G00239869

Magic Quadrant for Endpoint Protection Platforms

Published: 2 January 2013

Analyst(s): Peter Firstbrook, John Girard, Neil MacDonald

The endpoint protection platform provides a collection of security utilities to protect PCs and tablets. Vendors in this market compete on the quality of their protection capabilities, the depth and breadth of features, and the ease of administration.

Strategic Planning Assumption

By 2017, more than 50% of end-user devices will be restricted to running only apps that have been preinspected for security and privacy risks, up from 20% today.

Market Definition/Description

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, also known as mobile data protection
- Endpoint data loss prevention (DLP)
- Vulnerability assessment
- Application control (see Note 1)
- Mobile device management (MDM)

These products and features are typically centrally managed and ideally integrated by shared policies.

DLP, MDM and vulnerability assessment are also evaluated in their own Magic Quadrant or MarketScope analyses. Longer term, portions of these markets will get subsumed by the EPP market, as the personal firewall, host intrusion prevention, device control and anti-spyware markets have in the past. EPP suites are a logical place for convergence of these functions. Indeed, 53% of organizations in a recent Gartner survey[1] already use a single vendor for several of these functions, or are actively consolidating products. In particular, mobile data protection is the leading complement to EPP and purchasing decisions regarding the two products are increasingly made together. For most organizations, selecting a mobile data protection system from their incumbent EPP vendors will meet their requirements.

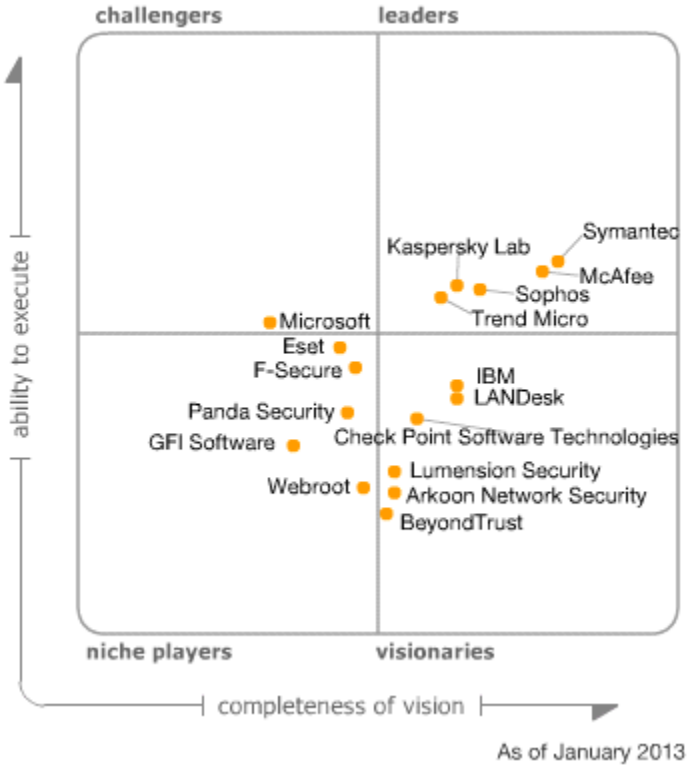
In 2012, the large enterprise EPP market is still dominated by Symantec, McAfee and Trend Micro, which together represent approximately 68% of the total revenue of Magic Quadrant participants. Sophos and Kaspersky Lab are the two other global leaders that are competitive across multiple functions and geographies, and push the combined Leaders quadrant market share to 85%. 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 to invest in new features and functionality (sometimes via acquisitions) to stay ahead, and to keep pricing rational. In the less demanding small and midsize market, competition is more intense. A number of Niche Player solutions are dominant in specific regions.

The total EPP revenue of the Magic Quadrant participants at year-end 2011 was roughly $2.8 billion, up 4% from 2010. We attribute this growth primarily to increased buying of more-expensive suites, offset by lower prices for low-end malware-only solutions. Consequently, EPP revenue growth is more a result of an inflow of revenue from other markets. We anticipate that growth will continue to be in the low single digits in 2013.

Microsoft is the best vendor in a position to challenge the incumbent Leaders, primarily due to attractive pricing in its enterprise agreements. Approximately one-third of enterprise buyers[1] indicate they are actively considering Microsoft or plan to do so during their next renewal periods. However, Microsoft's slow development, the lack of a single unified security management interface and mediocre test results will temper its adoption. Longer term, we believe that increased displacement of Windows endpoints with application-controlled OSs (such as Microsoft WinRT and Apple's iOS and OS X Mountain Lion) is the biggest market threat. These solutions shift the value proposition of EPP solutions from traditional anti-malware to MDM and data protection capabilities.

Magic Quadrant

Figure 1. Magic Quadrant for Endpoint Protection Platforms



Source: Gartner (January 2013)

Vendor Strengths and Cautions

Arkoon Network Security

Arkoon Network Security's StormShield EPP solution (formerly offered by SkyRecon Systems) is designed as a seamless integrated EPP with a focus on behavioral protection. Arkoon's Ability to Execute score is hampered by its relatively small market share and limited geographic presence, as well as its still-maturing management capabilities. StormShield EPP is a reasonable shortlist solution for organizations that are in supported geographies seeking a behavior-based approach to malware detection, and for those that are willing to invest extra effort to administer the advanced capabilities of the offering.

Strengths

- The vendor'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 a host-based intrusion prevention system (HIPS), a personal firewall, device control, encryption, and an optional, fully integrated signature-based, anti-malware engine licensed from Avira. The suite boasts a single lightweight agent (15MB, including anti-malware protection) that is extensible to support multiple functions and runs at the kernel level.

- We particularly like Arkoon's focus on advanced behavioral-based HIPS techniques, such as memory overflow protection, anti-keylogging, application control, rootkit detection, honey pots, privilege escalation, reboot protection and driver management. Remediation and status assessment are enabled with administrator-generated scripts.
- StormShield 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 blacklisting/whitelisting 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.
- Full-disk encryption and encryption for files and folders on fixed hard drives and removable devices is available. Recent improvements include support for fully encrypted logical containers in addition to per-file encryption.
- Arkoon has created a bundled mobile data protection product that includes Security Box and StormShield, but without any technical integration.

