Gartner

Research
G00219355

16 January 2012

Magic Quadrant for Endpoint Protection Platforms

Peter Firstbrook, Neil MacDonald, John Girard

Endpoint protection platforms continue to struggle to block typical malware threats, and are even less effective with low-volume targeted attacks. A few vendors have started to provide proactive tools, such as vulnerability detection and application control, that reduce the attack surface.

Market Definition/Description

(This document was revised on 18 January 2012. The document you are viewing is the corrected version. For more information, see the Corrections page on gartner.com.)

The enterprise endpoint protection platform (EPP) market is a composite market primarily made up of collections of products. These include:

- Anti-malware
- Anti-spyware
- Personal firewalls
- Host-based intrusion prevention
- Port and device control
- Full-disk and file encryption
- Endpoint data loss prevention (DLP)
- Application vulnerability management and application control

These products and features are typically centrally managed and ideally integrated at the policy level.

Despite the introduction of new players, the displacement of incumbents is still a significant challenge in the large-enterprise market. The biggest impact of the Magic Quadrant Challengers and Visionaries is to push the dominant market players into investing in new features and functionality (sometimes via acquisitions), and to keep pricing rational. However, in the sub-thousand-seat-level market, we do see more displacement, and buyers have more product choices due to lower management requirements. Current prices for comparable offerings are down from our last Magic Quadrant;

however, vendors are often substituting more-complete suite offerings with little or no increase in annual costs.

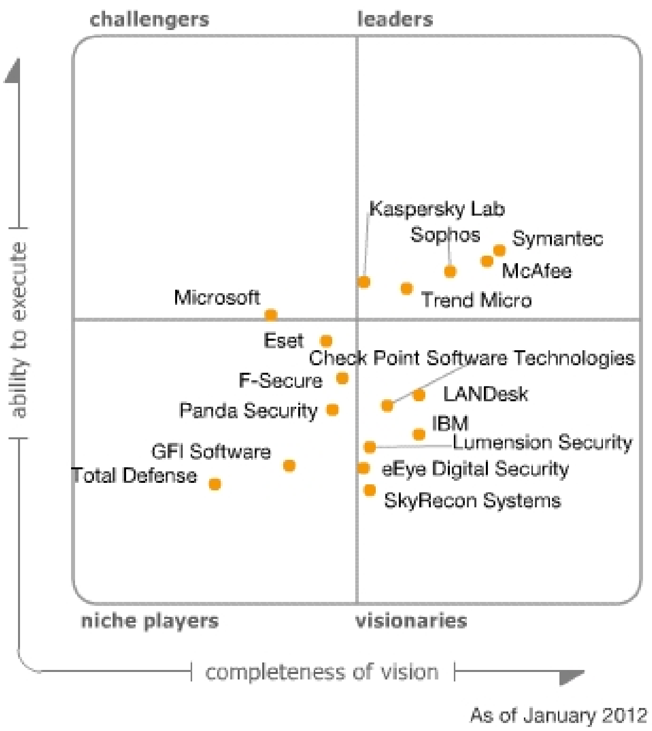
In 2010, the enterprise market was still dominated by McAfee, Symantec and Trend Micro, which represents approximately 60% of the total enterprise market. Notably, however, the share of these dominant players is down considerably from 85% in 2007. These market leaders are losing market share to increased competition, primarily in the lower end of the market with less than 1,000 seats, but also making inroads in larger accounts. Sophos and Kaspersky Lab are the primary beneficiaries of this trend, and these vendors are improving mind share and market share in the enterprise market.

The market size at year-end 2010 was approximately $3 billion, up 6% from 2009, following the macroeconomic recovery of enterprise PC growth. This is slightly higher than the 5% growth we projected in the 2010 Magic Quadrant. We anticipate growth rates to continue in the 5% range in 2011 and 2012.

Microsoft's impact on the enterprise market has not yet been significant; however, it increasingly appeared on the 2011 shortlists of customers due to recent improvements to its offering and licensing changes, which makes the solution effectively "free" to organizations licensed under Core CAL. We note that approximately one-third of enterprise buyers indicate that they are actively considering Microsoft or plan to do so during their next renewal periods. Microsoft continues to make steady product progress and is now, finally, poised to take some enterprise market share; however, its impact will be tempered by high growth on a small market share and product limitations (outlined here). Moreover, Microsoft's impact in the enterprise market may be influenced by the Windows 8 penetration rate, and any decision to include malware protection in Windows 8 is likely to face legal and regulatory issues, especially in Europe if it is viewed to unfairly affect market competition.

Magic Quadrant

Figure 1. Magic Quadrant for Endpoint Protection Platforms



Source: Gartner (January 2012)

Vendor Strengths and Cautions

Check Point Software Technologies

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

Strengths

- Like its network offerings, Check Point Endpoint Security uses a "software blade" architecture where clients pay for only the capabilities they need from a comprehensive suite of capabilities. These include personal firewall, anti-malware (licensed from Kaspersky Lab), full-disk encryption, network access control (NAC) and integrated VPN.

- Check Point's management console integrates malware protection and data encryption suite offerings. It offers a clean interface with easy navigation and quick access to summary data (overview/dashboard, organization, policies, reports and deployment) that is very similar to a network firewall interface. Reporting is significantly improved. The dashboard can be customized for each administrator. It provides good hierarchical and object-oriented policy, and can exploit network firewall policy objects, such as network zones, in a client firewall policy and can leverage installed gateway appliances as relays for client updates. Check Point offers a unique user-based management capability that allows administrators to develop and view user-specific policies across multiple devices.
- The personal firewall is comprehensive and includes extensive prepopulated program profiles, excellent location-based policies and very good VPN client integration.
- Check Point offers application control capabilities (which it calls program control) augmented with Check Point's Program Advisor service. This enables administrators to define 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.
- Check Point added browser protection technology from ZoneAlarm, which helps clients avoid malicious Web-based malware.
- Check Point added support for Mac clients in 2011.

Cautions

- Check Point is best known for its network-based protection solutions, and has had difficulty with penetration into the broader EPP market beyond its installed base of VPN, host firewall and encryption customers. Gartner customers rarely inquire about this solution. Moreover, the company is not forthcoming with financial and customer data that would allow us to accurately evaluate its progress in this market.
- Check Point is dependent on Kaspersky Lab for anti-malware signatures to review suspicious code samples and to prepare custom signatures for targeted malware. Although signatures are becoming a replaceable commodity, business disruptions in Kaspersky could affect Check Point customers. It is also increasingly challenged to 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.
- The management console provides a good summary view of the EPP agent status; however, it does not include any vulnerability or configuration assessments, nor does it have any integration with operations tools. The Compliance Blade does assess the configuration/security level of endpoints in the system and provides a detailed report showing compliance issues.
- The Check Point management console is a Windows client/server application and does not offer a browser-based option. Check Point is dependent on software distribution tools to install the initial client, and lacks the ability to remove other anti-malware products. The solution doesn't include many options to minimize the impact of scheduled scans, such as the impact on CPU use, or to avoid conflicts with critical programs.
- Check Point's program control solution can't prevent programs from installing. It only blocks network access via firewall permissions and terminates the process. Program control is not as flexible as competitive solutions to address the needs of large enterprises. For example, it doesn't have a good centralized way of

allowing trusted sources of change. An improved application control software blade that includes trusted sources of change is currently in pilot tests with customers.

- The SmartDefense HIPS policy isn't tunable and doesn't allow administrators to whitelist applications that incur false positives.
- Although Check Point has mobile device management (MDM) capabilities on its road map, it has not yet shipped these capabilities.
- Although Check Point introduced network-based DLP in 2011, Check Point's data protection strategy is still missing client-based content-aware DLP. An endpoint DLP security blade is currently in pilot tests with customers.
- Check Point protection is primarily limited to Windows endpoint PCs. Not all software blades are available for the Mac client, and it doesn't offer protection for specialized servers, such as Microsoft Exchange, Lotus Notes or Microsoft SharePoint.
- Although its agent will run in VMs, Check Point has no specific optimization for virtualized environments.

eEye Digital Security

eEye provides a unified management console for vulnerability analysis as well as malware and intrusion prevention capabilities, backed by its own malware research labs and augmented by a licensed signature database from Norman. Existing eEye Retina customers and enterprises that value integrated vulnerability analysis should consider eEye Blink.

Strengths

- In early 2011, eEye completed the transition of its customers to the Retina CS Console from its legacy management console. Retina CS manages eEye's network-based and endpoint vulnerability management products.
- The Retina CS management console is a Web/Flash-based user interface that manages the various eEye offerings. It provides role-based reporting and dashboards, dynamic associations of target machines via Active Directory and Smart Groups, as well as additional reporting modules for compliance, configuration and patching.
- Since our last analysis, the new antivirus engine improved the capability to detect "Fake AV" and other advanced malware, and is faster, consumes less memory and has a smaller update size. eEye has also added real-time alerting capability and a wizard-based application and network protection policy creation.
- Blink uses an embedded version of eEye's Retina Network Security Scanner to perform local vulnerability assessments and report the findings to the Retina CS console.
- The eEye Retina Protection Agent (RPA) is a subset of Blink designed to work alongside other EPP and antivirus solutions, and to provide agent-based vulnerability assessment and intrusion prevention services.
- eEye's central vulnerability management supports the capturing of malware events from more than 15 vendors and targeted Windows events, and integrates with Windows Server Update Services (WSUS) to allow patching.

