such as a prepackaged policy) are lacking, but expected in 2Q09.
- Sophos' agent is quite large, and some customers have complained about the high frequency of new client versions that must be rolled out before v.7.6.6, which added low delta version updates in 1Q09.
- Because it's designed for the enterprise market only, Sophos may suffer higher false-positive rates with consumer applications.
- Native-developed operations management tools, such as configuration and vulnerability management, are still immature, especially compared with the vendors that acquired or partnered with dedicated PCLCM vendors. Sophos doesn't have complete whitelisting capabilities, although it does have some application control functionality (described above). Patch analysis is part of its NAC Advanced product, which requires the legacy NAC management console. Sophos also lacks extensive vulnerability information. Sophos has some continuous automated device discovery capabilities via its automatic synchronization with Active Directory; however, greater functionality would be a welcome addition.

Symantec

Symantec continues to have the largest endpoint protection market share by a significant margin, and its flagship product, Symantec AntiVirus (SAV), underwent a major overhaul in 2007 and is now renamed Symantec Endpoint Protection (SEP) 11.0. Symantec continues to be a solid leader in this analysis based on significant improvements in the SEP, its data leak protection capabilities and PCLCM integration plans with Altiris. Symantec is an excellent shortlist inclusion for any large global enterprise, particularly those that appreciate the value of PCLCM and EPP integration.

Strengths

- A significant portion (~25%) of its installed base has now upgraded to and field tested SEP 11.0, and the product is in its fourth maintenance pack.
- The new management and reporting interface, based on the Sygate technology, is a significant improvement over the old SAV version. It's very task-oriented and provides significant improvements in reporting dashboards and usability.
- The anti-malware engine is also significantly improved with the addition of the Sygate personal firewall, port and device protection, and improved NAC in a single agent architecture. The new agent boasts a much-smaller footprint due to agent consolidation, and provides the fastest scanning speeds in recent tests (AV-Comparatives.org). Symantec also added a number of features to minimize the impact of scheduled scans.
- Malware protection is also enhanced with more HIPS prevention capabilities and higher detection accuracy.
- Symantec also offers data backup and remote access technology, and imaging technology, with Veritas and Ghost brands; however, these technologies haven't yet made their way into the EPP suite or management console.
- Symantec's acquisition of Altiris, a leader in the PCLCM market, will be a significant asset as the PCLCM integration trend continues. Symantec will be able to leverage PCLCM functionality, such as asset discovery/inventory, configuration management, vulnerability assessment, and software management and distribution capabilities.
- Symantec has also made significant investments in DLP, and 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 workflow engine, which enables organizations to automate security and operations processes, provides a good solution for organizations to integrate disparate applications into repeatable security and operations processes.

Cautions

- Symantec still receives low marks from customers for support and service. This issue is being addressed by senior management, but it will take time for improvements to be implemented. Larger customers should demand that named support engineers be assigned to their accounts.
- Despite improvements, Symantec continues to address code quality and testing because SEP 11.0 had numerous issues on release. However, service pack MR3, which was released in September 2008, has resolved most issues.
- Performance and resource requirements of the management server are still a problem for SMBs. The Small Business Edition is due in 2Q09, and it will focus on ease of use, simplified dashboards and reporting, management server performance and resource usage enhancements, and subscription licensing.
- The SAV to SEP upgrade is a significant undertaking and requires users to completely replace the agent and management infrastructure. It also requires additional training for the new management console and the expanded configuration options. Symantec has expended considerable resources to make this transition smoother with numerous deployment guidelines and support.
- Symantec must carefully manage the integration of the Altiris management framework, and should advertise its road map so that the migration strategy is very clear for customers and prospects.
- Altiris Patch Management and vulnerability management solutions are weak.
- Symantec is missing Windows Server 2008 support.
- Symantec is still missing its own integrated full-disk or file encryption, although it has licensed GuardianEdge. DLP has been integrated with the Altiris management console, while GuardianEdge encryption is integrated with SEP management, thereby complicating comprehensive data protection. We expect Symantec to acquire an encryption vendor in 2009.
- The converged SEP 11.0 client functionality and management console doesn't extend to Mac or Linux clients, or to its e-mail and Web gateways.
- The overlap with Symantec Critical System Protection and Symantec Control Compliance Suite needs to be rationalized and consolidated into a single management and reporting console.
- Buffer overflow technology from Sygate wasn't integrated. Most EPP competitors offer buffer overflow protection.
- Add-ons to the SEP 11.0 foundation can be expensive. Although SEP 11.0 is NAC-ready, even minimal policy enforcement capabilities require a NAC "starter edition" at roughly $10 per endpoint, and some clients have reported wireless NAC synchronization issues.