Cautions

- Although it continues to grow rapidly, StormShield has a very small market share in this Magic Quadrant. Neither SkyRecon nor its parent company Arkoon has significant brand recognition or a significant enterprise client base outside of Europe.
- StormShield does not participate in any of the prominent endpoint protection malware tests, so it is difficult to compare its malware detection performance against other solutions in the market.
- StormShield supports Windows only, and provides no Mac, Linux, Unix, mobile or email server support. Although it works in a virtual machine (VM) environment, there are no features specific to virtualization.
- The full-disk encryption product is immature, compared with those offered by the Leaders in this Magic Quadrant.
- Application control is suitable for allowing or blocking specific applications, or completely locking clients down, but it does not have workflow features or an application database that would allow a flexible application control environment.
- The only option for signature-based anti-malware protection is from Avira. Arkoon has a very small malware research team and is dependent on Avira for signature-based protections.
- The management interface is comprehensive, but not recommended for nontechnical users. The console lacks dashboards and context-sensitive help. Much of the advanced capability is achieved by administrators creating their own scripts.

- Ad hoc reporting is not supported. Reports can be filtered, but not changed, and it is not possible to drill down into details.
- There is no out-of-the-box security state assessment beyond the EPP agent status, and no significant integration with operations tools, such as vulnerability.
- The vendor does not yet offer a client DLP solution.

BeyondTrust

BeyondTrust acquired eEye Digital Security in May 2012, and plans to combine eEye's vulnerability analysis and endpoint protection with its privileged management solutions. Current Beyond Trust and eEye Retina customers and enterprises that value integrated vulnerability analysis should consider BeyondTrust's eEye Blink.

Strengths

- The management console of eEye Retina and eEye Blink is a 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, and additional reporting modules for compliance, configuration and patching. It also provides integration into Microsoft System Center.
- BeyondTrust enables the removal of Windows administrator rights while still selectively escalating privileges for legacy applications. It also provides tools for database monitoring and endpoint DLP.
- In addition to licensed anti-malware signature libraries from Norman, BeyondTrust now has a small, but very skilled, team of malware experts that provides excellent technical support and malware information.
- The anti-malware techniques include process execution rules, registry protection and file integrity monitoring.
- BeyondTrust is one of the few providers in this Magic Quadrant 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.
- BeyondTrust PowerBroker Mobile offers cloud-managed MDM, and Retina can provide a mobile vulnerability scan.

Cautions

- Prior to the acquisition, eEye was growing quite rapidly, however it had a very small market share in the EPP market, and did not come up in calls with Gartner clients often. eEye was one of the smallest vendors in this market. Its total staff size, including the research and engineering groups, was small compared, with the EPP industry average. Most of its installed base is in North America.

- The vendor's solution has the capability to blacklist applications, but it is a manual process with no trusted sources of change, not a full application control solution.
- BeyondTrust PowerBroker Mobile is in a separate, cloud-based management interface.
- Although the Blink team develops its own signature spyware database and cleanup routines, the solution relies on Norman for anti-malware signatures; therefore, business disruptions at Norman could impact Blink customers. Although the Norman anti-malware engine is tested regularly, Blink does not participate in any industry tests (other than the Virus Bulletin's VB100 test) to demonstrate the effectiveness of its collection of technologies. Automated malware damage cleanup capabilities are limited.
- Blink has limited device control capabilities and no encryption capabilities. It lacks the ability to enforce encryption on data that is written to external storage devices, but it does have a number of policies to limit access and writing to external devices.
- Blink supports only Windows OS desktop and server platforms (including Microsoft Internet Information Services [IIS]).
- The anti-malware agent works on a virtualized Windows host. However, it is not optimized for a virtualized environment.

Check Point Software Technologies

Check Point Software Technologies is a well-known, long-term network security company. It will appeal to organizations that value strong integration between remote access solutions, full-disk and media encryption, and the EPP suite.

Strengths

- Check Point offers selective activation of capabilities packaged as "software blades." Blades include a personal firewall, anti-malware (licensed from Kaspersky Lab), full-disk encryption, network access control (NAC) and an integrated VPN.
- Check Point's endpoint management console offers a clean interface with easy navigation and quick access to summary data. The dashboard can be customized for each administrator. Administrators may develop and view user-specific policies across multiple devices.
- In April 2012, Check Point launched ThreatCloud, which compiles a database of known Internet Protocol (IP) addresses that distribute malware, plus URLs and signatures of malicious applications.
- Check Point's Mobile VPN supports iPhone, iPad and Android mobile devices, and manages Exchange email synchronization.

Cautions

- Despite its significant enterprise network presence, brand and channel, the vendor has failed to significantly improve its market share or mind share in the EPP market, beyond its installed

base of VPN, host firewall and encryption customers. Gartner clients rarely inquire about Check Point's EPP solutions, nor does Check Point appear in competitive reviews from other sources.

- Check Point's dependence on Kaspersky Lab's engine and signature updates continues to challenge enterprise buyers to differentiate it from Kaspersky Lab, which is rapidly adding other competitive features.
- Check Point views MDM as a network manager's tool; consequently, MDM capabilities are in the SmartDefense dashboard, not the EPP dashboard.
- Check Point protection is oriented to Windows endpoint PCs. Not all software blades are available for OS X, and it doesn't offer protection for specialized servers, such as Microsoft Exchange, SharePoint or Lotus Notes.
- Although its agent will run in VMs, Check Point has no specific optimization for virtualized environments.
- Check Point's application control capabilities (which it calls "program control"), augmented with its Program Advisor service, are suitable for blocking or allowing a specific set of applications, but do not provide a manageable default deny application execution environment.
- Check Point does not currently offer integrated network and endpoint DLP, but is pursuing a 2013 road map in response to customer interest.

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 investment 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 solution.

Strengths

- The flagship enterprise product, Eset Endpoint Security, includes integrated anti-malware, anti-spam, HIPS, device control, Web content filtering and a personal firewall in a single-agent footprint. Installation can be tailored to specific needs by selecting only the modules that are desired.
- The low performance impact of the Eset product has been noted by many customers.
- Its 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. The vendor recently introduced Eset Live Grid, a cloud-based reputation service.
- The vendor supports a broad range of Windows clients and servers, including Exchange, Lotus Notes/Domino, Linux, and Novell NetWare and Dell storage servers; mobile devices (Windows

Mobile, Android and Symbian); and Apple OS X and Linux desktop platforms. In December 2012, the vendor launched Eset Endpoint Security for Android phones and tablets.

- Eset offers a limited MDM solution with the launch in 2011 of Eset Mobile Security Business Edition for Windows Mobile and Symbian. Eset recently launched Endpoint Security for Android.

Cautions

- The management interface is adequate, but it is still a Win32 application. Eset has a great point-in-time system inspector function, Eset SysInspector, but it cannot store historic asset information, nor does it provide any vulnerability or configuration information that would aid in security state assessments that go beyond AV status. A separate Web-based dashboard provides a flexible customizable reporting interface, but it does not allow for direct drill-down into the management console.
- Eset is reluctant to advance to data protection with encryption or DLP solutions.
- Removable media/port protection is a good addition, but policy is complicated by drop-down menus making it awkward, and a lack of encryption means policy cannot include the option to encrypt data on removable media.
- 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.
- Heuristics can add a performance impact, especially on older PCs, although it is not turned on by default.
- Eset doesn't yet offer application control.
- Although Eset Endpoint Security operates in a virtual environment and has a low system impact, it has not been optimized for these environments.