- All functions are packaged in a single agent, including the Norman signature engine. Layers of function are easily enabled or disabled by the administrator without making changes to the installed image or drivers. Security policies can be monitored and updated from outside the firewall without requiring a VPN.
- eEye is one of the few providers in this analysis to offer a service-level agreement (within 48 hours) on new critical exploits, meaning that it will protect against these exploits within 48 hours, even if the system is unpatched.
- eEye uniquely offers physical management appliances for rapid deployment and management, and offers a software as a service (SaaS) product for vulnerability assessment.
- eEye has a small but very skilled team of malware experts that provides excellent technical support and malware information.

Cautions

- eEye is one of the smallest companies in this market. Its total staff size, including research and engineering groups, is small compared with the EPP industry average. It has a limited presence outside North America and in organizations with more than 500 employees.
- Its solution has the capability to blacklist applications, but it is a manual process with no trusted sources of change. It offers limited NAC integration.
- Although eEye develops its own spyware signature database and cleanup routines, the solution relies on Norman for anti-malware signatures; business disruptions in Norman could impact eEye customers. Although the Norman anti-malware engine is tested regularly, eEye does not participate in many industry tests to demonstrate the effectiveness of its collection of technologies. Automated malware damage cleanup capabilities are limited.
- eEye has limited device control capabilities, but no encryption or DLP capabilities. It lacks the ability to enforce encryption on data that's written to external storage devices, but it does have a number of policies to limit access and writing to external devices.
- It supports only Windows OS desktop and server platforms (including IIS), so companies with other devices (for example, Apple Macintosh) and specialized servers (such as Microsoft Exchange or SharePoint) cannot use the product. It also does not have any MDM or protection capabilities.
- The anti-malware agent works on a virtualized Windows host. However, it is not optimized for a virtualized environment.

Eset

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

Strengths

- The flagship enterprise product, Eset Smart Security, includes integrated anti-malware, anti-spam and a 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, with a left click, install the EPP agent or perform other remediation activities.
- The Eset anti-malware engine is a consistently solid performer in test results. The Eset engine has a strong reliance on heuristics and generic signatures, and includes client-based malicious URL filtering and sandbox heuristics, which run all executable files in a virtual emulator.
- Recent improvements include active memory scanning and the addition of a whitelist to improve scanning performance.
- Eset supports a broad range of Windows clients and servers, including Exchange, Lotus Notes/Domino, Linux Solaris, and Novell NetWare and Dell storage servers, mobile devices (Windows Mobile Android and Symbian), and Apple OS X and Linux desktop platforms.
- Eset offers a limited MDM solution with the launch in 2011 of the Mobile Security Business Edition for Windows Mobile and Symbian.

Cautions

- Eset is lacking in management features for larger, more-complex organizations. The management console is long overdue for an update; it's very complex and lacks a clear, actionable dashboard view to enable more-rapid or automated problem identification and remediation. A separate Web-based dashboard provides a flexible customizable reporting interface, but it does not allow for direct drill-down into the management console. It also lacks many common enterprise capabilities, such as role-based administration, information and policy elements that can be delegated (or restricted) to end users and automatic rogue machine detection. It offers limited options for scheduled scan priority.
- It has very weak reporting. A lot of information is captured, but it is hard to get at, and there is no ad hoc reporting, just filtered log views. It is overly reliant on "parametric" groups to segment reporting data. Eset Sysinspector shows lots of detail about a client for troubleshooting; however, this data cannot be used across all clients for reporting or grouping.
- There is no significant security state assessment beyond EPP agents, such as application vulnerability and configuration assessments, and no significant integration with operations tools.
- Clients can be distributed by the management console; however, deinstallation of competitive solutions is an additional service cost that isn't included in the solution.
- The HIPS capability can only be activated or deactivated; it can't be selectively deactivated to allow specific false-positive files to execute. Heuristics can add a performance impact, especially on older PCs, although these are not turned on by default.
- Eset doesn't yet offer many of the additional EPP components, such as application control, encryption and DLP. Port/device control capabilities are not very granular, just block or allow.

- Although Eset operates in a virtual environment and has a low system impact, it has not been optimized for these environments.

F-Secure

F-Secure has been in the anti-malware industry for more than 20 years and has a very good track record for malware testing results. The company is focused on endpoint protection and is less interested in other aspects of the EPP market, such as data protection. F-Secure is a good choice for organizations in supported geographies that prefer dedicated malware protection solutions.

Strengths

- F-Secure provides on-premises software-based management and hosted solutions, as well as managed services via partners. It also offers very attractive pricing with monthly or yearly subscriptions.
- F-Secure has consistently good malware test results and performance tests. It provides cloud-based look-ups and a file reputation feature (DeepGuard), which considers file metadata such as prevalence, source and age before allowing files to execute. In 2011, cloud-based look-ups were extended to on-demand and scheduled scans.
- Its generic detection and removal of rootkits is delivered via BlackLight.
- F-Secure supports virtualized environments (VMware, Citrix and Microsoft Hyper-V), with database and policy update randomization. It also offers protection for Linux and Mac platforms.
- F-Secure has mobile clients for Android, Research In Motion, Symbian and Windows Mobile, and a cloud-based MDM capability primarily aimed at SMB organizations.

Cautions

- F-Secure is strongly based in the EU and has very little presence or brand recognition in other markets. It is growing much slower than the overall market.
- Although F-Secure develops some of its own signatures, the solution relies heavily on Bitdefender for its anti-malware signatures; business disruptions in Bitdefender could impact F-Secure customers.
- F-Secure's client/server-based (Windows or Linux) management interface is very limited and is lacking numerous enterprise features. It only has two roles ("full" or "read only"). It does not offer any state information beyond anti-malware status and does not provide any significant dashboard capability or any drill-down into remediation capability. Autodiscovery of new agents is a manual process and can't be scheduled. Reporting capability is very basic and does not allow for ad hoc reporting.
- F-Secure does not believe that encryption or DLP is relevant to its malware detection mission. It does not offer flexible device or port control, nor does it offer any application control beyond DeepGuard.
- MDM capability is not integrated into the endpoint management console.
- F-Secure does not provide any protection for SharePoint servers.

GFI Software

GFI Software offers a wide range of security solutions (notably, secure email Web gateways, email archives, vulnerability scanning, patch management, event monitoring, storage management and backup solutions) primarily for SMBs. GFI is a shortlist candidate for SMBs looking for a simple and lightweight anti-malware engine.

Strengths

- GFI's Vipre management interface is efficient and clean. It provides a large range of preinstalled movable dashboard widgets, and provides good ability to view and drill into log data and assign policy to groups and users. Since our last analysis, most of GFI's improvements were aimed at a fast, out-of-the-box installation process. It added a removal tool that uninstalls popular EPP solutions, Windows firewall autoconfiguration to allow the Vipre client to communicate policy and update servers, and an integrated database (the previous version required a separate SQL database). It also added a remote access tool for easy remote site management.
- Malware detection is augmented with MX-Virtualization, which analyzes malware in real time in a sandboxed environment on the PC.
- GFI offers client-based malicious URL blocking, rootkit scanning and automatic scanning of USB drives.
- The client is relatively lightweight and efficient, providing fast scanning.
- GFI offers Windows and Mac client support, as well as Exchange server versions.
- GFI offers a free Web-hosted malware analysis engine that provides immediate forensic feedback on submitted application files.

Cautions

- GFI is squarely aimed at the SMB market, where ease of use and set-and-forget functionality are assets. We do not have a lot of reference customers in the Gartner installed base, and GFI is not evaluated in most of the malware effectiveness testing, so performance and effectiveness are not well-documented.
- The Vipre management capability will be limiting for larger enterprises. It relies on Windows network browser or Active Directory information to find unmanaged machines.
- Reporting and dashboards are very basic. It does not have any ad hoc reporting capability, only filtered views of historical data. Role management is not scalable.
- It does not offer data protection capabilities, such as encryption and DLP.
- Although the company has some vulnerability and patch management assets, they are not integrated with the EPP suite. The solution does not provide a holistic security state assessment or any remediation capability.
- GFI does not provide any MDM capability or mobile endpoint protection products.
- It does not have any specific features to support virtual environments.

- The company does not have any hosted offerings for the management server, nor does it have real-time cloud-based update capabilities.
- It does not offer any application control capabilities.
- Device control is not part of the EPP suite.