Trend Micro

Trend Micro is the third-largest anti-malware vendor, with a significant market presence in the Asia/Pacific region and EMEA, and one of the largest worldwide networks of labs and monitoring capabilities. We anticipate that Trend Micro's major new projects, File Reputation and BigFix management integration, will have a positive impact on its vision score in 2010; however, as of this writing, neither is in general availability, so Trend Micro's execution score has declined slightly relative to other leaders. Trend Micro should be considered by organizations seeking a solid, signature-based anti-malware solution.

Strengths

- A major initiative in 2008 was the introduction of the File Reputation component of the Smart Protection Network (previously announced components included e-mail and Web reputation). This network of cloud-based data centers will enable OfficeScan v.10.0 (now in beta, with general availability in 2Q09) clients to perform a real-time query of global signature databases to get the very latest file reputation information. This lightens the client footprint and eliminates the signature distribution time lag.
- OfficeScan has antivirus, anti-spyware, Trend Micro basic firewall and Web Threat Protection in a single product.
- Starting with v.8, OfficeScan began providing additional protection from Web threats by enabling administrators to block malicious URLs at the product.
- Trend Micro also offers an advanced Intrusion Defense Firewall (IDF), developed by Third Brigade, as an optional plug-in for OfficeScan. IDF offers solid, deep-packet, inspection-based HIPS. (Trend Micro acquired Third Brigade, which developed the IDF, in May 2009.)
- In 2007, Trend Micro acquired Provilla, which provides endpoint DLP capabilities in LeakProof.
- OfficeScan provides network-based NAC with the Trend Micro Threat Management Solution.
- A recent strategic alliance with BigFix will improve management for large global customers, and enable customers to integrate endpoint security management and PCLCM solutions, such as asset/rogue discovery, vulnerability detection, patching and security configuration auditing.

Cautions

- Trend Micro continues to be very conservative in acquiring and integrating newer technologies, which affect its vision and execution scores.
- Although the BigFix partnership is positive, we would like to see a more-vigorous PCLCM integration strategy. Trend Micro will only be offering its customers BigFix's Patch Management Module and Power Management Module. Trend Micro customers that want to adopt other BigFix operations functions (such as configuration management, port control, vulnerability assessment and software management) must obtain them through the BigFix channel, thereby creating potential customer ownership challenges. Moreover, Trend Micro will promote the converged solution only for customers with more than 10,000 seats. Gartner believes that the market for converged products will be most appealing initially to the sub-5,000 seat level.
- Control Manager doesn't yet have the richness of reporting like some competitive solutions, and central management can be difficult. The BigFix partnership should improve manageability, but BigFix management will only be available in a special version of the product that's aimed at large organizations.
- OfficeScan provides no application control capabilities. However, the IDF plug-in can control applications at the network level, but can't block specific controls from running in a browser.
- OfficeScan provides no buffer overflow protection capabilities.
- Trend Micro has no device control capabilities without the BigFix management console.
- OfficeScan provides no encryption capabilities, although the Identum technology it acquired could eventually be used to provide file and folder encryption.
- OfficeScan doesn't have an agentless version, although it does have a hosted drop-down agent version with HouseCall Web scanner.
- 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. Trend Micro's NAC functionality is very limited, and Trend Micro isn't a strategic NAC vendor.

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 doesn't necessarily indicate that we have changed our opinion of that vendor. This may be a reflection of a change in the market and, therefore, changed evaluation criteria, or a change of focus by a vendor.

Evaluation Criteria Definitions

Ability to Execute

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

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

Sales Execution/Pricing: The vendor's capabilities in all pre-sales activities and the structure that supports them. This includes deal management, pricing and negotiation, pre-sales support and the overall effectiveness of the sales channel.

Market Responsiveness and Track Record: Ability to respond, change direction, be flexible and achieve competitive success as opportunities develop, competitors act, customer needs evolve and market dynamics change. This criterion also considers the vendor's history of responsiveness.

Marketing Execution: The clarity, quality, creativity and efficacy of programs designed to deliver the organization's message to influence the market, promote the brand and business, increase awareness of the products, and establish a positive identification with the product/brand and organization in the minds of buyers. This "mind share" can be driven by a combination of publicity, promotional, thought leadership, word-of-mouth and sales activities.

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

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

Completeness of Vision

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

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

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

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

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

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

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

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