F-Secure

F-Secure, a veteran of the anti-malware industry for more than 20 years, has a very good track record for malware testing results. The vendor 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 has consistently good malware test results and performance tests. It provides cloud-based look-ups and a file reputation feature, which considers file metadata (such as prevalence, source and age) before allowing files to execute. We particularly like the sandbox environment for behavior testing on Windows clients, which tests unknown applications in a virtual sandbox for malicious behavior.
- The vendor offers one of the better rootkit detection and removal tools, called BlackLight.

- F-Secure client agents are lightweight, with minimal performance impact.
- Basic device control functionality was recently introduced.
- F-Secure has mobile clients for Android, Research In Motion, Symbian and Windows Mobile, and a cloud-based MDM capability primarily aimed at SMBs. It also offers protection for a broad range of Linux variants and Mac platforms.

Cautions

- F-Secure has very little presence or brand recognition in markets outside of Northern Europe. It has a minimal market share, despite its long-term presence in the market, and it is growing much slower than the overall market.
- Although F-Secure develops some its own signatures and behavioral detection techniques for advanced threats, its solution relies heavily on Bitdefender for the majority of anti-malware signatures; business disruptions at 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 security state or asset information beyond anti-malware status, and does not provide any significant customizable dashboard capability or any drill-down into remediation capability. Autodiscovery of new unmanaged agents and Active Directory synching is partly a manual process and can't be scheduled, although automation exists for importing new agents and removing inactive agents. The reporting capability is very basic and does not allow for ad hoc reporting.
- F-Secure does not offer encryption or DLP capability. Device control is basic. It does not offer any application control capability.
- MDM capability is not integrated into the endpoint management console. Mac clients are not managed in the same console as Windows clients.
- F-Secure does not provide any protection for SharePoint servers (this is due in 1H13).
- Virtualization support is limited to optimization of the AV clients with randomization of scheduled tasks.

GFI Software

GFI Software has a portfolio of security offerings targeted at SMBs. It has expanded its Vipre Business offering during the past year, integrating patch management and MDM capabilities. GFI is squarely aimed at the SMB market, where ease of use and "set and forget" functionality are sought-after attributes. The vendor should be considered by SMBs looking for straightforward and easily managed anti-malware protection with a low performance impact.

Strengths

- The GFI Vipre console is straightforward and easy to use, and provides consistent management across Windows and Mac clients, as well as email anti-malware scanning.
- The latest version of Vipre Business Premium includes integrated PC application patch management capabilities from the GFI LanGuard offering, which will appeal to organizations that have no other solution for patch management.
- The latest versions of Vipre Business Premium and Vipre Antivirus Business include MDM capabilities for Android and iOS, also using the same integrated console.
- GFI offers a free, Web-hosted malware analysis engine that provides immediate forensic feedback on submitted application files.
- Signature-based anti-malware scanning is augmented with GFI's MX-Virtualization sandboxing technology, which analyzes malware in real time within a partitioned environment on the PC.

Cautions

- Network discovery of machines without agents uses NetBIOS or Active Directory, which limits discovery of devices to Windows-only devices.
- GFI's patch management capabilities are limited to Windows and Windows applications. Mac OS is on its road map.
- A device control solution is available separately for an additional cost; however, it uses a different management console, and GFI offers no option for full-drive encryption.
- Other than Exchange email filtering, GFI offers no DLP capabilities.
- GFI has no application control capabilities.
- GFI offers no specific integration with VMware's vShield APIs, although scanning can be randomized to reduce loading.
- The agent would benefit from better tamper protection.
- MDM capability is limited.

IBM

IBM's EPP offering is built on the foundation of its strong client management tool platform, the Tivoli Endpoint Manager (TEM; formerly BigFix). The core malware engine (now called TEM for Core Protection) is provided by Trend Micro, and advanced HIPS capability is provided by Proventia (formerly ISS). These tools are augmented with IBM's X-Force research labs. Large organizations that are considering IBM for client management tools or those looking at Trend Micro should include IBM on their shortlists.

Strengths

- TEM provides a converged endpoint management and security operations console that supports large enterprise needs across multiple endpoint types, including mobile devices.
- TEM for Security and Compliance offers fully integrated patch, configuration and vulnerability management, as well as the ability to monitor other EPP agents, such as McAfee, Symantec and Microsoft.
- TEM for Mobile Devices enables unified MDM of iOS, Android, Windows Phone, Windows Mobile and Symbian devices with the same management infrastructure. Services include inventory profile management, remote locate and wipe, and app deployment. IBM is rated a Visionary in the MDM software Magic Quadrant.
- Add-on components include TEM for Data Protection, which provides port/device control and DLP. Application control is offered via Bit9 integration with the TEM platform.
- The security and compliance analytics Web interface can establish and monitor built-in and admin-created key performance metrics and show compliance over time.
- The IBM Global Services group offers a mature managed security services.
- IBM server protection products boast very broad server support for Windows, Linux, HP-UX, Solaris and AIX, including 64-bit support for Windows and Linux, and new AIX 6.1 support.

Cautions

- IBM is starting to show some traction in this market; however, mind share for this solution, as represented by Gartner client inquiries, is still very low, despite IBM's obvious size and channel advantages.
- IBM appeals mostly to very large enterprise customers that value the integration of operations and security. The Win32 console is complicated and is not designed for nontechnical users.
- The vendor has a large and somewhat confusing product portfolio in this market, and prospective customers must carefully match desired features with specific product offerings. The complete suite is expensive.
- The TEM console is very powerful, and has more reporting and management capabilities than most EPP security solutions; however, it is still not fully optimized for the security role.
- TEM for Core Protection does not provide AV for Exchange, SharePoint, Lotus Notes and other specialized servers.
- Although IBM has its X-Force security analysis team, it is dependent on Trend Micro for its broad signature database. Disruptions at this critical partner could have an impact on IBM's customers. Integration of the latest Trend Micro engine into the TEM client can take a few 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 its large European installed base, improving its ability to execute. The vendor continues to broaden its offering with internally developed features that are tightly integrated into the client and management console, allowing for cross-feature policies. At the same time, Kaspersky Lab continues to perform very well in malware effectiveness testing. Organizations looking for an alternative vendor to the traditional market leaders should evaluate this vendor.