IBM

IBM built its EPP on top of a PC life cycle management platform, the Tivoli Endpoint Manager (TEM) acquired with BigFix. The core malware engine and firewall are provided by Trend Micro, now called TEM Core Protection (TEM-CP), and advanced host-based intrusion prevention system (HIPS) and firewall capability is provided by Proventia (formerly ISS). These tools are augmented with IBM's X-Force research labs. Large organizations that have a close relationship with IBM or Trend Micro should include IBM on their shortlists.

Strengths

- During 2011, IBM announced a new Security Systems Division to centralize all of its security assets, effective 1 January 2012, with a dedicated sales force, which should help in execution in 2012. It also enhanced performance in the TEM CP malware engine. It has also continued integration of management capabilities of a number of IBM products, including IBM Security Server Protection.
- This solution combines a unified console and a single agent for PC life cycle management, including power, patch and vulnerability management, with two options for endpoint protection: (1) a fully integrated solution leveraging Trend Micro as well as (2) the ability to monitor other agents such as McAfee, Symantec and Microsoft Forefront.
- Leveraging the capabilities of Trend Micro, the TEM-CP solution now provides VMware vCenter and Citrix Xen Server performance optimization capabilities, including virtualization awareness, serialization of antivirus scans to prevent resource contention, and intelligent scanning through caching of files based on VDI golden image. IBM also added Trend Micro's advanced device control and endpoint DLP solutions.
- IBM Security Server Protection, Proventia Server for Linux, and RealSecure Server Sensor provide deep packet inspection and HIPS capabilities, sharing the same Protocol Analysis Module of ISS network-based appliances. IBM server protection products boast very broad server support with Windows, Linux, HP-UX, Solaris and AIX, including 64-bit support for Windows and Linux, and new AIX 6.1 support.
- For mobile laptop users, the TEM Relay provides real-time visibility and control for endpoints, regardless of network location, and allows for updating malware definitions, engines and EPP.
- The IBM Global Services group offers a mature managed security services.

Cautions

- IBM has not executed well in the EPP market in the past, and it has not provided Gartner with enough information to accurately evaluate its current progress in this market. Mind share of this solution, as represented by Gartner customer inquiries, is very low despite IBM's obvious size and channel advantages. The new security services division should help in this regard and be reflected in a better execution during 2012.

- IBM has a large, and somewhat confusing and overlapping product portfolio in this market, and prospective customers must carefully match desired features with specific product offerings. The complete suite is expensive.
- The Tivoli Endpoint Manager is very powerful; however, it can be complex to use, and it is not optimized for the security role. The TEM management interface is not browser-based and has limited customization capability. IBM also has a Web-based reporting console and dashboard that has a totally different look and feel, and is not linked to remediation actions. Security-state assessments are still disjointed, lack prioritization and are missing from the dashboard. The look and feel of the Proventia products is also very different. Management of non-IBM solutions is limited to monitoring, and does not replace the native management servers and their configuration capabilities.
- IBM doesn't offer any integrated full disk encryption, (although BitLocker Management was added in Q4 2011) and has very limited application control capabilities.
- IBM's mobile device management (MDM) solution was in beta testing during this review; it is scheduled for release in 1Q12 and will be evaluated in the next Magic Quadrant.
- No support beyond Windows and Macintosh clients is offered, and there is no ISS firewall planned for Macs. Also, no support is offered for Microsoft Exchange, Lotus Notes, SharePoint and other specialized servers.
- Although IBM has its X-Force security analysis team, it has no signature-based anti-malware capabilities of its own and is dependent on Trend Micro. Disruptions at this critical partner could have an impact on customers. Integration of the Trend Micro engine into the TEM client offers a very different experience from a native Trend Micro Office Scan implementation and a potential forced delay in upgrading to the latest Trend Micro Client, although the last upgrade was only a lag of two months.

Kaspersky Lab

Kaspersky Lab continues to be one of the fastest-growing large vendors in this Magic Quadrant, and its brand awareness is growing outside of its large European installed base, improving its ability to execute. Kaspersky has released a new version of its solution that significantly improves its vision criteria with the inclusion of vulnerability management, application control and Web control capabilities. This nicely complements its traditional strength in malware effectiveness and customer satisfaction. Organizations looking for an alternative vendor to the traditional market leaders should evaluate Kaspersky.

Strengths

- The malware research team has a well-earned reputation for rapid and comprehensive malware detection, as well as small, frequent signature updates. During the study period, the solution was significantly improved with the addition of vulnerability patch management capability and application control capabilities, all of which can proactively protect endpoints by reducing the potential attack surface.
- The redesigned Kaspersky console is comprehensive and offers very granular control of its agent, improving manageability for large enterprises. The dashboards can be customized and are task-oriented, which helps administrators to focus on frequent decision points. Drill-down pathways into tasks are easy to understand. It also offers improved support for Active Directory, a security status dashboard, improved reporting capabilities and native client distribution capabilities. The solution was also improved with the addition of fine-grained device control.

- Kaspersky historically has a small disk and memory footprint, and has further improved this in its latest release. In addition, it offers a range of choices to limit resource utilization such as "don't run full scan on battery power."
- Kaspersky offers advanced HIPS features, including an isolated virtual environment for behavior detection, application and Windows registry integrity control, real-time inspection of code at launch, and integrated malicious URL filtering. On PCs, the endpoint agent, Kaspersky System Watcher, can perform a system rollback to flush bad configurations.
- Kaspersky offers broad endpoint platform support, including file servers such as Windows Server 2008, Windows 7 workstations, Citrix, Linux, Novell NetWare, Microsoft Exchange, Lotus Notes/Domino, Windows Mobile, BlackBerry, Android, and Symbian, as well as Microsoft Forefront Threat Management Gateway and EMC Celerra.

Cautions

- Kaspersky has added endpoint security for mobile phones, but its entry is less compelling when compared to the MDM market leaders. To catch up quickly with the major EPP players, an MDM acquisition would be helpful.
- A large number of policy templates are provided, but the policy management paradigm is flat and lacks the object-oriented inheritance of competitive offerings. Large numbers of involved users/templates will increase manual policy coding and require consistency reviews to avoid gaps in protection policies.
- Kaspersky doesn't yet offer any endpoint encryption capability (due in 2012) or DLP, which leading vendors in this market are using to increasingly leverage EPP sales.
- Its firewall offers no Wi-Fi-specific protection or policy support, and it has limited VPN policy options.
- Application control capabilities introduced in v.8 are good, but could be improved with better workflow capabilities and streamlined policy creation.
- A native NAC capability is missing.
- There is no SharePoint support, nor an offering uniquely targeted to address hosted virtual desktops, although both are on the road map for delivery in 2012.

LANDesk

LANDesk is one of the leaders in the PC configuration life cycle management (PCLM) market (see "Magic Quadrant for PC Life Cycle Configuration Management") and continues to benefit from our increased weight on more-holistic security state assessment and application control capabilities, which is only countered by a lack of a security management orientation in the product set. Lagging market and mind share growth is weighing down its Ability to Execute. LANDesk's Security Suite is an excellent choice for its existing customers or those seeking integrated solutions for security and operations.

Strengths

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

- The LANDesk console is comprehensive and includes all security management capabilities within the same console, alerting and reporting framework.
- LANDesk agent has a single, modular architecture so that security functionality (like anti-malware) may be activated as needed. Policy is very object-oriented, and reuse is common. We particularly like the concept of pilot groups that get advanced copies of changes, with a set delay for subsequent rolling updates, and the ease with which it can find, assess and update any aspect of a PC, even when it's off LAN.
- LANDesk offers MDM and security into its integrated suite to enable management of security functions of new platforms, such as iPads and mobile device platforms, and expanded this capability in late 2011.
- The base LANDesk Security Suite includes an anti-spyware signature engine (Lavasoft), personal firewall, HIPS (from its acquisition of Viguard), device control and file/folder encryption, vulnerability and configuration management, patch management, and limited NAC capabilities. Customers may use LANDesk to manage McAfee, Symantec, Sophos, Total Defense and Trend Micro, or they may choose to pay extra for LANDesk Antivirus, which is built around an entirely integrated Kaspersky malware scan engine.
- The LANDesk Security Suite also includes an integrated full-drive encryption option licensed from Credant, introduced in 2011, and includes support for persistent and nonpersistent hosted virtual desktop images. Credant can also centrally manage BitLocker through the LANDesk console.
- LANDesk HIPS and firewall technology capabilities include location-aware policies, buffer overflow protection, application whitelisting and blacklisting, and more-granular control of applications once they're executing. Whitelist administration is eased by a learning mode for the development of policies.
- LANDesk Configuration Manager provides extensive port and device control, including encryption capabilities for removable media.
- For mobile users, a LANDesk Management Gateway placed in the DMZ provides real-time visibility and control for endpoints, regardless of network location, improving visibility and control over mobile devices.
- LANDesk offers endpoint protection for Windows endpoints, and anti-malware for Microsoft Exchange. With an integration of Odyssey Software, LANDesk can offer full MDM capability.
- LANDesk is well-established in larger organizations, with more than half of its EPP installed base from organizations with at least 5,000 seats.
- In addition to its own firewall offering, LANDesk can manage the Windows firewall.

Cautions

- LANDesk doesn't perform its own malware research, although it does have 30 engineers researching and creating content and compliance standards. The solution relies on Kaspersky to review suspicious code samples and prepare custom signatures for targeted malware samples. Although signatures are becoming a replaceable commodity, business disruptions to important partners could have an impact on customers. Encryption capabilities are also provided by partners.
- Not all LANDesk Security Suite features are available on all managed platforms. LANDesk HIPS and the LANDesk Antivirus add-on support only the Windows platform and aren't supported for Linux. There's no malware support for Microsoft SharePoint, Lotus Notes or Windows Mobile clients. Macintosh platforms benefit from PCLM tools, but antivirus is supplied by a Kaspersky-branded solution.

- LANDesk needs to expand its application control capabilities to close the gap with dedicated application control solutions.
- LANDesk doesn't offer client-based content-aware DLP.
- Customer feedback indicates that the LANDesk console is designed from an operational perspective, the learning curve for security operations administrators who are used to working with traditional EPP or antivirus solutions will be steep.
- While LANDesk can discover and inventory virtual machines, and its agent will run within a virtual machine, it has no specific optimization for anti-malware protection in virtualized environments.

Lumension Security

Lumension first appeared in our 2010 Magic Quadrant, after it added a licensed anti-malware engine (Norman) to its PCLM suite. This integration and relationship continue in 2011. The Lumension Endpoint Management and Security Suite includes anti-malware, application control, patch and remediation, power management (with wake on LAN), scan, and security configuration management modules. Lumension also offers an IT governance, risk and compliance management (GRCM) capability as well as a risk manager capability. Existing Lumension customers or those seeking integrated solutions for security, operations and compliance should add Lumension to their shortlists.

Strengths

- The Web-based management interface includes all PCLM products, with similar task-based orientation and consistent navigation. Dashboards can be changed for a number of widgets, allowing administrators to have their own somewhat customizable dashboards. The step-through policy workflow is similar for PCLM and anti-malware policy. The solution offers a single unified client agent for antivirus, application control, patch and remediation for a broad range of client platforms. Lumension recently added new encryption capabilities and power management. The management interface provides rich role-based restrictions, including the ability to restrict log visibility to managed groups only.
- Lumension has significantly improved its application control capabilities in 2011, offering a comprehensive set of ways for enterprises to manage trusted change at endpoints. In addition, Lumension has built its own cloud-based file reputation Endpoint Integrity Service, which augments its application control offering for the look-up of unknown applications. For ease in deploying application control, it offers an improved application scanner for inventorying all applications and a quick lockdown capability that authorizes all installed applications, but blocks all new applications unless they are from trusted sources.
- Its historical strength in patch management provides an installed base to upsell its EPP offerings to. It has gained strength in device control from its acquisition of SecureWave.
- Lumension Device Control provides simple-to-use and comprehensive port and device control capabilities, which can limit the types of removable devices and media that may be used, the type of files that users are allowed to read/write, and specific device types. It can capture files that are written to or read from those devices and media, can limit the volume of data uploaded and downloaded, and can force encryption using a native encryption module. In 2011, Lumension fully integrated the device control module into its centralized console management system.

- Lumension can wrap around and manage the Windows firewall on Windows Vista and higher, and provides a generic framework for the management of other third-party firewalls.
- Integrated malware prevention from Norman includes sandbox capability that intercepts and prevents changes to host files, registry settings, and so on that are typically made by malware.
- Lumension console integration with Norman allows customers to submit suspicious files directly to Norman for analysis.
- A separate, stand-alone Risk Manager GRC tool provides security state information gathered from Lumension, and third-party tools illustrate compliance with corporate or regulatory standards over time.
- The Lumension Risk Management solution integrates information from Lumension's EPP console to provide a risk-based view of vulnerabilities, infections and remediation gaps across the entire organization.
- For full-drive encryption, in 2011 Lumension has partnered with Sophos.
- For content-aware DLP, in 2011 Lumension has partnered with RSA.
- In 2011, the company added integrated remote management capabilities for administrators to remotely control and administer the Lumension agent.
- In addition to patch management, Lumension's EPP has several capabilities of interest to operations, including wake on LAN and power management modules.

Cautions

- Lumension has limited brand awareness in the EPP market outside of its patch management installed base, and the majority of its EPP customers have less than 500 seats. While there is still market opportunity, Lumension has limited resources to aggressively target the market leaders. It needs to accelerate execution and raise its profile quickly to gain market and mind share before the Leaders execute on their application control and PCLM integration strategies, and eliminate Lumension's differentiation.
- Lumension has assembled its EPP capabilities from a variety of technology acquisitions and, as such, Lumension still feels like a collection of technologies rather than a cohesive EPP suite. GRCM is in a different interface.
- Lumension has no anti-malware labs of its own and is reliant on its anti-malware partner, Norman, to review suspicious code samples and prepare custom signatures.
- There is no personal firewall component; Lumension relies on the Windows firewall.
- Business disruptions at any of Lumension's partners could have an impact on customers. For example, in 2011, its full-drive encryption partner was switched from PGP/Symantec to Sophos.
- The company does not yet offer an MDM capability, although it is exploring an integration with a third-party offering this year.
- Its application control is lacking a database of known good applications.
- The management interface could be improved with continuous discovery scanning to discover new rogue clients on the network, user-defined dashboard widgets, improved ad hoc and hyperlinked drill-down

reporting, and more actionable and prioritized vulnerability and compliance information, as well as improved workflow between problem discovery and resolution.

- Although Lumension has extensive patch support for non-Windows platforms, its endpoint protection (application control, device control and anti-malware protection) does not extend beyond Windows endpoints and servers. It does not provide protection for Macintoshes or specialized servers, such as Microsoft Exchange.
- Although its agent will run in VMs, Lumension has no specific optimization for anti-malware protection in virtualized environments.

McAfee

McAfee has a broad portfolio of products, including network security components, data protection, risk and compliance, significant marketing resources, a solid operations capability, and a strong malware research and management team. The acquisition of McAfee by Intel brings financial and R&D resources, as well as tighter integration with Intel's technology. McAfee continues to be a solid Leader, based primarily on long-term leadership in cross-product management functionality, and it should be considered a strong vendor that's suitable for any enterprise.

Strengths

- McAfee's ePolicy Orchestrator (ePO) remains one of the better management platforms in this market. Advanced features include a multitier architecture, workflow improvements, filtering and policy by tags, support for user-based policy development, improved user interface design, and IPv6 support. It includes a trouble-ticketing system integration, such as integration with HP PC Help Desk and BMC Remedy. Microsoft integration improvements have been made to Active Directory and System Center Configuration Manager (SCCM), especially for asset reconciliation, software deployment and root cause event visibility. Endpoint protection is available with a SaaS-based management console for SMB organizations that do not want to deploy EPO on-site.
- McAfee recently announced the DeepSAFE platform, a McAfee-Intel jointly developed technology, which allows McAfee to develop hardware-assisted security products that take advantage of a "deeper" security footprint. DeepSAFE technology sits below the OS, and close to the silicon, allowing McAfee products to have an additional vantage point in the computing stack to better protect systems. The first product that relies on DeepSAFE technology is Deep Defender, a real-time kernel-level rootkit protection product to detect processes that are attempting to modify the Windows kernel.
- McAfee's integration of mobile data protection (MDP) solutions was well-executed in terms of time to maturity, bundling options and pricing. McAfee EMM support is offered for Android, iPhone/iPad, Nokia S60, webOS, Windows Mobile 6.x and Windows Phone 7 models.
- McAfee recently acquired NitroSecurity, a security information and event management (SIEM) solution provider, which we anticipate will improve ePO's SIEM capabilities across its product line. This will make it a higher-value platform by improving its ability to correlate system status, security incidents and external events to help focus operator attention on what's most important.
- Technology acquired from Solidcore Systems has significantly improved for PCs, and now offers very good application and change control capabilities, with numerous trusted sources of change as well as a large

categorized application database. New capabilities include workflow integration for automated approval of new whitelisted applications at the server and desktop level, as well as a managed whitelist in the cloud.

- McAfee SiteAdvisor, along with the McAfee host Web filtering add-on module, helps users avoid malicious websites and enables the enforcement of acceptable usage policy.
- McAfee Management for Optimized Virtualized Environments (MOVE) is one of the few solutions to optimize anti-malware for virtual environments.
- The combination of McAfee Risk Advisor, Vulnerability Manager, remediation module, and integration with Microsoft System Center and McAfee Security Innovation Alliance partners provides improved capabilities for security state reporting.
- McAfee has a strong endpoint DLP solution that can integrate with its more comprehensive enterprise DLP solution.