Strengths

- The MMC management console is comprehensive and offers granular control and policy. The dashboards can be customized with predefined graphs and are task-oriented. We particularly like the security status dashboard, which rolls up warnings of vulnerability, AV client status, infection information, network events and OS error reports.
- Kaspersky is building out an impressive array of traditional client management tools, including vulnerability analysis, patch management, application inventory, application control and MDM.
- Kaspersky Mobile Security provides MDM capability and security agents for mobile clients. Advanced functionality includes Web threat protection, application control and jailbreak detection.
- Application control capabilities provide a fully categorized application database and trusted sources of change, as well as offering client-level Web filtering for managing websites and Web applications.
- Kaspersky Lab is introducing centrally managed file-level and full-disk encryption with preboot authentication for hard drives and removable devices, integrated with endpoint security policies and application and device controls.
- Device control capabilities are very detailed. The solution was recently improved with the addition of integrated files, removable media and a full-disk encryption solution. Encryption is integrated into device control policy to optionally force encryption on removable media.
- The malware research team has a well-earned reputation for rapid and accurate malware detection. The vendor 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.
- The agent has a small disk and memory footprint for an integrated solution, and signature updates are small and frequent.
- Kaspersky Lab offers broad endpoint platform support, including an agentless VMware vShield solution with an intrusion prevention system/intrusion detection system (IPS/IDS) using VMware Network Extensibility (NetX) technology, all managed by Kaspersky Security Center.

Cautions

- Kaspersky Lab's client management tool features (such as vulnerability and patch management) are still maturing and are not replacements for enterprise solutions. However, they are good for the enterprise security practitioner to validate operations, or to replace or augment SMB tools.
- The vendor has added numerous new capabilities to its MMC management console, making it significantly more complex for less technical small business users, although it is possible to hide unused functionality in the Kaspersky Security Center management console.
- Kaspersky Lab doesn't yet offer DLP.
- Security products for Exchange and Forefront Threat Management Gateway have their separate management servers and are not integrated with other Kaspersky Lab products.

LANDesk

LANDesk is a pioneer in the integration of client management tools, MDM and security. Its solutions target organizations that want to leverage endpoint management infrastructures to manage desktop security capabilities. LANDesk has several native security features, but it is largely reliant on partners Kaspersky Lab and Credant Technologies (recently acquired by Dell) for anti-malware and encryption. LANDesk Security Suite is an excellent choice for the vendor's current customers, and a good shortlist candidate for enterprises seeking integrated security and operations.

Strengths

- The LANDesk console is comprehensive and provides the ability to view IT operational dashboards, alongside security-related dashboards, in a browser or native iOS app.
- The LANDesk agent has a single, modular architecture so that security functionality (such as anti-malware) can be activated as needed. Policy is very object-oriented, and reuse is common.
- Automated provisioning and state management is particularly useful to easily reimage PCs in the case of pervasive malware.
- The vendor acquired MDM provider Wavelink to enable management of security functions for iPads, Android and other mobile device platforms, and LANDesk is rated a Niche Player in the MDM software Magic Quadrant.
- The base LANDesk Security Suite includes an anti-spyware signature engine (from Lavasoft), a personal firewall, HIPS, device control and file/folder encryption, vulnerability and configuration management, patch management, and limited NAC capabilities. Customers can use LANDesk to manage McAfee, Symantec, Sophos, Total Defense and Trend Micro solutions, or they may choose to pay extra for LANDesk Antivirus, which leverages an integrated Kaspersky Lab malware scan engine. It can also manage the Windows firewall.
- The LANDesk Security Suite also includes an integrated full-drive encryption option, licensed from Credant, and it can also centrally manage Microsoft BitLocker through the LANDesk console.

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

Cautions

- Despite several years in the security market, LANDesk's market share and mind share remain very low.
- LANDesk doesn't perform its own malware research, although it does have engineers researching and creating content and compliance standards. The LANDesk Security Suite relies on Trend Micro to review suspicious code samples and prepare custom signatures for targeted malware samples. Although signatures are becoming a replaceable commodity, business disruptions at 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. There's no malware support for Unix, Linux, SharePoint, Lotus Notes and Android, or for Windows Mobile clients. Macintosh platforms benefit from client management tools, but AV is supplied by a Kaspersky-branded solution.
- LANDesk needs to expand its application control capabilities with better workflow and an application database.
- LANDesk doesn't offer client-based, content-aware DLP.
- Customer feedback indicates that the LANDesk console dashboard and reporting are designed from an operations perspective, versus a security-oriented focus.
- While LANDesk can discover and inventory VMs and its agent will run within a VM, it has no specific optimization for anti-malware protection in virtualized environments.

Lumension Security

The Lumension Endpoint Management and Security Suite (LEMSS) is delivered as a single-server, single-console, single-agent architecture that includes AV, application control, encryption, device control, patch management and remediation. The vendor recently acquired leading application control vendor CoreTrace to improve the application control capabilities of the LEMSS platform. Current Lumension customers, or those seeking integrated solutions for security, operations and compliance, should add the vendor to their shortlists.

Strengths

- The Web-based console manages all client management tools, with similar task-based orientation and consistent navigation. The full capability is delivered by a single-agent footprint, and individual modules can be licensed and delivered as pluggable services in the agent.
- The anti-malware engine is licensed from Norman, and includes sandbox capability that intercepts and prevents changes to host files, registry settings and other malicious changes.

- Application control capabilities benefit from a cloud-based file reputation service.
- Lumension Device Control is a complete solution for managing and restricting USB and other ports.
- Lumension resells Sophos SafeGuard Easy full-disk encryption.
- LEMSS provides a generic framework for the management of third-party security agents, such as Windows firewalls.

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 fewer than 500 seats.
- The pricing structure makes the vendor too expensive for users with competitive patch management solutions.
- Lumension has no anti-malware labs of its own and is reliant on anti-malware partner Norman to review suspicious code samples and prepare custom signatures. Disruptions to this relationship could have consequences for Lumension's customers.
- There is no personal firewall component; Lumension relies on the Windows firewall.
- Encryption requires the Sophos SafeGuard Easy management server and console to set policy.
- Native application control is limited, compared with leading solutions. The acquisition of CoreTrace will bolster this capability, but integration will take some time.
- Endpoint protection (application control, device control and anti-malware protection) does not extend beyond Windows endpoints and servers. Linux and Solaris support is now available for application control.
- Although its agent will run in VMs, Lumension has no specific optimization for anti-malware protection in virtualized environments.
- The vendor does not yet offer MDM capability or content-aware DLP capabilities.

McAfee

McAfee (a wholly owned subsidiary of Intel) holds the second-largest EPP market share worldwide and offers a broad portfolio of information security solutions. McAfee's ePolicy Orchestrator (ePO) policy management and reporting framework provides a platform that is very capable and scalable to support all McAfee products. The vendor should be considered by any large enterprise worldwide seeking solid management and reporting capabilities across a number of disparate security controls.

Strengths

- McAfee rapidly integrates acquired technology (such as encryption, DLP and application control) into its ePO platform for consistent management, reporting, logging and alerting. ePO creates stickiness, thus increasing the switching costs of organizations considering alternatives.
- McAfee VirusScan Enterprise is a full EPP offering with integrated firewall, device control and anti-malware scanning, including behavioral heuristics. Rule-based HIPS capabilities, encryption and DLP are available as additional, optional modules, all manageable within ePO.
- McAfee Application Control is a full-featured, market-leading solution for PCs and servers that fully supports sources of trusted change.
- Due to the acquisition by Intel, McAfee has expanded the number of engineers dedicated to information security and has extended its security product road maps for several years. An anti-rootkit technology, McAfee Deep Defender, is innovative in its approach, utilizing Intel's Virtualization Technology (VT) for memory introspection, and is the first of several innovative projects to exploit hardware-assisted security.
- The recent acquisitions of NitroSecurity (security event and information management) and ValidEdge (malware execution sandbox) expand McAfee's portfolio.
- McAfee Enterprise Mobility Management, offers basic MDM capability and is sold separately. (McAfee is rated a Niche Player in the MDM software Magic Quadrant.)
- McAfee Risk Advisor (available for an extra charge) can be used to provide a prioritized, risk-based view into ePO events.
- McAfee's Management for Optimized Virtual Environments (MOVE) has offered optimized anti-malware scanning in virtualized environments for two years, and, with MOVE 2.5, it offers agentless anti-malware scanning in VMware environments using native vShield API integration.

Cautions

- ePO is powerful, but at the cost of complexity. Smaller organizations will likely find the offering too complex for their resources and requirements. An SMB-friendly version of ePO is not planned until 2013. As an alternative to ePO, McAfee has provided a software as a service (SaaS)-based management console targeted at SMBs.
- McAfee's customers frequently cite overall agent footprint/impact on performance as an issue.
- McAfee has invested in overall service and support, and shows improvement; however, execution is inconsistent, as Gartner still receives some complaints from customers regarding support.
- In publicly available anti-malware testing results (such as from AV-Comparatives.org and AV-Test.org), McAfee's core malware protection capabilities have lagged. The vendor states that its focus on vulnerability-facing (versus threat-facing) protection requires trade-offs, and that end-to-end testing (such as from NSS Labs) is more representative. Improving test results is a key McAfee product management objective for 2013.

- McAfee Host Intrusion Prevention for Desktops is not widely deployed at desktops due to technical and administrative resource requirements, and is more applicable to servers where it overlaps significantly with McAfee's Application Control technology.
- Enterprise Mobility Management is not yet fully integrated into ePO (due in 1Q13).
- Intel's directional oversight into longer-term McAfee security projects is focused primarily on PC and server security, where Intel is dominant. Market acceptance of Deep Defender has been lackluster and plans for additional Deep products are less comprehensive than comparable products, such as Bromium.

Microsoft

Microsoft's Endpoint Protection solution (MEP; formerly Forefront) is intimately integrated into the popular System Center management console, and Microsoft licensing often includes MEP at no additional cost for many organizations, making it an attractive shortlist candidate. While Microsoft and Windows have many of the components of a modern EPP solution, the quality of the components and the disjointed management experience have not resulted in significant market share growth outside of budget-constrained organizations. We view MEP as a reasonable solution for Windows-centric organizations licensed under Core Client Access License (CAL) that have already deployed Microsoft System Center Configuration Manager and that have additional mitigating security controls in place.

Strengths

- Microsoft has made gradual improvements in signature-focused malware detection testing versus other vendors as a result of its investment in more proactive detection methods (such as system monitors, hidden system drivers, anti-emulation detection, JavaScript emulators, generic signatures and vulnerability-shielding capabilities). Microsoft's Malware Lab also benefits from a vast installation of the consumer version of this engine (Windows Defender and Security Essentials) and its online system check utilities, which provide a petri dish of malware samples.
- MEP relies on the software distribution capability of System Center Configuration Manager for deployment and updates. Existing System Center Configuration Manager shops need only deploy the MEP agent. System Center Configuration Manager supports a dedicated endpoint protection role configuration. MEP also allows on-demand signature updates from the cloud for suspicious files and previously unknown malware.
- Organizations that are licensed under Microsoft's Enterprise CAL (ECAL) or Core CAL program receive MEP at no additional cost, leading many organizations to consider Microsoft as a "good enough" way to reduce EPP budget expenses.
- The vendor recently added support for Mac and Linux clients via licensing of Eset.
- Microsoft offers an advanced system file cleaning that replaces infected system files with clean versions from a trusted Microsoft cloud.

Cautions

- Microsoft 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 quite high, driven primarily by cost considerations for Microsoft enterprise license holders. However, few organizations appear to be migrating, except those that are very budget-constrained.
- Microsoft System Center Configuration Manager 2012 and Active Directory are prerequisites to MEP. System Center Configuration Manager is not as easy to deploy and maintain as purpose-built EPP management platforms, and is overkill for organizations that use other PC management solutions. System Center Configuration Manager 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. There are only six preconfigured reports, although the offering includes a custom reporting capability. System Center Configuration Manager is too heavy for users of Microsoft Windows Small Business Server Essentials.
- Although it is gradually improving its signature effectiveness, MEP's performance in more advanced malware testing has been well below average.
- Despite the integration with system and configuration management, MEP does not provide a single security state assessment that combines the various security indicators into a single prioritized task list or score.
- Microsoft has been slow in providing improvements to its EPP solution.
- MEP clients rely on Windows user/administrator rights management for tamper protection. Users and applications with administrator rights can disable the client.
- MEP still lacks numerous capabilities common in other security solutions, including, advanced device control, integrated full-disk encryption, DLP and application control. Windows features, such as Firewall, BitLocker, AppLocker and Group Policy Objects, are not as full-featured as comparable solutions from leading vendors, and management of these components is not integrated into a single policy interface.
- MEP provides support for virtual environments by enabling randomization of signature updates and scans, and offline scanning. It does not integrate with vShield or provide agentless solutions.
- Windows Firewall capability lacks advanced capabilities, such as multiple location policy (it supports only two locations), extensive logging and granular policy controls. System Center Configuration Manager can manage some Windows Firewall policies, but using Group Policy Objects natively provides more extensive control, complicating management.