Cautions

- McAfee core malware protection capabilities have improved in some recent test results (such as antivirus comparatives); however, it has lagged in this area. Agent footprint size and scan performance are also areas that still require significant improvement.
- While Intel can help McAfee improve in the core enterprise and consumer EPP markets in the near term (that is, 12 to 24 months), longer-term investments in Intel priorities may distract McAfee from customer priorities, especially in the network security market. McAfee customers should evaluate the progress of the acquisition by monitoring McAfee's achievements in its core markets very closely. Intel's reluctance to provide detailed financial information will make this task more difficult.
- While McAfee's core EPP capabilities are well-managed, customers attempting to extend security management beyond the EPP using McAfee's increasing collection of tools (such as, Risk Advisor policy auditor, Nitro, Deep Command) will find a mixed bag of capabilities that need to be better presented in ePO, and better articulated to customers and channel partners.
- Overall satisfaction with McAfee service and support remained an issue with customers in 2011, and McAfee received one of the lower overall customer satisfaction scores in our survey of references. McAfee's 2010 disruptive false positives, which caused some customers significant disruptions, are still cited by customers as an example. While McAfee appears to be investing in service and support improvements, these have yet to be fully realized by McAfee customers.
- DLP is not integrated with the McAfee personal firewall, or with EPP policies, which may require companies to create duplicate policies for different subsystems.
- McAfee's HIPS solution is not gaining wide acceptance on endpoints due to administrative overhead. It is still difficult to granularly disable rules (that is, per application) to address false positives and can be noisy, partly due to uncorrelated alarms. McAfee has created best practices deployment guides and improvements in HIPS v.8 to alleviate these deployment challenges.

Microsoft

After a significant delay due to architectural changes, Microsoft released a new version of its EPP offering at year-end 2010 (after the publication of our 2010 EPP Magic Quadrant), Forefront Endpoint Security (FEP), replacing Forefront Client Security (FCS). FEP is now managed within System Center Configuration Manager (SCCM), providing a common view for configuration, patching, update and endpoint protection, including the Windows firewall. FEP is part of a broader Forefront-branded family that includes Forefront Protection for Exchange Server and Forefront Protection for SharePoint, which share a common name but different code base and management consoles. These two specialized Forefront server solutions are very attractive solutions for these platforms due to tight management integration and promising road maps. In March 2011, Microsoft announced licensing changes that make FEP effectively "free" for many organizations. This, combined with the large installed base of SCCM, placed Microsoft on the shortlist of many organizations in 2011 and significantly raised Microsoft's ability to execute over our previous Magic Quadrant. FEP is a reasonable solution for Windows-centric organizations licensed under Core CAL that have already deployed SCCM and that have other mitigating controls for security functionality that FEP does not provide.

Strengths

- Microsoft made a number of improvements in the anti-malware engine with its new version, including the addition of a number of system monitors, hidden system driver and anti-emulation detection, as well as enhanced JavaScript emulator, generic signatures, and vulnerability shielding capabilities.
- FEP relies on the software distribution capability of SCCM. Deployment of the new release of FEP will require only the purchase and deployment of the agent. No additional management servers or consoles should be required for SCCM organizations. SCCM also provides the infrastructure for signature updates; however, FEP also allows on-demand signature updates from the cloud for suspicious files and previously unknown malware.
- Organizations that are licensed under Microsoft's Volume Licensing programs receive FCS at a discount. Organizations that are licensed under Microsoft's ECAL or Core CAL program receive FEP at no additional cost, leading many organizations to consider Microsoft's FCS as a "good enough" way to reduce EPP budget expenses.
- FEP provides some direct management of the Windows Firewall.
- Forefront Protection 2010 for Exchange Server and Forefront Protection 2010 for SharePoint benefit from tight integration with these platforms and multiple scan engines.
- FEP provides support for virtual environments by enabling randomization of signature updates and scans, and offline scanning.

Cautions

- Microsoft SCCM 2007 (r.2) and Active Directory are prerequisites to FEP. SCCM is not as easy to deploy and maintain as purpose-built EPP management platforms and overkill for organizations that use other PC management solutions. SCCM is a capable software distribution and management platform; however, it is not designed for the unique needs of the security practitioner. Dashboard indicators are minimal and not customizable. It does not have granular role-based capability. There are only five preconfigured reports, although it includes custom report capability. The FEP reports only show anti-malware activity.

- Although it has improved, FEP's performance in malware testing has been well below average.
- We expect Microsoft to improve the development cadence with this latest release; however, since 2003, when Microsoft acquired GeCad, it has been glacially slow in providing improvements to Forefront.
- Forefront clients rely on Windows user/administrator rights management for tamper protection. Users and applications with administrator rights can disable the client.
- Forefront still lacks numerous capabilities common in other security solutions, including Android, Mac and Linux clients, advanced device control, integrated full-disk encryption, DLP, and application control.
- FEP 2010 is not supported to run on Small Business Servers (SBSs), the product is not intended for SBS installations, and you will have to use Forefront Client Security for SBS.
- There is no policy migration between FCS and FEP.
- Windows Firewall capability lacks advanced capabilities such as multiple location policy (it supports only two locations), extensive logging and granular policy controls. SCCM can manage some firewall policy, but using Group Policy Objects natively provides more extensive control, complicating management.

Panda Security

Panda offers several cloud-based security solutions. It has a very effective endpoint protection solution that is managed in a SaaS-based management console. It also offers secure Web and email gateway functionality delivered as cloud-based solutions. SMBs seeking easy-to-manage cloud-based solutions should consider Panda as a good shortlist entry in the geographies it supports.

Strengths

- Panda will focus future efforts on its SaaS-based management solution for endpoint protection, which is fully hosted by Panda (Panda Cloud Office Protection). References cite it as being extremely valuable for managing remote installations.
- Panda emphasizes remote control support for end users and has made it easy to call remote support sessions from the administration console. This is suitable to small-scale users that can justify operator-intensive interactions.
- The Windows-based management interface provides granular role-based management and group-level configurations, but, at the same time, simple and frequent tasks are easy to perform. Status updates for problem resolutions are effectively summarized on the main screen. The solution provides an easy-to-use report scheduler that delivers reports in a PDF. A large selection of template policies are provided, as well as many standard reports.
- Panda malware detection includes several proactive HIPS detection techniques and performs well in malware tests. 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. Panda recently launched device control capabilities.

- Panda Security for Desktops and Panda Security for File Servers use a cloud database look-up to detect new threats. This approach is a hybrid between a local antivirus agent and a secure Web gateway, and offers a way to quickly scale malware analysis, but is dependent on an online connection.
- Malware Radar is Panda's network-crawling malware and vulnerability audit tool. It can be a good utility for double-checking incumbent anti-malware accuracy. In particular, it helps ensure continuity of protection in enterprises that must run several antivirus products.
- Panda pricing is very competitive, and there are no upfront license costs, only an annual subscription.

Cautions

- Panda Security is slowly expanding from its EMEA presence, radiating outward from its Spain headquarters. However, weakness in Spain's economy in 2011 impacted Panda's growth, with the company laying off 30% of its workforce. Seventy percent of its business remains in Europe, and mind share remains weak in other geographies.
- The legacy on-premises and SaaS product solutions are diverging as Panda puts more development effort into its cloud offering. Buyers need to ask for a road map to determine if and where functional and management gaps may occur. The server-based management console (not Panda Cloud Office Protection) is still a Windows fat client, and no alternate browser console is offered. It lacks advanced features, such as adaptable dashboards, consolidated compliance status indicators, hyperlink drill-downs to log data and custom reporting. Some review tasks are difficult; for example, policy browsing is initiated in undersized pop-up windows. A tendency for operations to come and go in pop-up windows could be distracting to the operator.
- Malware Radar uses a different scanning engine, with more-advanced detection techniques activated (which takes longer to scan and potentially produces more false positives) than the base Panda product. Malware Radar uses a separate console for reporting its information (for example, critical vulnerability information surfaced by Malware Radar isn't visible in the main console).
- The standard product lacks location or use-case awareness that could be considered to alter protection rules. Panda is building location awareness into its cloud service.
- Panda's HIPS capabilities are powerful, but Panda's HIPS policy doesn't provide a monitor-only mode to enable testing and tuning before deployment. Moreover, TruPrevent identifies files only by name, and can be thwarted by changing file names.
- The scripting method used to define events and actions does not offer directed syntax, which would reduce the learning curve.
- Panda still lacks advanced firewall features, such as location-based policies, wireless-specific firewall options and VPN integration options.
- There's only one option to minimize the impact of scheduled scanning (CPU load limitation), although end users can delay scanning if they're authorized.
- The agent managed by Cloud Office Protection is a subset of the full Panda client — for example, it lacks HIPS capabilities and provides no application control capabilities.

- Panda is focused on traditional workstation support and has not done enough to stay competitive with the forays of leading vendors into the MDM market. Panda delivered on its road map for Mac workstations and delivered a full product during the study period.
- Panda doesn't support Microsoft SharePoint, nor does it offer a solution that addresses the needs of terminal services or hosted virtual desktop environments.
- Panda doesn't yet offer encryption or DLP.