Panda Security

Panda Security is the first EPP vendor to fully embrace cloud delivery of security services. It offers EPP, email, Web gateways and PC management capabilities, all delivered within a cloud-based

management console. SMBs seeking easy-to-manage cloud-based solutions should consider Panda as a good shortlist entry in supported geographies (primarily Spain, Germany, Sweden, Portugal, the Benelux region and North America).

Strengths

- 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 PDF format. A large selection of template policies is provided, as well as many standard reports.
- Malware detection includes several proactive HIPS detection techniques. Panda's HIPS capability includes policy-based rules, vulnerability shielding and behavior-based detections. Trusted Boot ensures that all boot elements are trustable upon restart; and administrators have granular control to modify policies or add exclusions. Panda uses a cloud database look-up to catch the latest threats.
- Panda recently added a remote PC system management solution, which includes audit, configuration, patch and software distribution capabilities, and remote control.
- Panda also recently launched a "whitelisting as a service" option that ensures that executables are trustable.
- Panda pricing is very competitive, and there are no upfront license costs, only an annual subscription.

Cautions

- The vendor is slowly expanding from its EMEA presence, radiating outward from its Spain headquarters. However 70% of its business remains in Europe, and mind share remains weak in other geographies.
- Although Panda has several large customers, the cloud-based solutions are primarily designed for SMBs that favor ease of use over depth of functionality.
- Panda Cloud Office Protection represents the primary growth engine of the company. The legacy on-premises solutions are less strategic.
- 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.
- Panda Cloud Systems Management does not yet include support for mobile devices. It is primarily an asset inventory and remediation tool. It lacks critical security management capabilities, such as vulnerability and application control.

- The vendor is more focused on the endpoint than the server. Panda does not have any specific optimization or integration for virtualization platforms or for Microsoft SharePoint.
- 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. Basic MDM capabilities will be offered as built-in functionality in 1Q13.
- Panda doesn't yet offer encryption or DLP.

Sophos

Sophos is one of a few companies in this Magic Quadrant that sells exclusively to enterprise markets. Strong products and steady progress on a road map that addresses critical capabilities provide strong execution and growth. Given its origins, Sophos has particularly strong market penetration in Europe, although it is slowly gaining mind share in North America. The vendor primarily appeals to buyers who want simplified administration and management with solid support.

Strengths

- Sophos' management interface is, by design, very easy to use and highly capable out of the box, without excessive fine-tuning.
- Sophos also provides a vulnerability monitoring solution to reduce the attack surface of PCs.
- Data protection is enhanced with an increasing range of DLP features and context-driven encryption policies, which can be applied to data written to removable media.
- A new optional feature in SafeGuard Enterprise extends Sophos encryption to file servers and cloud storage at an additional charge.
- The vendor's products are designed to play well in virtualized environments, providing randomized scanning and updating, memory sharing, and encryption.
- Used in a VM, the SafeGuard disk encryption product does not allocate the full disk size upfront. This helps reduce the support burden for source and backup holographic versatile disc (HVD) images stored on servers.
- The Sophos Mobile Control MDM solution is designed specifically to address the needs of bring your own device (BYOD) scenarios. It is rated a Niche Player in the MDM software Magic Quadrant.
- Client-based URL filtering blocks known malicious sites, and Sophos is integrating its EPP with its Web and firewall gateway products to provide a more holistic security solution.

Cautions

- Sophos' generally weak marketing presence, particularly in North America, may cause buyers to fail to consider new features, thus miss opportunities or buy other products, because Sophos is not assertive in efforts to communicate and keep customer relationships up to date. A lack of consumer market presence further reduces opportunities for visibility.

- The vendor was recently embarrassed by a "false positive" that was very time-consuming for customers to remediate. The root cause of this event was largely avoidable with a better-designed testing process. We believe that Sophos management is aware of the gravity of this error and will do what is needed, but it represents a major black eye for a company that prides itself on service and support.
- Sophos' acquisition of unified threat management (UTM) gateway vendor Astaro may create new opportunities to compete with companies like McAfee, but does not improve Sophos' competitive standing in EPP. Indeed, EPP purchases might be impaired if buyers believe that these products will become interdependent. At the time this Magic Quadrant was prepared, there was no integration or common management console between Astaro UTM products and the EPP suite.
- Sophos MDM is now integrated with EPP management; however, it is not driving competitive buyer selections, based on Gartner client feedback and general industry product reviews. The acquisition of Dialogs (MDM and remote access solutions) may have future effects, which will be evaluated in next year's research.
- Reference customers commented on the need for better malware remediation tools from Sophos.
- Application control allows for selected blocking policies suitable to block specific applications or application classes that may be undesirable, but it is not suitable for a default deny execution environment.

Symantec

Symantec has a broad portfolio of security and management capabilities, and is the worldwide leader in EPP market share across enterprises and consumers. For enterprises, Symantec's primary offering is Symantec Endpoint Protection (SEP), currently in version 12. For servers, an extra package called Symantec Critical System Protection provides stronger host-based intrusion capabilities. To pull together its myriad consoles, Symantec has created an overlay console for administrators called Symantec Protection Center (SPC), where higher-level reporting and dashboards across products are available with drill-down access to native consoles with single sign-on. Symantec is a good choice for any organization looking primarily for solid anti-malware endpoint protection.

Strengths

- SEP 12 provides a full-featured EPP solution, including anti-malware protection, device control and its Sonar engine for behavioral heuristics. Encryption capabilities and DLP are available as separately charged (and managed) offerings.
- For protection from zero-day and targeted attacks, Symantec was a pioneer in the delivery of community and cloud-based file reputation services via Insight, introduced with SEP 12. Furthermore, Insight shares information and cooperates with Sonar to reduce false positives.

- For optimization of scanning in virtualized environments, SEP 12 can share its Insight cache across instances. Furthermore, in November 2012 the ability to use a dedicated VM for this purpose, utilizing the vShield APIs, was introduced.
- An innovative free plug-in to the SPC provides IT analytics capabilities and offers data cubes for the analysis of SEP data.
- For server-based HIPS, Symantec Critical System Protection has broad platform support, compared with competitors.
- Symantec has solid MDM capabilities from its acquisitions of Odyssey and Nukona (which provides app isolation). Symantec is rated a Challenger in the MDM software Magic Quadrant.
- Symantec Power Eraser is a good tool for scrubbing hard-to-remove infections and provides a free alternative to Malwarebytes.

Cautions

- Because of multiple acquisitions, Symantec administrators routinely interact with multiple consoles through the SPC overlay. For example, Symantec Critical System Protection uses a different console from SEP, and newer products (such as encryption) are integrated directly at the SPC level, but haven't yet been integrated for reporting.
- The Insight file reputation technology only works on file downloads and is not a full application control solution, such as those offered by McAfee, Bit9 and others.
- Although it has some vShield integration to remove critical processing from each VM, Symantec still does not offer the agentless anti-malware scanning that Trend Micro, Kaspersky Lab and McAfee offer.
- Customers using both Altiris device management and SEP 12 receive no particular synergy, except data from both can be brought together and analyzed with Symantec's IT analytics capabilities within SPC.
- Removable device encryption requires a confusing set of policies across Symantec's encryption products and SEP's device control functionality.

Trend Micro

Trend Micro is the third-largest enterprise anti-malware vendor, with a large worldwide installed base focused on the Asia/Pacific region and EMEA. Trend Micro offers two primary endpoint protection offerings — OfficeScan for desktops and laptops, and Deep Security for servers. An overlay console architecture called Control Manager can pull information from both to provide an overall dashboard, as well as policy management across endpoint and messaging security. It is the new focal point for the integration of Trend Micro capabilities, such as MDM. Trend Micro is a good shortlist candidate for buyers looking primarily for anti-malware capability.

Strengths

- Trend Micro was an early adopter of vShield API integration for agentless Deep Security anti-malware scanning in virtualized environments, including agentless network-based IPS, firewall and integrity monitoring.
- Trend Micro offers broad platform support on servers, compared with competitors.
- OfficeScan protection is augmented by malicious URL filtering, critical resource and process protection, and behavioral monitoring.
- For improved host-based firewall protection in OfficeScan, Trend Micro offers the deep-packet-inspection-capable firewall from Deep Security as a plug-in to OfficeScan, called Intrusion Defense Firewall (IDF).
- A recently launched network-based sandbox solution called Deep Discovery executes suspect code in a virtual environment and provides forensic information about the threat. It is very innovative and especially useful for organizations concerned about targeted threats.
- Trend Micro offers a simple and easy-to-use MDM capability, and is rated a Niche Player in the MDM software Magic Quadrant.

Cautions

- Trend Micro has historically been very conservative and tepid with new EPP capabilities, such as encryption and application control. More recently, it has shown signs of leadership with Deep Discovery.
- Trend Micro administrators may have to use multiple consoles. The vendor does not currently offer a single console to fully manage security settings for OfficeScan and Deep Security, although Control Manager can provide dashboarding and reporting across both products. Newer offerings such as DLP and encryption are integrated into Control Manager, while MDM is a cloud-based management console.
- vShield integration providing agentless scanning applies only to Deep Security, not to OfficeScan. For this reason, some clients use Deep Security to protect desktop workloads running in virtual desktop infrastructure sessions.
- Trend Micro does not offer application control capabilities, although this is on the vendor's road map.
- There is no out-of-the-box security state assessment beyond the EPP agent status, and no significant integration with operations tools, such as vulnerability.

Webroot

Webroot reappears in this Magic Quadrant after a complete redesign of its malware engine built on a foundation provided by the 2010 acquisition of Prevx. The new version, Webroot SecureAnywhere Business — Endpoint Protection, completely abandons traditional on-device malware signatures for

a behavior-based approach that utilizes cloud databases to keep the client small and fast. Webroot SecureAnywhere is a reasonable shortlist inclusion for organizations in supported geographies seeking a lightweight behavior-based approach to malware detection. It can also be a good additional tool for high-security organizations.

Strengths

- Webroot SecureAnywhere is one of the few vendors to completely use behavioral rules over binary signatures to identify threats. The solution leverages a cloud intelligence network, rather than a large local on-device database. This results in a very small and fast client agent. It also allows Webroot to mine aggregate behavior information from endpoints for new threats, and it removes the need for signature definition updates.
- Webroot SecureAnywhere provides a remote management tool, built-in application process monitoring, change log and rollback functionality to ease remediation, and it provides forensic information. It also features remote application management controls using its override function and a built-in identity and privacy shield to minimize the loss of sensitive data from unknown malware.
- Administrators can build policies around the actions to be taken on files introduced onto the endpoint, including those via USB or CD/DVD.
- The vendor also offers Webroot SecureAnywhere Business — Mobile Protection from within the same management console. This provides security and basic MDM capability for Android and iOS devices. The Webroot management console is cloud-based and does not require a local server.

Cautions

- Although Webroot SecureAnywhere is built on the Prevx engine that has been in production in consumer products for awhile now, the enterprise version is still relatively immature (launched in February 2012). The management console and features are aimed primarily at the needs of professional and SMB buyers.
- Due to its behavior-based malware detection approach, existing malware testing does not accurately reflect capabilities, making it hard to compare efficacy to other solutions.
- Event log data is stored on the endpoints, making search across multiple clients difficult.
- Webroot does not have support for specialized servers, such as Exchange and SharePoint. There is no specific optimization for virtualization, but the lightweight engine and cloud-assisted design helps.
- Webroot SecureAnywhere for Mac is currently only supported in the consumer Web console, not the business console.
- SecureAnywhere is strictly an anti-malware utility. It does not provide any data protection capabilities, such as encryption or DLP or port/device control, nor does it provide application control or endpoint management utilities, such as vulnerability or patch management.

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

eEye Digital Security was acquired by BeyondTrust, and Arkoon Network Security acquired SkyRecon Systems. These vendors now appear under their parent company names. Webroot reappears in this year's Magic Quadrant after the launch of its new anti-malware engine and enterprise console.

Dropped

eEye Digital Security was acquired by BeyondTrust and Arkoon Network Security acquired SkyRecon Systems. These vendors now appear under their parent company names.

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 evaluated in this research, 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 criteria used to evaluate vendors were overall viability and market responsiveness and track record. These criteria were evaluated for their contributions to the vertical dimension of the Magic Quadrant.

- **Overall Viability:** This includes 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.

- **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.
- **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.
- **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 the vendor on customer satisfaction with the company and the product.
- **Operations:** We evaluated vendors' resources 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 2013)

Completeness of Vision

The most important Completeness of Vision criteria in this analysis 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 the following product differentiators:
  - **Anti-Malware Detection and Prevention Capabilities:** This is the speed, accuracy, transparency and completeness of signature-based defenses, as well as the quality, quantity, accuracy and ease of administration of non-signature-based defenses and removal capabilities for installed malware. We looked at test results from various independent testing organizations and used Gartner inquiries as guides to the effectiveness of these techniques on modern malware.
  - **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 endpoint management operation integration have shown considerable leadership and were given extra credit for showing up as 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 DLP.
  - **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.
- **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 and/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 2013)

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 of 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

Protection from common consumer malware, as well as more advanced persistent threats, is the top critical consideration for EPP buyers. There is significant variation in the quality of attack prevention, as illustrated by malware testing.[2] Buyers should look for solutions that offer a broad cocktail of protection techniques.