SkyRecon Systems

SkyRecon's StormShield is designed as a seamless integrated EPP with a focus on behavioral protection. SkyRecon's Ability to Execute score is hampered by its relatively small market share and limited geographic presence, lack of its own native malware detection engine, and its still-maturing management capabilities. SkyRecon is a reasonable shortlist vendor for organizations that are in supported geographies seeking a replacement to Cisco CSA (which has reached its end-of-life stage), advanced HIPS capabilities and are willing to invest extra effort to administer the advanced capabilities of the offering.

Strengths

- The company's flagship product, StormShield Security Suite, is designed to address system and data protection via an extensible EPP capability that integrates multiple layers of security. These include HIPS, a personal firewall, Device Control System (DCS), encryption and an optional, fully integrated signature-based, anti-malware engine licensed from Avira.
- We particularly like the company's focus on advanced HIPS 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 designed from the ground up to work together.
- SkyRecon effectively uses policy-based restrictions to minimize the attack surface with object-oriented policies and configurations that are easy to set up. Policy-based application control is improved by a "challenge response" mechanism, which allows users to add software if they type in the justification for the installation in a pop-up window.
- SkyRecon offers extensive memory protection. Other defenses include rootkit detection, honey pots, privilege escalation and reboot protection.
- The Professional edition includes device control and NAC capabilities.
- The firewall provides good Wi-Fi policy options, as well as options to force VPN connections, and has been improved to perform deeper protocol analysis and protection from advanced cache poisoning attacks.
- Full-disk encryption is available and is included with StormShield Secure Edition.
- Flexible Data Encryption (FDE) offers encryption for files and folders on fixed hard drives and removable devices, and has been improved to support fully encrypted logical containers in addition to per-file encryption. FDE is integrated with the DCS service to provide device encryption and to audit device file activities.

- SkyRecon has a single management interface and a single lightweight agent (15MB including anti-malware protection) to support its multiple functions.
- As part of its HIPS focus, the product features granular device control policies, including controlling access to optical drives and blocking print-screen printing for a specific application.
- A 64-bit Windows support provision was added in 2011.
- To help with brand name awareness and create upsell opportunities, a free consumer edition — SPe — was released in 2011.

Cautions

- Although it continues to grow rapidly, SkyRecon is still one of the smaller vendors in this Magic Quadrant. Neither SkyRecon nor its parent company, Arkoon, has significant brand recognition or an enterprise client base outside of Europe. Arkoon also does not have a significant business presence outside of European markets.
- It supports Windows only and provides no Mac, Linux, Unix, mobile or email server support.
- SkyRecon has dropped its relationship with Panda. The only option for anti-malware protection is from Avira. SkyRecon has a very small malware research team and is dependent on Avira for signature-based protections.
- The management interface was comprehensive, but with this power comes complexity and likely a steep learning curve, The console lacks context-sensitive help. Help file documentation is available only in a PDF.
- Ad hoc reporting is not supported. Reports can be filtered but not changed, and it is not possible to drill down into details. No dashboard function is present.
- There is no significant native security state assessment beyond the EPP agent, and no significant integration with operations tools.
- It does not yet offer a client-based, content-aware DLP solution.

Sophos

Sophos is one of the few anti-malware companies dedicated to the enterprise market. It continues to execute well with strong product development and has one of the fastest large-company growth rates in this market. Improvements in v.10 introduced in 2011 focus on reducing the attack surface of endpoints using vulnerability analysis, as well as increasing the range and correlation of detection mechanisms, providing more opportunity to catch threats early. It should be considered a strong vendor that's suitable for all organizations, but particularly those that prefer simplified management capabilities.

Strengths

- Version 10 updated Sophos' integrated URL-filtering capability to block known malicious websites, as well as productivity filtering to block categorized websites.
- Sophos added vulnerability detection for a number of applications in v.10, allowing prioritized identification of vulnerable applications.

- Sophos provides basic application control capabilities that enable administrators to block installation of unwanted applications or application classes (for example, point to point [P2P] and remote access).
- Sophos continues to have a strong reputation for support and service from customers and its channel.
- Windows, Mac, Linux and Unix clients are all supported in the management console.
- Sophos also offers full-disk and file encryption, encryption key management, endpoint DLP, and very granular device control in its suite.
- Sophos recently completed the acquisition of UTM Gateway Astaro, which offers Web, email, wireless, and SSL VPN capability.
- Sophos offers a new MDM capability that includes a rich set of capabilities, including enterprise configuration remote locate, lock and wipe.
- For virtual environments, Sophos provides randomized scanning and updating, memory sharing, and encryption.

Cautions

- Its lack of consumer products has resulted in low brand recognition. The company must continue to focus on expanding its international channel and marketing.
- Although it does have a growing number of very large enterprise customers, and the management console is designed for ease of use and low administrator overhead, it lacks the depth of large-enterprise features. Policy development is eased with pop-up windows, check boxes or prepopulated menu lists, which can be limiting for more-experienced administrators. The dashboard is not very graphical, nor does it allow much customization or alerting capability. Dashboard elements were limited to the state of the EPP solution rather than more holistic state assessment. Vulnerability assessments were notably missing in the dashboard (it is found in the event viewer). It does not link directly to patch management systems. Reference customers found the reporting capability limited, although Sophos recently added export capabilities to Splunk and other tools, and an improved analytics capability is in the road map.
- Web productivity filtering in the endpoint is limited to 15 Web categories and has limited reporting and policy capability managed in the EPP management server. An additional 40-plus website categories with more granular reporting and management are available with the deployment of the secure Web gateway server.
- The application control capability is limited to blocking a specific set of unwanted but not malicious applications and caching verdicts on good applications for scanning speed. It would be difficult to lock down to a specific set of applications due to the lack of processes and workflow to allow for trusted change (due in 2H12).
- While Sophos' endpoint DLP is an integrated component of the EPP agent, DLP capabilities are weaker than vendors that specialize in the more comprehensive enterprise DLP market.
- MDM is in a separate Web-based management interface. It does not offer traditional anti-malware for mobile clients.
- Its virtual environments cannot scan offline images or gold images (due in 2H12).
- There is no integration or common management console between Astaro UTM products and the EPP suite.

Symantec

Symantec has a broad portfolio of security and information protection solutions including PC operations management, encryption, DLP, two-factor authentication, SIEM, significant marketing resources, a solid operations capability, and a strong malware research and management team. In 2011 Symantec released SEP 12, the first major new version since Symantec Endpoint Protection 11 (SEP 11) launched in 2007. This new version contains a number of security improvements. Symantec continues to be a solid Leader, based primarily on its solid test results and management capability. It should be considered a strong vendor that's suitable for any enterprise.

Strengths

- SEP is now on its second major release (v.12). The latest version introduces a new scan engine already in use in the consumer Norton solution. Two particularly notable new features for the enterprise are "Insight," which allows administrators to set policy for downloaded files based on the age and global prevalence of an application, and Sonar, which provides additional real-time behavior-based application and process monitoring. By reversing the paradigm to by default deny new unknown files, Insight is a very deterministic method of blocking polymorphic, targeted or zero-hour threat types from being accidentally or maliciously downloaded from the Internet.
- Symantec significantly eased the upgrade process in SEP 12 to make it similar to a release update.
- SEP 12 performs very well on dynamic tests of malware detection rates as well as performance impacts tests (see Note 1). SEP provides an integrated system lockdown capability to lock PCs down to known whitelists that can be created by inventory or a gold image.
- The Symantec management interface is very good and provides multiple advanced features such as virtual grouping, granular role-based policy, very granular location-based firewall policy, and excellent reporting capability. The Symantec Protection Center (SPC) ties its various security products together. SPC provides a Web portal to enable quick access to the underlying management consoles of DLP, Brightmail, Critical System Protection, Web Gateway and Endpoint Protection. It provides a very flexible analytics engine with dashboard views into each product and customizable reporting capabilities. Symantec offers a Small Business Edition that reduces complexity of the management experience for sub-100-seat environments, as well as a SaaS-based management console in Symantec.cloud.
- Symantec provides good port and device controls, mobile device synchronization, and the best firewall of any ranked vendor. Symantec has also made significant investments in encryption with the acquisition of Guardian Edge and PGP.
- Symantec covers the full range of endpoint and servers, and Symantec Mobile Management (SMM) is a new solution in the security portfolio designed to enable management and security of a fleet of mobile devices. Symantec Critical System Protection is a separate solution aimed at server protection, which is better optimized for the unique needs of server security functions than SEP.
- SEP 12 added several features to improve performance in virtual servers, including the capability to detect VIM machines, a shared insight cache, whitelisting of unchanged VIM files and resource leveling to avoid contention. Symantec also offers a command line offline image scanner tool.

- Symantec has a very strong enterprise DLP solution, which continues to rank very highly in the DLP Magic Quadrant (see "Magic Quadrant for Content-Aware Data Loss Prevention") and provides comprehensive enterprise DLP capabilities.