Protection from highly targeted, new and low-volume attacks require a more proactive approach grounded in solid operations management processes, such as vulnerability analysis, patch management and application control capability. In particular, application control, which restricts execution to known good applications, is proving effective in demanding security environments.

Any security solutions can, in theory, be bypassed. Buyers should look for good repair tools, as well as the capability to alert administrators about threats that may have had a longer dwell time or more virulent infections. Forensic information should be sufficient to enable administrators to perform their own manual inspections for missed components of more-complex infections.

Solutions should provide a holistic security state assessment and a prioritized action plan to remediate potential security gaps. This not only enables administrators to proactively lower the attack surface on endpoints, but can also provide a performance metric that can be tracked over time to demonstrate security operations effectiveness.

Solutions should include MDM capabilities and data protection for mobile devices and employee-owned devices. Buyers should favor solutions that have a short-term road map of integration of the MDM capability into the broader suite.

Performance on virtual servers is an increasingly important critical capability. Consider the level of optimization and integration for virtual servers, but do not assume that solutions must be centralized to provide good performance.

Server platforms are commonly supported by EPP vendors; however, optimal server protection may require additional features and protection mechanisms, such as file integrity monitoring or Web application firewalls. Enterprise buyers should consider specialized server solutions.

Solutions that take a more operational tool approach will be more flexible and will provide more state information, more forensic information and better remediation capability. IT organizations that cannot handle the increased complexity should outsource EPP management to managed security service providers (MSSPs).

Market Overview

Major improvements in the EPP solutions included in this Magic Quadrant analysis focused primarily on continued improvements in the following areas:

- Software management capability
- Application Control
- MDM
- Data protection

These are positive improvements. The focus on application management (i.e., inventory, vulnerability assessment and patch management) is a tacit admission by vendors that they can no longer protect devices by relying solely on a reactive malware database. Despite years of improvements to anti-malware defenses, the rate of infections remains stubbornly high. A recent Gartner survey[1] showed that more than one-third of respondents had infections in the past 12 months that required more than a half-hour to clean. Test results[2] consistently show that all solutions fail to detect between 2% and 10% of known threats. Application management capabilities, such as inventory vulnerability assessment and patching, are critical to reducing the attack surface of endpoints. In most cases, the EPP application management solutions are not designed to replace dedicated enterprise client management tools; however, they do provide good enough capabilities for SMBs and/or provide tools for the enterprise security administrator. The exception to this rule is the enterprise client management tool vendors that have integrated anti-malware protection (i.e., LANDesk, IBM, Lumension Security, and Microsoft).

Application management is also a key prerequisite to application control. Application control is an excellent proactive security control, because it restricts endpoints to only running known good applications. Apple's iOS is a prime example of a successful application control environment. "Lean forward" organizations are already using application control to protect general-purpose PCs and designated-purpose PCs, such as point of sale or process control devices. We anticipate application control will be mainstream by 2017, and that over 50% of endpoints (including tablets and smartphones) will, by default, only run preapproved applications. Indeed, in a recent Gartner survey,[1] only 16% of users were not considering application control, while 25% had already deployed it.

Ultimately, all EPP solutions must provide a range of protection options — from very restrictive application control for single-purpose devices to light-touch configuration compliance checks for unmanaged employee devices. To that end, MDM capability provides the necessary tools to secure the rapidly changing endpoint mix as organizations expand from Windows/Intel (Wintel) dominance

to increasingly capable tablets and mobile devices. Some MDM solutions also provide excellent tools (such as application isolation utilities) to address data security issues presented by employee-owned devices. Concurrently, more-traditional tools (such as DLP and encryption) are gaining new importance, due to the rise in employee-owned devices. Currently, most EPP vendors in this Magic Quadrant analysis offer separate MDM solutions. Longer term, we anticipate that MDM-like functionality will blend fully with EPP functionality, creating a more versatile platform that can both control native security features and drop in appropriate additional security utilities across all device platforms and ownership models, ranging from hypermanaged desktop servers and PCs to completely unmanaged employee-owned tablets and phones.

Two major disappointments in the current crop of EPP solutions that need to be addressed in future products are improved security state assessments with recommended actions and an improved forensic incident response capability. While many EPP solutions have adopted flexible, customizable dashboards, very few offer good security state assessments that provide actionable, prioritized advice on how to improve the security of endpoints. Also missing are higher-level management dashboards that provide longer-term trending information on the achievement of management objectives and targets. No vendors in this research have really developed the type of information, analytics and workflow that might significantly aid in forensic response. Indeed, even a simple indicator of potential dwell time is lacking. All vendors treat every malware infection the same. However, it is clear that malware that has a longer residence (or dwell time) and those that are components of multiphased attacks require a different response. The increase in application inventory and event information resulting from more focus on application control can provide a good forensic event trail, if it is retained and searchable.

Finally, an unintended consequence of the expanding capability of EPPs is that they are becoming more complex to use, which is not ideal for small businesses or IT organizations that cannot afford increased training and administrator workload. We anticipate that more vendors will fracture products into small business solutions that focus on ease of use and more-complex enterprise solutions. We also anticipate that larger enterprise versions will incorporate more MSSP features to allow the MSSPs to service the SMB market.

Recommended Reading

Some documents may not be available as part of your current Gartner subscription.

"Magic Quadrants and MarketScopes: How Gartner Evaluates Vendors Within a Market"

"Magic Quadrant for Mobile Data Protection"

"Best Practices for Data Loss Prevention: A Process, Not a Technology"

"Understanding the Limitations of Content-Aware DLP for Mobile Devices"

"Magic Quadrant for Mobile Device Management Software"

"Magic Quadrant for Client Management Tools"

"Best Practices for Mitigating Advanced Persistent Threats"

"The Growing Importance of Cloud Access Security Brokers"

"Endpoint Protection Platforms Blending Security, System Management and Data Protection"

"MarketScope for Vulnerability Assessment"

Evidence

[1] Online survey of 113 EPP reference customers conducted by Gartner in 3Q12.

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

Note 1 Application Control

Application control solutions, sometimes referred to as application whitelisting, provide a type of endpoint protection capability. Basic application control solutions control whether a given piece of executable code is allowed to execute with more granular solutions, subsequently offering varying degrees of control over what an application can do once it is running, as it interacts with system resources. Modern application control solutions have evolved to support the dynamic requirements of end-user systems via the use of global whitelists and trusted sources of change.

Evaluation Criteria Definitions

Ability to Execute

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

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

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

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

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

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

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

Completeness of Vision

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

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

GARTNER HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
USA
+1 203 964 0096

Regional Headquarters
AUSTRALIA
BRAZIL
JAPAN
UNITED KINGDOM

For a complete list of worldwide locations,
visit http://www.gartner.com/technology/about.jsp