Cautions

- Symantec has made a number of visionary investments for its EPP solution; however, it has not provided fast integration of its various acquisitions. The SPC provides a common reporting engine; however, it does not replace the need for management servers, nor does it provide a common management framework that allows for policy objects to be used across products or a common user interface design. It also does not integrate the SaaS versions of products with their software counterparts.
- Symantec still has to integrate full-disk encryption into the SEP management server, although it has integrated it at a reporting level in SPC.
- Symantec has not done a good job of taking advantage of its PC life cycle tool capability (Altiris) for improved security.
- The MDM console isn't as attractive or user-friendly as competitors, and could use updating and better full-device life cycle administration.
- Port control capability is spread over multiple products (SEP, Encryption and DLP), which may create enforcement gaps and complicate management.
- Symantec Critical System Protection is a separate product from SEP 12, overlaps in some capabilities, and uses a different agent and management console, although it is integrated into SPC. It is primarily deployed in servers.
- SEP 12 does not have a flexible application control capability. Insight file reputation provides only limited indicators of what files are (source URL and application developer), nor does it allow for broad options for trusted sources of change (only signed applications). Insight only works as files are downloaded from the Internet or on scheduled scans.

Total Defense

CA spun its EPP product to a private equity firm in 2011. The new company is called Total Defense. CA's former development partner, HAL, continues to provide all product development, engineering, support and threat research. Total Defense's r.12 EPP solution remains very focused on core anti-malware prevention with very basic management capabilities.

Strengths

- The r.12 console is based on an Adobe Flex user interface and offers basic management and reporting capabilities. Notable features include the capability to stream alerts about critical external events and the ability to create a custom interface using a limited number of widgets and filters.
- The Total Defense firewall can enforce policies by network context, and it provides capabilities to set policies to defend or deny the operation of a new network interface, including restricting which ports and services are active.

- Total Defense's HIPS capability includes numerous system checks, as well as vulnerability shielding, sandbox execution and behavioral anomaly detection. Its learning mode capability eases setup and policy creation.
- The r.12 provides basic port and device controls, including control over USB, Bluetooth, CD, infrared device, DVD and floppy disk drives.
- Total Defense offers very broad platform support, including several varieties of Unix/Linux, Mac, Palm, Windows Mobile, VMware, Microsoft Hyper-V and Citrix presentation servers, as well as specialized servers, such as Microsoft Exchange, Lotus Notes/Domino, Novell NetWare, NetApp and EMC storage servers.
- Total Defense offers solid application control capabilities, with a large categorized database of known good applications.

Cautions

- The r.12 console is still lacking advanced features, such as extensive control over scheduled scans, flexible administrator role creation, flexible reporting, virtual groups, reporting on machine characteristics and more-actionable intelligence on the holistic state of an endpoint. Information presented in the dashboard is limited to the state of the EPP agent.
- Total Defense's lack of participation in multiple independent anti-malware testing makes it difficult to validate malware detection effectiveness. Total Defense lacks a comprehensive view of system events that would enable more holistic protection and management.
- The application control solution is basic, and lacks workflow and dynamic help desk and customizable end-user messages.
- Total Defense is lacking support for MDM, and there are no specific features or policy options for virtual environments.
- Total Defense lacks integrated full-disk/file encryption products, or DLP, and is unable to enforce encryption on data written to external storage devices.
- Reference customers were not enthusiastic in their endorsement of Total Defense, and specifically cited the need for better support.

Trend Micro

Trend Micro is the third-largest enterprise anti-malware vendor, with a significant market presence in Asia/Pacific and EMEA. Trend Micro offers integrated management of endpoint anti-malware, DLP and MDM in a single console. Trend Micro was one of the first vendors to optimize for virtualized environments. It also offers a very strong server protection suite. Trend Micro should be considered a strong vendor that's suitable for any enterprise.

Strengths

- Trend Micro's OfficeScan provides anti-malware, DLP and basic firewall and Web threat protection in a single product. It also offers an optional advanced deep-packet-inspection-based HIPS firewall (Intrusion

Defense Firewall) in a single agent and management interface. It also offers good mobile data encryption, as well as MDM.

- OfficeScan protection is bolstered by the capability to block malicious URLs at the client level, critical system resources and process protection, which blocks malicious changes and behavioral monitoring.
- Trend Micro was the first vendor to introduce a cloud-based signature capability — the Smart Protection Network. This network of cloud-based data centers allows clients to perform real-time queries of global signature and Web reputation databases to get the very latest reputation information.
- OfficeScan provides a virtual desktop infrastructure (VDI)-aware solution (Citrix and VMware). This improves performance and security by preventing resource contention, and by leveraging base image prescanning to avoid duplicate scanning among multiple virtual desktop images, which has a significant impact on VDI density. Its server protection solution, DeepSecurity, provides an agentless VM solution.
- Trend Micro offers a SaaS-based management console.
- Trend Micro offers broad platform coverage for endpoints and servers, including native Mac support, mobile device protection, Microsoft SharePoint, Microsoft Exchange and network-attached storage in a single management console.
- The administrator console can be reconfigured with customized graphics, colors, layout and displayed elements. If a company has multiple monitor sites, this interface allows them to be viewed in separate frames under common management. Policy templates are also good and include choices such as on-network, off-network and PC interface.
- A new cloud service — SafeSync — provides protected file sharing and can be policy linked to parts of the Trend Micro endpoint security suites, such as mobile data protection. Trend Micro also offers full-disk, and file and folder encryption, as well as basic channel DLP capabilities suitable for compliance.
- Trend Micro offers a unique threat management service, which combines out-of-band VMware servers that monitor networks for malicious traffic with a service-assisted remediation and incident management service to its premium support customers. It also offers it as a stand-alone solution to monitor incumbent EPP solution effectiveness.

Cautions

- The management interface is sometimes clumsy and requires too many pop-up notifications and confirmation steps. It doesn't yet have the richness of reporting or dashboards that other solutions do. Rogue client detection is a manual process.
- Trend Micro product management has not embraced PCLM integration, nor appreciated the value of more-holistic security state assessments or application control. Trend Micro has licensed its OfficeScan engine to IBM, which provides some of this capability.
- OfficeScan provides few application control capabilities. However, the Intrusion Defense Firewall plug-in can control applications at the network level, but can't block specific controls from running in a browser and is an additional charge. However, execution and firewall behavior rules are in different policy settings, complicating management. For practical purposes, most buyers will set controls by individual application and will find this method to be hard to scale.

- OfficeScan port and device control capabilities are very limited, granting just read-only or executing control on storage devices. The advanced firewall and device control features available in the IDF and DLP plug-ins are much more extensive than those included in the base OfficeScan client. In particular, the Advanced Device Control capabilities of the DLP plug-in provide administrators granular control over device access and functions.
- Its endpoint DLP is weaker than vendors that specialize in this market. Trend Micro is not a major vendor in the more comprehensive enterprise DLP market.
- OfficeScan uses a different agent, management console and reporting framework than Trend Micro's server-targeted offering, DeepSecurity. For hosted virtual desktops, either could be used. However, only DeepSecurity offers agentless anti-malware scanning, but requires a different console than physical desktops.
- 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. In general, Trend Micro has a long way to go to build North American brand awareness. Clients tend to regard Trend Micro as only a supplier of basic antivirus applications.

Vendors Added or Dropped

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

Added

F-Secure returns to the Magic Quadrant this year. CA spun its EPP solution out to Total Defense, and that product appears under the new company name.

Dropped

CA spun its EPP solution out to Total Defense, and that product appears under the new company name.

Inclusion and Exclusion Criteria

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

- Detection and cleaning of malware (for example, viruses, spyware, rootkits, trojans, worms), a personal firewall, and HIPS for servers and PCs.
- Centralized management, configuration and reporting capabilities for all products listed here, which are sufficient to support companies of at least 5,000 geographically dispersed endpoints.
- Global service and support organizations to support products.

Evaluation Criteria

Ability to Execute

The key Ability to Execute (see Table 1) criteria used to evaluate vendors were overall viability, market responsiveness and track record. These criteria were evaluated for their contribution to the vertical dimension of the Magic Quadrant:

- **Overall Viability:** This included an assessment of financial resources (such as the ability to make necessary investments in new products or channels), and the experience and focus of the executive team. We also looked at the business strategy of each vendor's endpoint protection division and how strategic it is to the overall company.
- **Market Responsiveness and Track Record:** We evaluated each vendor's track record in bringing new, high-quality products and features to customers in a timely manner.
- **Sales Execution/Pricing:** We evaluated the vendor's market share and growth rate. We also looked at the strength of channel programs, geographic presence, and the track records of success with technology or business partnerships.
- **Marketing Execution:** We evaluated the frequency of vendors' appearances on shortlists and RFPs, according to Gartner client inquiries, as well as reference and channel checks. We also looked at brand presence and market visibility.
- **Customer Experience:** We primarily used reference customers' satisfaction scoring of the vendor in an online survey and data received from EPP vendor reference customers and resellers and Gartner clients during our inquiry process to score vendors on customer satisfaction with the company and the product.
- **Operations:** We evaluated companies' resources that were dedicated to malware research and product R&D.

Table 1. Ability to Execute Evaluation Criteria

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

Source: Gartner (January 2012)

Completeness of Vision

The most important vision criteria in this analysis (see Table 2) were market understanding and the sum of the weighted offering/product strategy score:

- **Market Understanding:** This describes the degree to which vendors understand current and future customer requirements, and have a timely road map to provide this functionality.
- **Offering (Product) Strategy:** When evaluating vendors' product offerings, we looked at these product differentiators:
  - **Anti-malware Detection and Prevention Capabilities:** This is the speed, accuracy, transparency and completeness of signature-based defenses, as well as the quality, quantity, accuracy and ease of administration of non-signature-based defenses and removal capabilities for installed malware. We looked at test results from various independent testing organizations and used Gartner inquiries as guides to the effectiveness of these techniques on modern malware.
  - **Management and Reporting Capabilities:** This is comprehensive centralized reporting that enhances the real-time visibility of end-node security state and administration capabilities, which eases the management burden of policy and configuration development. Vendors that have embarked on PCLM-style operation integration showed considerable leadership and were given extra credit for showing up positive on this criterion.
  - **Application Management Capability:** We looked for the ability to provide a holistic state assessment of an endpoint security posture, and prioritized guidance and tools to remediate and reduce the potential attack surface. This capability includes configuration management, vulnerability management and integration with patch management tools. We also looked for the capability to apply a flexible default deny-application control policy that allows for trusted sources of change and can handle requirements ranging from full lockdown to allowing any trusted application to run.
  - **Data and Information Protection:** This is the quantity and quality of integrated technology to protect data that resides on endpoints, such as full-disk encryption and data leak prevention. Although we have argued that these technologies aren't mandatory requirements of every buyer, they do demonstrate vendor vision and leadership in this market.
  - **Device and Port Control Capabilities:** We explored the granularity and integration of policy-based controls for a broad range of ports and peripheral devices, such as USB and printer ports. We looked for granular control of a range of device types, interaction with encryption and DLP policy, and convenience elements, such as end-user self-authorization options.
  - **Supported Platforms:** Several vendors focused solely on Windows endpoints, but the leading vendors are able to support the broad range of endpoint and server platforms typically found in a large-enterprise environment. In particular, we looked for support for virtualized environments, and Mac and mobile devices as well as specialized servers, such as email and collaboration servers.
- **Sales Strategy:** We evaluated each vendor's licensing and pricing programs and practices.
- **Innovation:** We evaluated vendor responses to the changing nature of customer demands. We accounted for how vendors reacted to new malicious code threats, such as spyware and advanced persistent threats, 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.

Table 2. Completeness of Vision Evaluation Criteria

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

Source: Gartner (January 2012)

Quadrant Descriptions

Leaders

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

Challengers

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

Visionaries

Visionaries invest in the leading-edge (aka "bleeding-edge") features — such as advanced malware protection, data protection and/or management capabilities — that will be significant in the next generation of products, and will give buyers early access to improved security and management. Visionaries can affect the course of technological developments in the market, but they haven't yet demonstrated execution. Clients pick Visionaries for best-of-breed features, and in the case of small vendors, clients may enjoy more personal attention.

Niche Players

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

Context

Malware protection is still the key requirement of EPP; however, blacklisting and behavior-based solutions are failing to adequately protect endpoints.

Protection from highly targeted, new and low-volume attacks requires a more proactive approach grounded in solid operations management processes such as vulnerability analysis, patch management and more-precise application management control.

Some solutions are getting better at providing more-holistic security state assessments of endpoints. This enables prioritized activities to lower the attack surface. These solutions, however, are still maturing.

Integrated protection and management for the increasing array of mobile devices such as tablets and smartphones are still rare, but will be critical future capabilities as these endpoint types receive more business use.

Performance in a virtual environment is an increasingly common RFI requirement that several vendors are starting to address.

Server platforms are commonly supported by EPP vendors; however, optimal server protection may require additional solutions or the selection of an alternative solution or vendor.

Market Overview

We continue to view the protection from malware as a primary purpose of the EPP solution, and this year, we focused our analysis on features or enhancements that result in higher detection rates or improved ability to reduce the attack surface on endpoints.

Improvements in malware scanning engines primarily focused on performance of the scanning engine, broader signatures to catch family threats and improving the value of cloud-based look-ups. As polymorphism techniques continue to improve and targeted threats rise, threat labs are focusing on creating accurate signatures that are precise enough to provide a low number of false positives, but broad enough to catch new variants of old threats. Behavior protection is also useful in detecting new variants. Cloud look-up capabilities, first introduced by Trend Micro, are maturing and beginning to collect more metadata about files and behavior Threat labs are also increasingly collecting information about good as well as bad files to reduce false positives, improve scanning performance and provide a foundation for default deny application control policy.

Vendors are also starting to invest in tools and processes to provide more proactive protection. Several vendors (McAfee, Lumension Security, LANDesk, Kasperksy Lab and Total Defense) have introduced or improved application control capability to lock devices down to run only a set of known good applications. Vulnerability detection and patch management also offer a foundational way to prevent malware from exploiting known application flaws, because the best way to prevent malware is to close the vulnerability hackers are targeting. Sophos, eEye Digital Security and Kaspersky Lab added or improved vulnerability detection capability. Microsoft integrated directly with SCCM this year to reduce complexity and take advantage of underlying operational infrastructure. Microsoft, LANDesk, IBM-BigFix and McAfee now integrate security directly with operational tools. The integration of these tools is a welcome trend, because they can help security operations teams get a more holistic state assessment of the endpoint and perform fast remediation to reduce the attack surface of endpoints. Many of these tools and integration points, however, are not well-instrumented or efficient. We hope to see improvement next year as these tools get field-tested.

As mobile devices become more capable, we see protection for these devices as becoming a key future requirement of EPP. While several vendors have anti-malware engines for Android and Windows Mobile, what most buyers are interested in is integrated mobile device security management capabilities (for example, ensuring the device is password-protected, is encrypted, can be remotely wiped if the device is lost or stolen, and checking to see if the device has been jailbroken). Indeed, we anticipate that future EPP will closely resemble today's MDM platforms; they will be capable of monitoring as well as managing a diverse array of endpoints from tablets to VDI, and they must be capable of enabling native security functions in hardware and operating systems, and adding new functionality where native capabilities are lacking. There are more than 100 vendors at play in the MDM space, and Symantec, McAfee, Sophos, and Trend Micro are developing a standing in that market. Yet, few vendors have really integrated full MDM capabilities with EPP management. We believe future organizations will want the same teams to manage and secure all endpoints.

Because most malware comes from the Web, several solutions have improved Web protection techniques, mostly by using URL filtering capabilities to block suspicious, low-reputation websites. However, some products also perform JavaScript and Web page analysis. Several vendors now offer visual indicators of website reputation, either in search results or in the browser itself, as a way to educate end users about potentially malicious websites. Blocking all communication with malicious sites is a much more proactive and effective way to block malware early in the infection chain than attempting to block the threat with a signature during infection.

Server protection capabilities are also of interest to clients. While all of the EPP solutions evaluated in this Magic Quadrant support running on generic Windows servers, several of the vendors — Symantec, Trend Micro and IBM have offerings specifically targeted at server platforms that include capabilities such as file integrity monitoring and vulnerability shielding. However, these tools often require a different product and management console than endpoints. Ideally, EPP vendors should offer the capability to protect a desktop, laptop or server from a set of commonly managed controls, and let the organization decide what mix of controls is best suited to protect a given device in its expected usage scenario (see "How to Devise a Server Protection Strategy").

As server virtualization and hosted virtual desktops become more common, EPP solutions are increasingly adapting to the needs of these environments. While most solutions will run in a virtual guest environment without modification, the performance impact, especially of scheduled scans, will affect the density of guest VMs per server. Techniques such as randomized scanning, scanning of offline guests, scanning gold images, scan result caching, and random signature updates provide improved performance in virtual environments. Several vendors have added or improved these techniques this year (Trend Micro, McAfee, Symantec and Sophos). Integration with virtualization management consoles such as VMware's vSphere vShield Endpoint (see "VMware Pushes Further Into the Security Market With Its vShield Offerings") can also ease management, but this capability is very rare. Native integration with a hypervisor using "introspection" (see "Radically Transforming Security and Management in a Virtualized World: Concepts" and "Radically Transforming Security and Management in a Virtualized World: Considerations") offers the possibility of "agentless" anti-malware scanning. Multiple vendors have this on their road maps; however, only Trend Micro has shipped clientless capabilities that would reduce the footprint of anti-malware engines in each guest by taking advantage of VMware's vShield Endpoint introspection APIs.

Note 1 Performance/Malware Detection Testing

Good performance and malware detection testing information is available from PassMark Software (antivirus-comparatives and antivirus-test), Virus Bulletin and NSS Labs.

Ability to Execute

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

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

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

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

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

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

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

Completeness of Vision

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

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